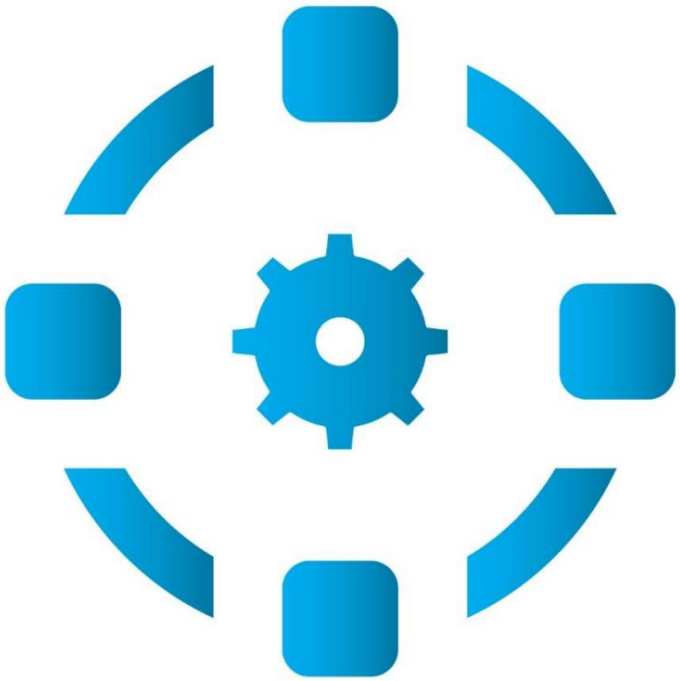
CCN-CERT IA-13/19

Ciberamenazas y Tendencias. Edición 2019



Mayo 2019

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

Fecha de Edición: mayo de 2019

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. SOBRE EL PRESENTE INFORME

Buena parte de la información aquí recogida es el resultado de la experiencia del CCN-CERT durante los meses precedentes a su publicación, en el desarrollo de sus competencias. Asimismo, se han tenido en cuenta otras fuentes documentales, nacionales e internacionales, públicas y privadas, y se ha contado con la colaboración de entidades externas, profesionales y miembros del mundo académico.

1.1. Contenido / Ámbito

Este documento contiene un análisis de las ciberamenazas, nacionales e internacionales, de su evolución y tendencias futuras, y ha sido realizado con el propósito de resultar de utilidad a los responsables de seguridad de la información de las entidades del sector público español, las organizaciones de interés estratégico y, en general, a las empresas, los profesionales y ciudadanos de nuestro país.

El ámbito territorial del presente Informe es mundial, aunque se ha puesto el acento en los países del entorno europeo y occidental. Asimismo, en determinados epígrafes, se han realizado acotaciones específicas para España y los intereses españoles en el extranjero, con especial incidencia en las redes y sistemas de información de las entidades de su Sector Público.

1.2. Base documental

La información que ha servido de base para la confección del presente Informe proviene de diferentes fuentes: documentos internos del CCN y sus organismos homólogos internacionales (especialmente de la Unión Europea, EE.UU. y los socios y aliados de España), documentos emanados de las unidades especializadas de los organismos públicos españoles, documentación de terceros (empresas y organizaciones privadas) y, finalmente, estudios y trabajos de profesionales del sector privado y miembros de la Academia.

A todos ellos, un año más, nuestro agradecimiento.

1.3. Clasificación y periodo de aplicación

El presente Informe se publica “SIN CLASIFICAR”, no estando sujeto, por tanto, a las restricciones relativas a la información clasificada.

Los datos referidos a los “Ciberincidentes de 2018” comprenden el año natural 2018 incluyendo, en algún caso y para mejor comprensión de la evolución de los hechos citados, algún dato relativo al último semestre de 2017 y los primeros meses de 2019. El apartado “Tendencias”, contiene algunos hechos que, en las materias citadas, será previsible esperar en los próximos meses.

3. RESUMEN EJECUTIVO

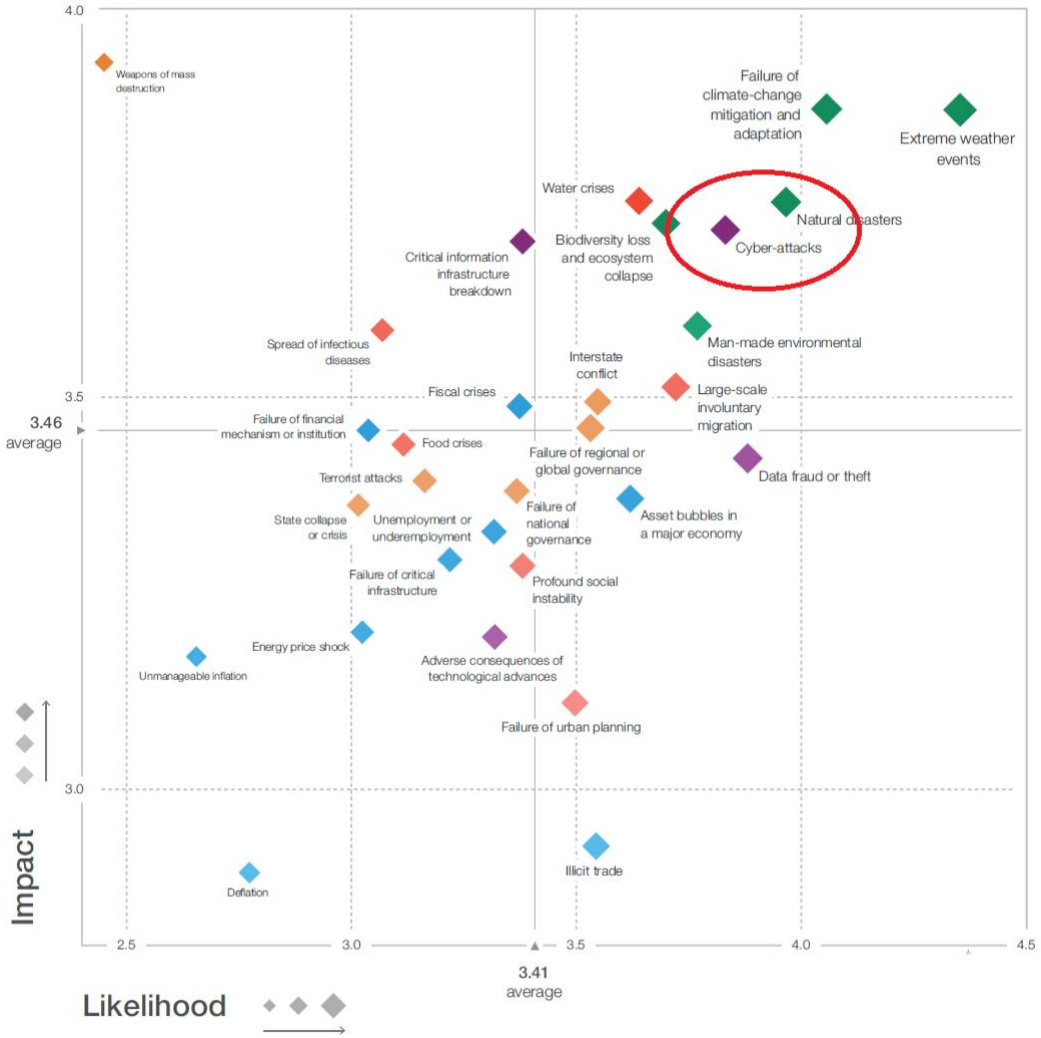
A mediados de 2018, el número de usuarios de internet en todo el mundo sobrepasaba con creces los cuatro mil millones de personas, sobre un total estimado de más de siete mil millones y medio de habitantes. En otras palabras: el 55% de la población mundial utilizan internet.

La figura siguiente muestra el desglose de los usuarios mundiales de internet atendiendo a su ubicación geográfica[1].

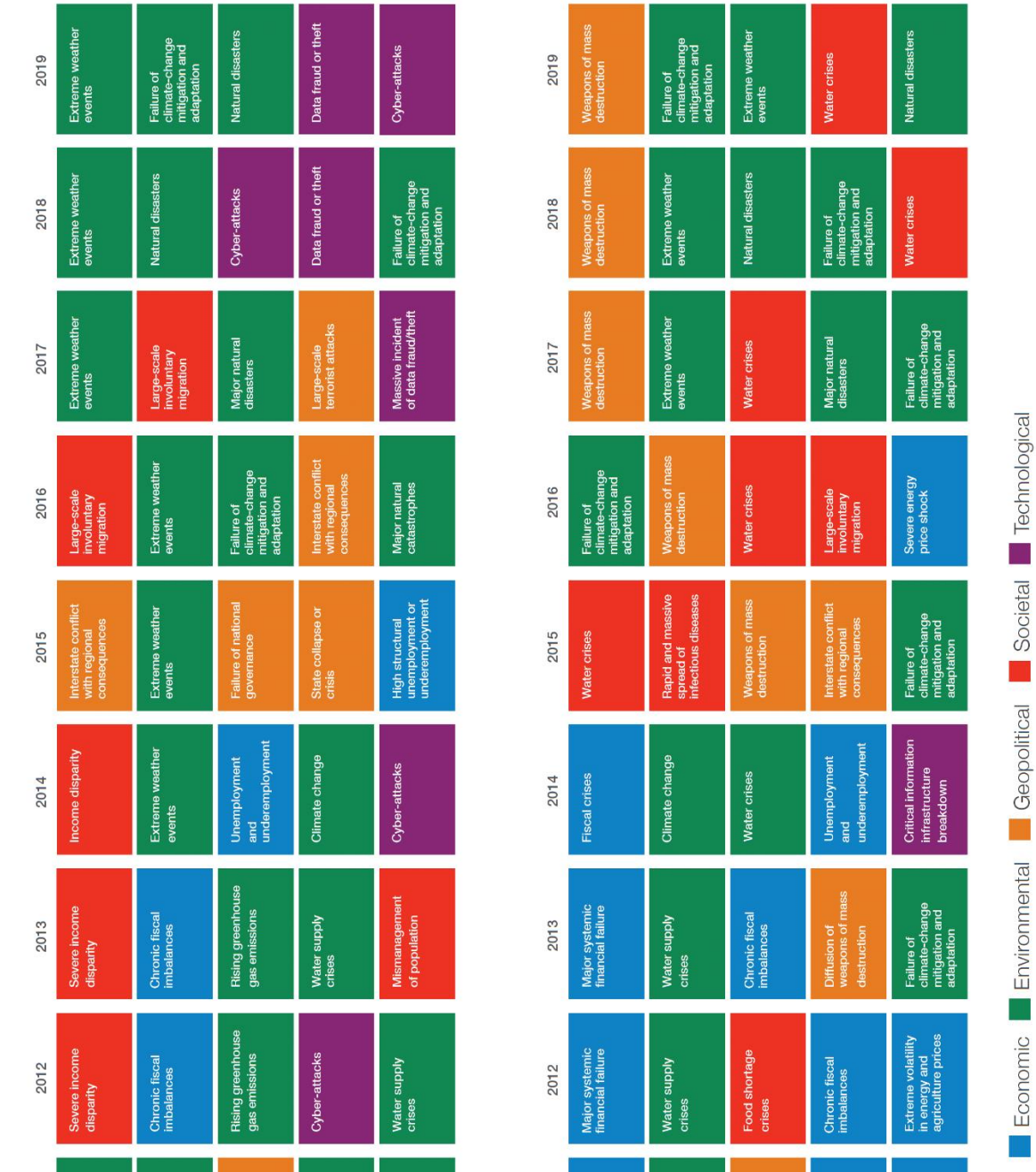
WORLD INTERNET USAGE AND POPULATION STATISTICS JUNE 30, 2018 - Update						
World Regions	Population (2018 Est.)	Population % of World	Internet Users 30 June 2018	Penetration Rate (% Pop.)	Growth 2000-2018	Internet Users %
Africa	1,287,914,329	16.9 %	464,923,169	36.1 %	10,199 %	11.0 %
Asia	4,207,588,157	55.1 %	2,062,197,366	49.0 %	1,704 %	49.0 %
Europe	827,650,849	10.8 %	705,064,923	85.2 %	570 %	16.8 %
Latin America / Caribbean	652,047,996	8.5 %	438,248,446	67.2 %	2,325 %	10.4 %
Middle East	254,438,981	3.3 %	164,037,259	64.5 %	4,894 %	3.9 %
North America	363,844,662	4.8 %	345,660,847	95.0 %	219 %	8.2 %
Oceania / Australia	41,273,454	0.6 %	28,439,277	68.9 %	273 %	0.7 %
WORLD TOTAL	7,634,758,428	100.0 %	4,208,571,287	55.1 %	1,066 %	100.0 %

Como en años precedentes, el World Economic Forum (WEF) sitúa los ciberataques entre los riesgos globales más significativos, tal y como muestra la figura siguiente[2].

[1] Fuente: Internet World Stats. (Véase: https://www.internetworldstats.com/stats.htm)
[2] Fuente: World Economic Forum, "The Global Risks Report 2019". 14Th edition. 2019.

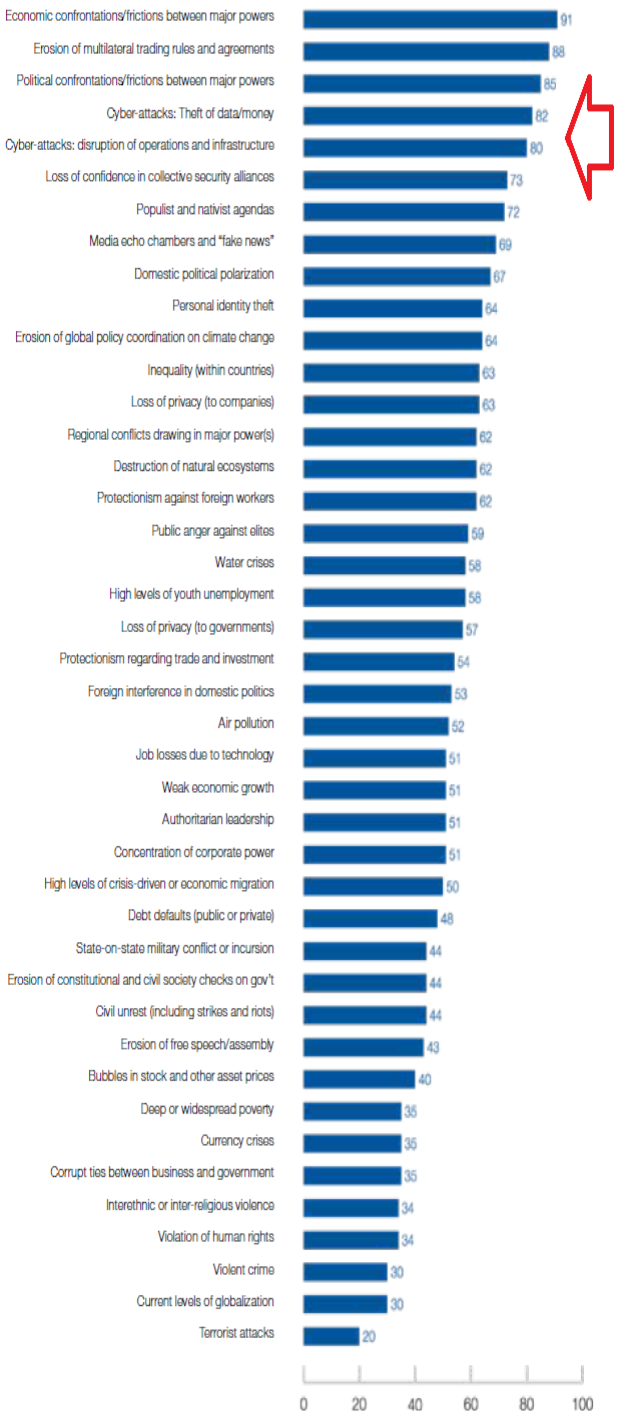


La evolución temporal de los riesgos señalados por el WEF se muestra en el cuadro siguiente.


Top 5 Global Risks in Terms of Likelihood
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
1st
Asset price collapse
Storms and cyclones
Severe income disparity
Income disparity
Interstate conflict with regional consequences
Large-scale involuntary migration
Extreme weather events
Extreme weather events
Failure of climate-change mitigation and adaptation
2nd
Slowing Chinese economy (<6%)
Flooding
Chronic fiscal imbalances
Extreme weather events
Extreme weather events
Extreme weather events
Large-scale involuntary migration
Natural disasters
Failure of climate-change mitigation and adaptation
3rd
Chronic disease
Corruption
Rising greenhouse gas emissions
Unemployment and underemployment
Failure of national governance
Failure of climate-change mitigation and adaptation
Major natural disasters
Cyber-attacks
Natural disasters
4th
Global governance gaps
Fiscal crises
Biodiversity loss
Cyber-attacks
Water supply crises
Climate change
State collapse or crisis
Interstate conflict with regional consequences
Large-scale terrorist attacks
Data fraud or theft
Data fraud or theft
5th
Retrenchment from globalization
Global governance gaps
Climate change
Water supply crises
Mismanagement of population
Cyber-attacks
High structural unemployment or underemployment
Major natural catastrophes
Massive incident of data fraud/theft
Failure of climate-change mitigation and adaptation
Cyber-attacks
Top 5 Global Risks in Terms of Impact
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
1st
Asset price collapse
Fiscal crises
Major systemic financial failure
Fiscal crises
Water crises
Failure of climate-change mitigation and adaptation
Weapons of mass destruction
Weapons of mass destruction
Weapons of mass destruction
2nd
Retrenchment from globalization (developed)
Climate change
Water supply crises
Climate change
Rapid and massive spread of infectious diseases
Weapons of mass destruction
Extreme weather events
Extreme weather events
Failure of climate-change mitigation and adaptation
3rd
Oil price spikes
Geopolitical conflict
Chronic fiscal imbalances
Water crises
Weapons of mass destruction
Water crises
Water crises
Natural disasters
Extreme weather events
4th
Chronic disease
Asset price collapse
Chronic fiscal imbalances
Diffusion of weapons of mass destruction
Unemployment and underemployment
Interstate conflict with regional consequences
Large-scale involuntary migration
Major natural disasters
Failure of climate-change mitigation and adaptation
Water crises
5th
Fiscal crises
Fiscal crises
Extreme energy price volatility
Extreme volatility in energy and agriculture prices
Failure of climate-change mitigation and adaptation
Critical information infrastructure breakdown
Failure of climate-change mitigation and adaptation
Severe energy price shock
Failure of climate-change mitigation and adaptation
Water crises
Natural disasters
Economic
Environmental
Geopolitical
Societal
Technological

Como señala el WEF, la tecnología sigue ocupando un papel importante en la configuración del panorama de riesgos globales para los individuos, los gobiernos y las empresas. En el informe citado, el "***fraude y robo masivo de datos***" fue clasificado como el cuarto riesgo más importante a nivel mundial, en un horizonte de 10 años, situando los "***ciberataques***" en quinta posición, lo que mantiene el patrón del pasado año. Pese a todo, la mayoría de los encuestados auguran un crecimiento de los riesgos de ciberataques en 2019, especialmente en lo relativo a la sustracción de dinero y/o datos (82%) y la interrupción de las operaciones (80%).

La encuesta refleja, además, la aparición de nuevas fuentes de inestabilidad a medida que se incrementa la penetración de las tecnologías digitales en la vida cotidiana. Alrededor de dos tercios de los encuestados esperan que los riesgos asociados a las **noticias falsas** y el **robo de identidad** aumenten en 2019, mientras que las tres quintas partes auguran lo mismo en relación con la pérdida de privacidad.



Source: World Economic Forum Global Risks Perception Survey 2018–2019.

Los ciberataques, unidos a una escasa adopción de medidas de seguridad, propiciaron nuevamente en 2018 la aparición de brechas masivas relacionadas con información personal. Probablemente, la mayor de ellas tuvo lugar en la **India**, donde la base de datos de identificación del gobierno, Aadhaar, sufrió múltiples violaciones que comprometieron los datos de los 1.100 millones de ciudadanos registrados.

Informaciones de enero señalaron que los delincuentes estaban vendiendo el acceso a la base de datos a un precio de 500 rupias cada 10 minutos. En marzo, una brecha de seguridad de una empresa estatal de servicios públicos permitía el acceso indiscriminado a nombres y números de identificación[3]. En otros lugares del planeta, las violaciones de datos personales afectaron a 150 millones de usuarios de la aplicación MyFitnessPal[4], y a alrededor de 50 millones de usuarios de Facebook[5].

Como ha mostrado 2018, las vulnerabilidades pueden provenir de orígenes absolutamente inesperados. Así lo evidenciaron, entre otras, las amenazas ***Meltdown*** y ***Spectre,*** que pusieron de manifiesto graves debilidades en el hardware, en lugar de en el software, como venía siendo lo habitual.

El pasado año también fue testigo de ciberataques dirigidos a las infraestructuras críticas. Las potenciales vulnerabilidades tecnológicas se han convertido en un problema de seguridad nacional. La segunda fuente de riesgos más citada en el Informe del WEF ha sido, precisamente, el emparejamiento de los ciberataques con las caídas de las infraestructuras de información críticas.

Por otro lado, la utilización de las técnicas de aprendizaje automático (***machine learning***) o el uso de modelos de **Inteligencia Artificial** (IA) son, cada vez, más frecuentes y sofisticados, evidenciando un creciente potencial para amplificar los riesgos existentes o crear nuevos riesgos; especialmente, cuando Internet de las Cosas (**IoT**) es capaz de conectar cientos de millones de dispositivos. En una investigación realizada por Brookings, el 32% de los encuestados señaló que considera la IA como una amenaza para la humanidad, frente al 24%, que opinaba en sentido contrario[6]. El pasado año, IBM detectó un código dañino dirigido, basado en técnicas IA, capaz de "ocultar" una amenaza sobradamente conocida -*WannaCry*-, en una aplicación de videoconferencia, activándose únicamente cuando reconocía el rostro del objetivo[7]. Es probable que aparezcan novedades del mismo perfil en otros campos, por ejemplo,

[3] Véase: BBC. 2018. "Aadhaar: 'Leak' in World's Biggest Database Worries Indians". BBC News. 5 January 2018. https://www.bbc.com/news/world-asia-india-42575443 . También: Whittaker, Z. 2018. 'A New Data Leak Hits Aadhaar, India's National ID Database". ZDNet. 23 March 2018. https://www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database/

[4] Véase: Hay Newman, L. 2018. "'The Under Armour Hack Was Even Worse Than It Had To Be". Wired. 30 March 2018. https://www.wired.com/story/under-armour-myfitnesspal-hack-password-hashing/

[5] Perez, S. and Z. Whittaker. 2018. "Everything You Need to Know about Facebook's Data Breach Affecting 50M Users". TechCrunch. 28 September 2018. https://techcrunch.com/2018/09/28/everythingyou-need-to-know-about-facebooks-databreach-affecting-50m-users/

[6] Véase: West, D. M. 2018. "Brookings Survey Finds Worries over AI Impact on Jobs and personal Privacy, Concern U.S. Will Fall behind China". Brookings. 21 May 2018. https://www.brookings.edu/blog/techtank/2018/05/21/brookings-surveyfinds-worries-over-ai-impact-on-jobs-andpersonal-privacy-concern-u-s-will-fall-behind-china/

[7] Véase: Stoecklin, M. Ph. 2018. "DeepLocker: How AI Can Power a Stealthy New Breed of Malware". SecurityIntelligence. 8 August 2018. https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthynew-breed-of-malware/

acciones en biología sintética, para utilizar la IA en la creación de nuevos agentes patógenos.

Uno de los *Future Shocks* para los años 2019 y siguientes son las consecuencias de la "**computación afectiva**", entendida como los modelos de IA capaces de reconocer, responder y manipular las emociones humanas. Entre los impactos más generalizados -y perturbadores- de la IA de los últimos años se encuentra su capacidad como mecanismo de ejecución de "cámaras de eco y noticias falsas", un riesgo que el 69% de los encuestados espera que aumente en los próximos años. Durante 2018, diversos equipos de investigación estudiaron el despliegue de 126.000 tweets y descubrieron que aquellos que contenían noticias falsas superaban a aquellos otros que contenían información verdadera, alcanzando la superficie de ataque (las personas) seis veces más rápido. Parece claro que la interacción entre las emociones y la tecnología se convertirá, probablemente, en una fuerza cada vez más disruptiva.

Aunque no ha habido nuevas oleadas de **ransomware**, este vector de ámbito global, sigue siendo especialmente peligroso, tal como quedó demostrado en los ataques *Petya/NotPetya* en la segunda mitad de 2017. Pese a todo, nuevas familias de ransomware siguen surgiendo permanentemente (como *Bad Rabbit* en octubre de 2017).

Sea como fuere, el **código dañino** ha seguido aumentando en 2018: hay más de 800 millones de programas conocidos de este tipo y alrededor de 390 mil nuevas variantes se suman diariamente a esa cifra. En el entorno móvil, ya se contabilizan más de 27 millones de programas de malware, solo para Android.

Los métodos de distribución masiva de código dañino también se han desarrollado en los últimos años. Por ejemplo, en 2017, el malware se distribuyó en varias ocasiones (como en el caso de *NotPetya,* por ejemplo) al comprometer los archivos o los servidores de actualización de software comercial. Además, y pese a ser conocidas, las familias de malware se modifican continuamente, incorporando funciones dañinas adicionales. Desde septiembre de 2017, el malware *Emotet* – que comenzó su andadura en 2015 como un troyano bancario, ha venido añadiendo módulos para spam, DDoS, espionaje de datos, robo de identidades, detección de sandbox, etc.- ha sido el vector usado en varios ataques en Europa.

Las **botnets de IoT** continúan evolucionando, aunque las nuevas instancias como *Hajime* y *IoT_reaper/IoTroop* no han sido tan significativas como *Mirai*. No obstante, es de esperar la aparición de nuevas -y grandes- botnets que perpetren ataques de alto impacto, y todo ello como resultado del rápido crecimiento en el número de móviles y dispositivos IoT vulnerables. En diciembre de 2017 y principios de 2018, la botnet *Andrómeda* distribuyó código dañino -troyanos bancarios, especialmente- en millones de ordenadores de todo el mundo.

Asimismo, se ha evidenciado un incremento en las revelaciones de **fugas de datos de identificación** (credenciales), lo que ha facilitado la comisión de ataques dirigidos y/o contra servicios en la nube deficientemente configurados.

Pese a la existencia de mecanismos específicos para la protección frente a **ataques DDoS** -aunque su coste de implantación es significativo-, las nuevas técnicas de amplificación usadas por los atacantes (*memcached,* por ejemplo) hacen que el nivel de la amenaza siga siendo elevado. En el primer trimestre de 2018 se han notificado en Europa ataques DDoS de hasta 190 Gbps.

Como se ha adelantado, a principios de enero de 2018, se descubrieron **vulnerabilidades** graves en la arquitectura del **hardware** de casi todos los procesadores Intel, ARM y AMD. Se trata de una nueva clase de vulnerabilidades (*Meltdown/Spectre*), resultado de errores de diseño. Desafortunadamente, las actualizaciones no pueden cerrar completamente tales brechas de seguridad, y pensar en la sustitución de todos los procesadores afectados no es realista. Por tanto, sigue existiendo el riesgo de que tales vulnerabilidades puedan explotarse durante un período de tiempo por determinar, lo que constituye una nueva amenaza para los servicios en la nube.

En 2018 también se ha producido del despegue de una nueva amenaza: la **cripto-minería ilegal**, actividad muy atractiva en términos de beneficios económicos, circunstancia a la que hay que añadir que las infecciones pueden permanecer largo tiempo sin ser detectadas. En varios casos, además, se ha constatado el uso de botnets y exploits-kits para distribuir código dañino de este tipo.

A modo de conclusión, y en comparación con 2017, el riesgo en 2018 no solo no ha disminuido, sino que puede afirmarse que ha aumentado y, sobre todo, se ha vuelto más complejo; lo que conlleva un aumento correlativo del coste de la protección de los sistemas.

Como en anteriores ediciones, el cuadro siguiente muestra los agentes de las amenazas más significativos durante 2018, la tipología de sus acciones y sus víctimas[8].

[8] Fuente: Esta matriz de amenazas se basa en la tipología de actores estudiada por M. de Bruijne, M. van Eeten, C. Hernandez Gañan y W. Pieters en "Hacia una nueva tipología de actores de amenazas cibernéticas. Un método híbrido para la evaluación de seguridad cibernética" (NCSC (TU Delft 2017)).

	GOBIERNO/ ADMÓN. PÚBLICA	INFRAESTRUCT. CRÍTICAS	EMPRESAS	CIUDADANOS
Estados y grupos patrocinados por Estados	Espionaje	Sabotaje	Espionaje	Espionaje
	Manipulación de información	Interrupción de servicios	Manipulación de sistemas	
	Acciones Híbridas	Espionaje		
Delincuentes	Interrupción de servicios	Interrupción de servicios	Robo de información	Manipulación de sistemas
	Manipulación de sistemas	Manipulación de sistemas	Manipulación de información	Interrupción de servicios
	Robo de información		Interrupción de servicios	Manipulación de sistemas
			Manipulación de sistemas	Robo de información
Terroristas	Sabotaje	Sabotaje		
Hacktivistas	Interrupción de servicios	Interrupción de servicios	Interrupción de servicios	
	Manipulación de información	Manipulación de información	Robo de información	
			Manipulación de información	
Cibervándalos y Script Kiddies	Interrupción de servicios	Interrupción de servicios	Interrupción de servicios	Robo de información
	Robo de información	Robo de información	Robo de información	
Insiders (personal interno)	Robo de información	Robo de información	Robo de información	
	Interrupción de servicios	Interrupción de servicios	Interrupción de servicios	

Se incluye una breve descripción de las amenazas que se citan:

- Interrupción de servicios: Deterioro intencionado y temporal de la disponibilidad de la información, los sistemas de información o los servicios de información.
- Sabotaje: Deterioro intencionado y a largo plazo de la disponibilidad de la información, los sistemas de información o los servicios de información, incluyendo su eventual destrucción.
- Manipulación de la información: Alteración intencionada de la información, con pérdida de su integridad.

- Robo de información: Copiado o eliminación de la información, afectando a su confidencialidad.
- Espionaje: Menoscabo de la confidencialidad de la información, generalmente protagonizado por actores estatales o patrocinados por Estados, que copian o eliminan información.
- Manipulación de sistemas: Acciones de deterioro de sistemas o servicios de información, orientadas a atacar la confidencialidad o integridad de la información o los sistemas, pudiéndose utilizar para perpetrar otros ataques.
- Amenazas híbridas: Acciones coordinadas y sincronizadas -con origen, habitualmente, en Estados y elementos patrocinados por Estados-, que atacan deliberadamente vulnerabilidades sistémicas de otros Estados y/o sus instituciones, a través de una amplia gama de medios y en distintos sectores-objetivo: políticos, económicos, militares, sociales, informativos, infraestructuras y legales, utilizando el ciberespacio como la herramienta más versátil y adecuada para sus propósitos.

4. LA REALIDAD DE LOS CIBERINCIDENTES DE 2018

En los siguientes epígrafes se desarrollan los aspectos más significativos de lo que ha constituido la base de los ciberincidentes ocurridos en 2018.

1) La soberanía digital de los Estados

La utilización de tecnología fabricada en otros Estados constituye una fuente de preocupación para los gobiernos de todo el mundo, muy especialmente de Europa, tradicionalmente más celosa de la intimidad de sus ciudadanos que otros continentes[9].

Aunque es relativamente novedoso, el concepto de "soberanía digital" se puede resumir a grandes rasgos como el impulso de un país para recuperar el control sobre sus propios datos y los de sus ciudadanos. En el lado militar, incluye también la posibilidad de un Estado para desarrollar capacidades ofensivas y defensivas de ciberseguridad sin depender de tecnología extranjera. En el aspecto económico, por su

[9] Francia, de forma singular, ha sido especialmente activa en este sentido. En octubre de 2018, tanto la Asamblea Nacional francesa como el Ministerio de Defensa francés, declararon que sus dispositivos digitales dejarían de usar Google como motor de búsqueda predeterminado. En su lugar, utilizarían Qwant, un motor de búsqueda francés y alemán que se enorgullece de no rastrear a sus usuarios. Días antes de la decisión de Qwant, el secretario de estado para asuntos digitales francés, Mounir Mahjoubi, había criticado la Ley de la Nube de los Estados Unidos, una nueva norma que permitiría a Estados Unidos acceder a los datos almacenados en las nubes de las compañías estadounidenses doquiera que se encuentren en el mundo. Añadió que Francia ya estaba preparando una respuesta con otros estados europeos para "sopesar" el tema. (Fuente: Wired, en https://www.wired.co.uk/article/google-france-silicon-valley)

parte, abarca cuestiones que van desde la tributación de las grandes empresas tecnológicas hasta la creación de nuevas empresas de origen local.

2) Los Estados como principal fuente de las amenazas

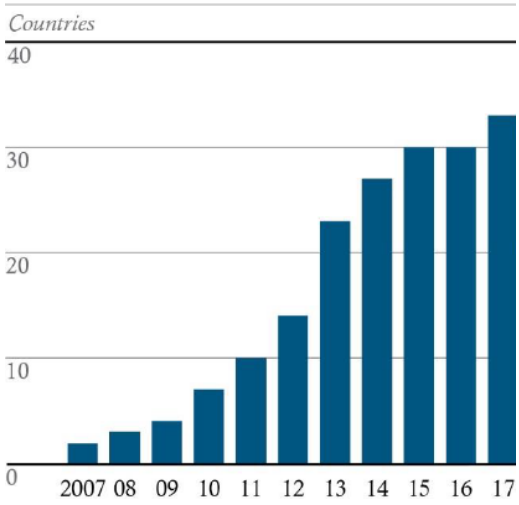
Como hemos señalado, los Estados (y los grupos patrocinados por Estados), y sus acciones contra otros países, sus instituciones, empresas y ciudadanos, siguen representando la ciberamenaza más significativa.

El objetivo perseguido por este tipo de ataques es siempre el mismo: sustraer información para mejorar su posición estratégica, política, económica o innovadora: espionaje. A este objetivo se ha unido, en los últimos años, tratar de influir en la opinión pública de los países atacados o interrumpir la normal prestación de servicios esenciales (sabotaje). Todo ello ha traído como consecuencia que la estrategia seguida por el atacante, directamente o a través de terceros previamente infectados[10], y que las herramientas para la perpetración y para la defensa desarrolladas por los propios actores, adquiridas a terceros o sustentadas en servicios de terceros, formen ya parte habitual del arsenal de los Estados.

No obstante, pese a los importantes recursos de que disponen los agentes de las amenazas, en este tipo de ataques suele ser habitual el uso de técnicas muy simples -tales como el phishing, por ejemplo-, que suelen dar buenos resultados porque se aprovechan de las vulnerabilidades humanas de la víctima, de la que recaban información sensible o confidencial, que luego puede usarse para un ataque posterior.

Las medidas más efectivas contra este tipo de ataques pasan por una adecuada concienciación en los usuarios y en la adopción de una normativa interna que señale con claridad qué puede hacerse y qué está prohibido cuando se usan medios electrónicos corporativos.

La figura muestra la evolución de estos últimos años en relación con el número de países con capacidades para perpetrar ciberataques significativos[11].



[10] Como en el caso del ataque *NotPetya*, que comprometió previamente al software que la compañía M.E. Doc distribuyó entre sus clientes.

[11] Fuente: Office of the Director of National Intelligence: Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community (Feb., 2018)

Finalmente, conviene resaltar que un ciberataque a gran escala suele comportar daños colaterales no previstos originariamente por el atacante, pudiendo alcanzar a muchas otras víctimas, incluso en distintos países[12], en una propagación incontrolada de consecuencias sociales impredecibles.

3) El incremento en el número de agentes de las amenazas

La mayor parte de los informes referidos al pasado año coinciden en señalar que el número de agentes de las amenazas ha aumentado significativamente. La accesibilidad a nuevas herramientas de ataque y la dificultad permanente para probar la autoría han sido las principales causas de este incremento.

Por otro lado, pese a que estos actores siguen prefiriendo el uso de técnicas y procedimientos de ataque específicos, 2018 ha evidenciado que cada vez es más frecuente que distintos tipos de actores usen las mismas herramientas[13].

La difusión mundial de las herramientas de ataque -usadas tanto por Estados como por organizaciones delincuenciales-, la colaboración entre grupos de atacantes y las acciones de "falsa bandera" son todos ellos evidencia de la dificultad de atribuir el uso de una táctica a un determinado grupo de actores.

Este "intercambio" dificulta aún más la atribución de la autoría de los ataques, propiciando falsas atribuciones y arrastrando consecuencias que pueden derivar en graves incidentes internacionales[14].

4) Los ataques a la cadena de suministro

En los últimos años se han acreditado varios ataques que han utilizado la cadena de suministro para distribuir software dañino. Uno de los ejemplos más significativos fue *NotPetya*, que se propagó en Ucrania a través de la actualización de una aplicación de contabilidad. Este método presenta dos ventajas para el atacante: utilizar un proveedor de confianza como origen de la distribución dañina y acotar la superficie del ataque, sin que sea fácil determinar cuáles son exactamente los objetivos perseguidos.

Esta realidad hace que las medidas de seguridad deban extenderse también a las organizaciones suministradoras de productos y servicios[15].

---

[12] Este fue el caso de *WannaCry*, que además de extenderse a más de 150 países, tuvo un señalado impacto económico y social (como, por ejemplo, en el Reino Unido, donde hizo caer los sistemas de información de buena parte del sistema sanitario británico).

[13] Por ejemplo, el exploit *EternalBlue*, filtrado por el grupo *Shadow Brokers*, se usó para perpetrar el ataque *WannaCry* de 2017. Otro ejemplo: las similitudes técnicas encontradas entre el ransomware *Petya* y el software para sabotajes *NotPetya* y el uso de materiales sustraídos de las acciones entre grupos de actores rivales. (Véase, por ejemplo: Kaspersky, *Spy wars: how nation-state backed threat actors steal from and copy each other*, October 2017. Blurring lines).

[14] Véase: Looking Ahead: Cyber Security in 2018 (https://www.fireeye.com/blog/executive-perspective/2017/12/looking-ahead-cyber-security-in-2018.html)

Aunque los prestadores de servicios están sometidos a las leyes de su país de origen, son muchas las regulaciones en materia de seguridad de la información que están extendiendo sus obligaciones a las operaciones que se desarrollan más allá de sus propias fronteras[16].

Naturalmente, y de forma independiente a las exigencias legales, las instituciones siempre pueden -y deben- establecer requisitos de seguridad para aquellas empresas que les presten servicios o suministren productos. La inadecuación de tales productos o servicios al nivel de seguridad exigido podría comportar la retirada del producto o servicio o su inadmisibilidad para presentarse a concursos públicos que involucren determinadas tecnologías.

A la vista de la efectividad y los beneficios que comporta para los atacantes, es previsible que este tipo de acciones se mantenga en los próximos años.

5) Las acciones de los grupos terroristas, yihadistas y hacktivistas

Durante 2018, la amenaza proveniente de grupos terroristas o hacktivistas se ha mantenido estable. Aunque los grupos yihadistas han continuado con sus acciones de propaganda digital, reclutamiento y recaudación de fondos, no han perpetrado -hasta ahora- ningún ciberataque significativo más allá de desfiguraciones de páginas web y sustracción de datos. Parece claro que, por el momento, siguen prefiriendo las acciones en el mundo físico[17].

6) Ciberdelincuencia y datos personales

En los últimos años, los ataques contra los datos personales se han incrementado, y no solo por parte de ciberdelincuentes o grupos hacktivistas, sino también por Estados[18]. El objetivo perseguido suele ser la comisión de ciertos delitos (fraude con tarjetas de crédito, por ejemplo), robo de identidad (credenciales), suplantación, espionaje, etc., y suelen estar dirigidos contra aquellos que más

[15] Es el caso, por ejemplo, de la aplicación en España del **Esquema Nacional de Seguridad** (RD 3/2010 – ENS), cuyo ámbito se extiende también a las entidades del sector privado que presten servicios a las entidades públicas, cuando tales servicios se encuentren dentro del ámbito de competencia de aquellas. En este mismo sentido, el Organismo de Certificación del Centro Criptológico Nacional, evalúa y certifica la capacidad de un producto para manejar información clasificada o sensible. Su Catálogo de Productos STIC, publicado en 2018, ofrece un listado de productos con unas garantías de seguridad contrastadas a organismos del sector público o entidades privadas que den servicios a éstos y que se encuentren afectados por el ENS.

[16] Tal es el caso, por ejemplo, de las transposiciones nacionales de la Directiva Europea NIS (seguridad de las redes y los sistemas de información), que plantean exigencias en materia de ciberseguridad a los prestadores de servicios digitales, independientemente del pais de Europa en el que se encuentren radicados.

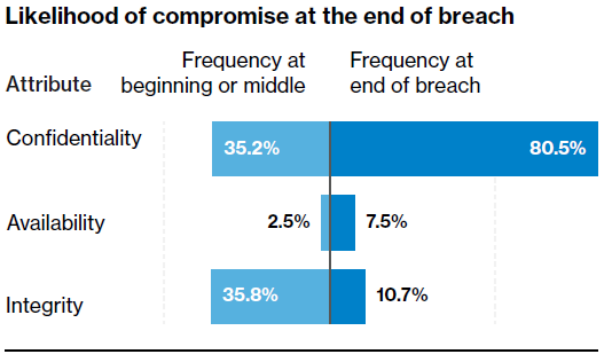
[17] ENISA Threat Landscape Report 2017. 15 Top Cyber-Threats and Trends, 1.0. ETL 2017. January, 2018

[18] Véanse:
https://www.crowdstrike.com/resources/reports/2018-crowdstrike-global-threat-report-blurring-the-lines-between-statecraft-and-tradecraft/ y
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN

información de este tipo tratan: prestadores de servicios, comercio electrónico, entidades del sector público e, incluso, instituciones educativas.

Se ha de hacer notar que determinados tipos de información personal (como la que suele usarse para la creación de identidades) no permite su alteración (la impresión dactilar, el nombre o la fecha de nacimiento de una persona no admite cambios), lo que hace muy difícil -o imposible- la reducción del impacto[19].

Sea como fuere, parece que la pérdida de la confidencialidad de los datos suele ser el resultado más frecuente de los ataques, tal y como se muestra en la figura, lo que es especialmente cierto en los ataques dirigidos (APT), en relación con acciones de ciberespionaje[20].



7) Abuso de datos y noticias falsas

A través de un acuerdo comercial con Facebook (uso app ThisIsYourDigitalLife para tests de personalidad), Cambridge Analytica recolectó más de 50 millones de datos de usuarios, permitiendo explotar la actividad en redes sociales privadas que luego fueron utilizados mediante la técnica del microtargeting para anuncios políticos durante las elecciones presidenciales de 2016 en EE.UU.

Es sabido que el análisis masivo de datos a través de las actuales herramientas de Big Data permite extraer perfiles detallados de preferencias y tendencias personales en muchas áreas, no solo en política. Del mismo modo que las noticias falsas persiguen influir en las opiniones y el comportamiento de los individuos, la información personal distribuida en las redes sociales (Facebook, Twitter, LinkedIn, etc.), una vez analizada y correlacionada adecuadamente, puede posibilitar el desarrollo de sofisticados -e individualizados- ataques de ingeniería social.

8) Elementos facilitadores de los ciberataques

Los elementos facilitadores, pese a no constituir por sí mismos herramientas de agresión, son aquellas entidades o componentes que, en un instante dado,

[19] Cinco Días (3 de diciembre de 2018): "Hemos recibido más de 300 notificaciones de brechas de seguridad y, de ellas, menos de 10 han supuesto actuaciones de investigación en la Inspección". (Mar España, directora de la AEPD).
[20] Fuente de la figura: Verizon: 2018 Data Breach Investigations Report.

incrementan la accesibilidad y/o la efectividad de ulteriores ataques o los métodos usados en su comisión. Tal es el caso, por ejemplo, de los delincuentes que intercambian información sustraída (datos personales, credenciales de identidad o datos de tarjetas de crédito), propiciando posteriores ataques; o las entidades que construyen, alquilan o ponen a disposición de terceros (en la Dark Net), infraestructuras para la comisión de tales acciones (botnets, por ejemplo), posibilitando que agentes de las amenazas con escasos conocimientos puedan perpetrar ataques de forma fácil y a un coste asumible, etc. Las acciones de todos estos elementos facilitadores disminuyen el umbral de exigencias para los atacantes[21].

Por su parte, como hemos venido señalando, la incesante conexión de nuevos dispositivos IoT a Internet, para los que la seguridad no constituye un objetivo de diseño, propiciando con ello la distribución de código dañino o participando en ataques DDoS, constituye también un significativo elemento facilitador de esta problemática.

Finalmente, el **cryptojacking**[22], pese a ser una realidad bastante novedosa, conformará una de las amenazas más serias de los próximos años. Como es sabido, las acciones relacionadas con esta metodología persiguen obtener ingresos usando la capacidad de proceso de los ordenadores de las víctimas, situación que puede alcanzarse atacando redes Wi-Fi[23], sitios web o, incluso, ofreciendo alternativas a la publicidad[24].

9) Los tiempos implicados en los ciberataques

En la generalidad de los casos analizados, y cuando los ataques tienen éxito, el plazo para que se vea comprometido el sistema de información sigue siendo muy corto.

Aunque no puede determinarse en todos los casos cuánto tiempo se requiere para la recopilación de la inteligencia previa, el tiempo que media entre la primera acción hostil hasta el compromiso de un activo se mide, frecuentemente, en términos de segundos o minutos. Sin embargo, el plazo para su descubrimiento o detección (que

[21] Aunque el denominado *Crime-as-a-Service* (*CaaS*) existe desde hace algunos años, se ha vuelto más accesible. Las herramientas que se alquilan son cada vez más avanzadas y versátiles, y su número está creciendo significativamente. (Véase: https://www.bankinfosecurity.com/interviews/crime-as-service-top-cyber-threat-for-2017-i-3406)

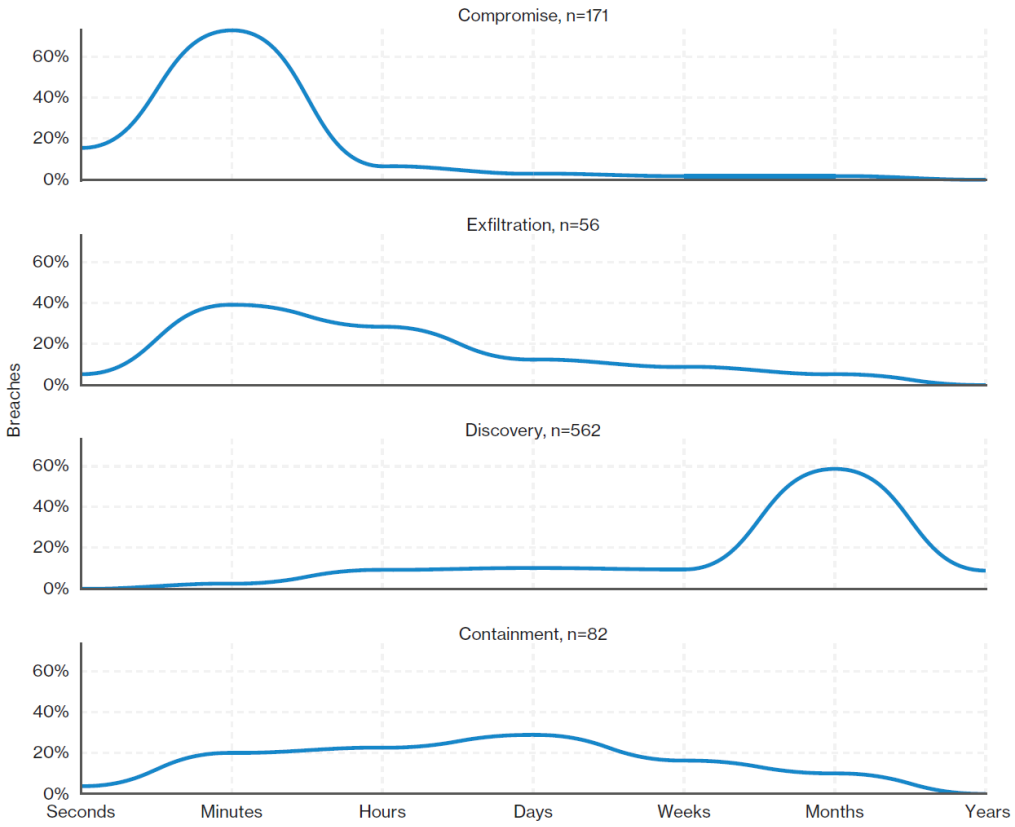
[22] Existen determinados sitios web -de dudosa consistencia ética- que dan a elegir al usuario entre mostrar publicidad o colaborar con la capacidad de procesamiento de su ordenador para ejecutar cryptomining).

[23] Véase: Sophos: Starbucks Wi-Fi hijacked customers' laptops to mine cryptocoins, en https://nakedsecurity.sophos.com/2017/12/14/starbucks-wi-fi-hijacked-customers-laptops-to-mine-cryptocurrency/

[24] Por ejemplo, uno de los actores que ofrece código de minería criptográfica como servicio a los propietarios de sitios web es Coinhive. (Véase: Kreb on Security: Who and What Is Coinhive?, en https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/)

depende, en gran medida, del tipo de ataque) suele expresarse en días, semanas o meses.

La figura siguiente muestra un gráfico con una estimación de los tiempos implicados en los ciberataques[25].



5. AGENTES DE LAS AMENAZAS

Como todos los años, ENISA ha elaborado un cuadro en el que se señalan las amenazas más significativas, atendiendo simultáneamente al tipo de actor y al vector de ataque usado[26].

[25] Fuente: Verizon: 2018 data Breach Investigations Report.
[26] Fuente: ENISA – Threat Landscape Report 2019 (Jan, 2019).

Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	→
2. Web Based Attacks	↑	→
3. Web Application Attacks	➲	→
4. Phishing	↑	→
5. Denial of Service	↑	↑
6. Spam	➲	↓
7. Botnets	↑	↑
8. Data Breaches	↑	↑
9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	➲	→
11. Information Leakage	↑	↑
12. Identity Theft	↑	→
13. Cryptojacking	↑	NEW
14. Ransomware	↓	↓
15. Cyber Espionage	↓	→

1.4. Los Estados como agentes de las amenazas

Durante el periodo analizado, se ha evidenciado un incremento en el uso de código dañino por parte de los Estados dirigido a explotar vulnerabilidades de los sistemas de información de las Infraestructuras Críticas. Frecuentemente, el objetivo de tales ataques es obtener información sobre el grado de implantación de las medidas de seguridad de las organizaciones, al objeto de poseer datos suficientes que les permita planificar ataques futuros. Esta actividad se ha detectado, especialmente, contra objetivos europeos.

En septiembre de 2017, la compañía de seguridad Symantec informó sobre nuevos ataques por parte de un grupo conocido como *Dragonfly 2.0*[27]. Esta campaña, también conocida con el nombre de *Havex*, *Crouching Yeti, Koala Team* y *Energetic Bear*, se centró en explorar el entorno operativo de las compañías de energía y en la instalación de puertas traseras. Además de los motivos relacionados con el ciberespionaje, el objetivo final estaba más dirigido a facilitar un sabotaje posterior.

Los equipos de investigación detectaron ataques de este tipo en EE. UU., Turquía y Suiza.

Aunque el código dañino usado posibilitaba sabotear Sistemas de Control Industrial, en la práctica se usa, principalmente, para acciones de ciberespionaje. El actor utilizó dos exploit-kits (*LightsOut* y *Hello*) y varias herramientas de acceso remoto (RAT) (*Havex*, *Karagany* y *Oldrea*). En marzo de 2018, investigadores de la compañía de seguridad Cylance sugirieron que los routers Cisco comprometidos también fueron utilizados en los ataques[28].

En octubre de 2017, el US-CERT norteamericano informó sobre ataques de actores muy especializados a infraestructuras críticas, vinculados a la campaña Dragonfly 2.0[29]. Los atacantes concentraron su atención en los accesos poco seguros de pequeñas redes para penetrar en las redes de las principales organizaciones del sector energético. El análisis realizado por el US-CERT reveló que, allí donde no estaba implementada la autenticación de doble factor, los detalles de inicio de sesión

[27] El grupo *Dragonfly*, también conocido como *Energetic Bear*, ha estado activo desde, al menos, 2011, cuando atacó a compañías de defensa y aviación en Estados Unidos y Canadá. En una segunda fase, *este grupo* centró su actividad en las empresas de energía de EE. UU. y Europa, a principios de 2013. En 2014, los expertos en seguridad de Symantec descubrieron una nueva campaña dirigida a organizaciones ubicadas en Estados Unidos, Italia, Francia, España, Alemania, Turquía y Polonia. *Dragonfly* llevó a cabo una campaña de ciberespionaje contra operadores de redes de energía y las principales empresas de generación eléctrica, operadores de oleoductos y proveedores de equipos industriales del sector energético. De acuerdo con el informe JAR-16-20296A publicado por el Departamento de Seguridad Nacional de EE. UU., *Dragonfly* es un actor ruso vinculado al gobierno.

[28] Ver: Cylance: https://threatvector.cylance.com/en_us/home/energetic-dragonfly-dymalloy-bear-2-0.html

[29] Véase: Alert (TA17-293A) Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors (en https://www.us-cert.gov/ncas/alerts/TA17-293A)

recopilados se usaron para obtener acceso a la red de las víctimas, lo que permitió a los atacantes realizar un reconocimiento de la red interna e, incluso, de los propios sistemas ICS.

Como se señaló durante 2017, el grupo *Shadow Brokers* publicó herramientas de hacking cuyo origen se atribuye a los servicios de inteligencia norteamericanos.

Las herramientas más significativas fueron *Eternal Blue* y *Eternal Romance*, que explotan el protocolo de intercambio de archivos SMB en sistemas Windows, y la herramienta *DoublePulsar*, una puerta trasera que puede instalarse en los sistemas infectados para ejecutar código dañino. El uso de estas acciones se ha publicado recientemente.

El código dañino Triton-Trisis, dirigido a sistemas de seguridad.

En diciembre de 2017, se descubrió un código dañino que podía reprogramar los sistemas de seguridad Triconex de la compañía Schneider Electric. Estos sistemas se utilizan como medio de respaldo en la seguridad de procesos Industriales, químicos o nucleares, siendo usados en miles de plantas de fabricación en todo el mundo.

En marzo de 2018, el New York Times informó que el código dañino pudo haber sido utilizado en un intento para sabotear una planta petroquímica en Arabia Saudita[30]. Según este periódico, el malware podía ser capaz de modificar un sistema de control con el propósito de causar una explosión. Un pretendido error en el código pudo haber evitado la catástrofe. Debido al alto nivel de sofisticación del ataque, se asoció con un actor estatal.

Nuevos datos en relación con los ataques dirigidos al abastecimiento eléctrico en Ucrania

En el período del informe anterior, un ciberataque provocó la caída de una buena parte de la infraestructura eléctrica de Ucrania. En junio de 2017, la empresa de seguridad ESET publicó un informe de investigación sobre el malware pretendidamente utilizado en el ataque. El código usado, al que los investigadores denominaron *Industroyer*, podía comunicarse con los sistemas de control industrial (ICS) que se utilizan para el control de redes eléctricas. Además, también podría usarse

[30] Véase: The New York Times: A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try (en https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html)

contra organizaciones de otras industrias y/o países. Una condición previa importante es que el atacante debe tener acceso a la red del objetivo. El ataque también fue analizado por investigadores de la compañía de seguridad Dragos, que atribuyó la acción al grupo *Electrum*. Se señaló, entonces, que este grupo estaba estrechamente asociado con el grupo *Sandworm*, que ya había estado actuando durante varios años en campañas de espionaje contra empresas e instituciones de Ucrania y contra varios sectores en Europa y Estados Unidos, incluido el sector energético, el gobierno, las telecomunicaciones y el sector académico.

Como se ha señalado, en junio de 2017, el vector del ciberataque *NotPetya* (también denominado *PetrWrap, GoldenEye* y *ExPtr*), fue el software de contabilidad de la compañía M.E.Doc. Los atacantes usaron las credenciales sustraídas de inicio de sesión para insertar código dañino en una actualización de dicho software. Tras la infección, el código dañino -que utilizó componentes de diversas procedencias, tales como el exploit *EternalBlue* que se había utilizado anteriormente en *WannaCry*- se propagó como un gusano dentro de las redes de las organizaciones afectadas. Aunque en un principio se pensó que se trataba de ransomware, las investigaciones posteriores revelaron que el descifrado no era posible, impidiendo por tanto el pago de extorsiones y evidenciando que el atacante no era un delincuente que persiguiera ingresos.

Varias compañías de seguridad afirmaron que *NotPetya* estaba específicamente dirigido a Ucrania. Como se ha señalado, el Servicio Secreto ucraniano, Estados Unidos y el Reino Unido acusaron directamente a Rusia de participar en el ciberataque[31].

[31] Véase: BBC News: UK and US blame Russia for 'malicious' NotPetya cyber-attack (en https://www.bbc.com/news/uk-politics-43062113)

Finalmente, en agosto y septiembre de 2017, el popular software *CCleaner* fue infectado con el troyano *Floxif*[32]. El código dañino se inyectó en el programa durante la fase de desarrollo, lo que hacía que la firma electrónica del programa fuera correcta. La empresa de seguridad Cisco Talos reveló que se trataba de un ataque dirigido[33]. De los 700.000 sistemas que hicieron contacto con el Servidor C&C, se detectó una infección de segunda fase, oculta en, al menos, 20 sistemas de información.

```
$DomainList = array(
"singtel.corp.root",
"htcgroup.corp",
"samsung-breda",
"Samsung",
"SAMSUNG.SEPM",
"samsung.sk",
"jp.sony.com",
"am.sony.com",
"gg.gauselmann.com",
"vmware.com",
"ger.corp.intel.com",
"amr.corp.intel.com",
"ntdev.corp.microsoft.com",
"cisco.com",

"uk.pri.o2.com",
"vf-es.internal.vodafone.com",

"linksys",
"apo.epson.net",
"msi.com.tw",
"infoview2u.dvrdns.org",
"dfw01.corp.akamai.com",
"hq.gmail.com",
"dlink.com",

"test.com");
```

Las víctimas fueron las principales empresas del sector tecnológico.

Además de ello, los actores estatales siguen utilizando spearphishing para el ciberespionaje. En marzo de 2018, el Departamento de Justicia norteamericano dio a conocer detalles de los cargos contra nueve iraníes, acusados de sustraer 31 TB de documentos y datos de más de 140 universidades americanas, 30 empresas, cinco organizaciones gubernamentales y más de 176 universidades en otros 21 países.

Parece demostrado que los atacantes utilizaron los datos de inicio de sesión de los empleados, que habían sido sustraídos usando correos electrónicos de phishing, acciones que habrían ocurrido entre 2013 y 2017[34]. Los sospechosos estaban vinculados al Instituto Mabna, una organización iraní creada en 2013 con el objetivo explícito de obtener ilegalmente acceso a fuentes académicas no iraníes a través de ciberataques. En sus acciones, los actores habrían estado recopilando información de investigaciones, datos científicos, secretos industriales y propiedad intelectual. Según el FBI, el instituto fue contratado por varios elementos del gobierno iraní, incluida la Guardia Revolucionaria Islámica, una de las entidades responsables de recopilar

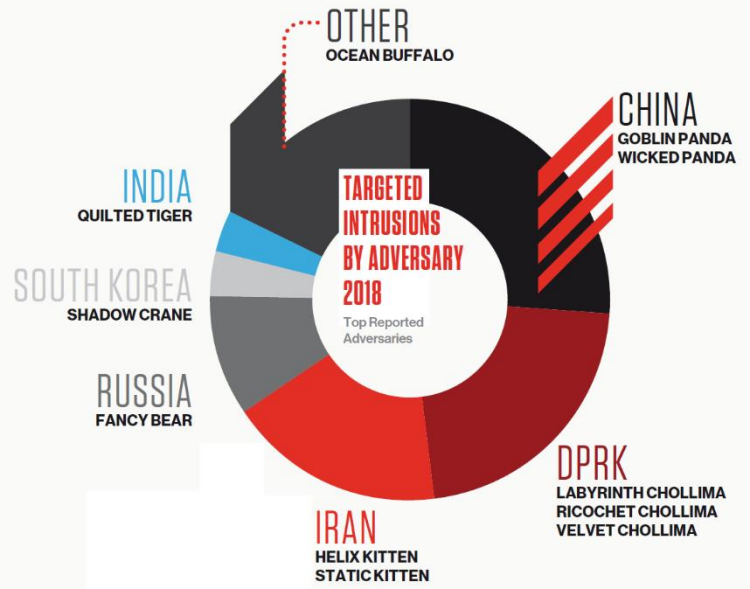
[32] Véase: Forbes: Hackers Hid Backdoor In CCleaner Security App With 2 Billion Downloads -- 2.3 Million Infected (en https://www.forbes.com/sites/thomasbrewster/2017/09/18/ccleaner-cybersecurity-app-infected-with-backdoor/#13fa078f316a

[33] Véase: Cisco Talos: CCleaner Command and Control Causes Concern (en https://blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html)

[34] Véase: USA, Department Of Justice: Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps, (en https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary)

información. El FBI ha señalado que los atacantes sustrajeron datos para el gobierno iraní y ofrecieron los datos sustraídos a través de dos sitios web iraníes (megapaper.ir y gigapaper.ir).

Para finalizar, atendiendo a un informe de Crowdstrike, incluimos la distribución de los ciberataques de este tipo, por estado[35].



Las amenazas híbridas patrocinadas por Estados - Eliminación de cuentas de Facebook

El 3 de abril de 2018 Facebook eliminó numerosas cuentas y páginas en sus plataformas Facebook, WhatsApp e Instagram, que estaban asignadas a la Agencia Rusa de Investigación de Internet (IRA). La IRA rusa es una "fábrica de trolls", presuntamente patrocinada por el Estado, que distribuye contenido falso en las redes sociales, utilizando cuentas falsas. Las cuentas afectadas, en su mayoría de un sitio denominado *IRA Open*, eran de habla rusa y habían difundido información falsa o contenido que pretendía influir en la opinión pública[36].

Sumando todas las cuentas, páginas y banners publicitarios afectados que podrían haber distribuido dicho contenido, Facebook estima un total de aproximadamente un millón de páginas vistas. En septiembre de 2017, Facebook anunció que los actores rusos habrían invertido cerca de 100.000 dólares en publicidad

[35] Fuente: Crwodstrike: 2019 Global Threat Report.

[36] Se trata de un ejemplo más de lo que se han denominado "Amenazas Híbridas". Sobre este tema puede consultarse el Documento de Trabajo "Amenazas Híbridas: nuevas herramientas para viejas aspiraciones", (Dr. Carlos Galán, Real Instituto Elcano, en http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/dt20-2018-galan-amenazas-hibridas-nuevas-herramientas-para-viejas-aspiraciones)

para difundir información falsa entre junio de 2015 y mayo de 2017.

A principios de 2018, Twitter anunció que había identificado casi 4.000 cuentas de usuarios conectadas al IRA ruso, diez semanas antes de las elecciones presidenciales de EE. UU. Estas cuentas se utilizaron para publicar unos 180.000 tweets, el 8,4% de los cuales estaban relacionados con dichos comicios.

Por su parte, la plataforma de blogs Tumblr anunció, en marzo de 2018, que también había identificado 84 cuentas vinculadas al IRA ruso.

1.5. Los ciberdelincuentes

La delincuencia sigue encontrando en el ciberespacio un medio cada vez más rentable para desarrollar sus acciones ilícitas.

En 2018, los ciberdelincuentes continuaron siendo uno de los grupos más activos de agentes de las amenazas, con más del 80% de la actividad dañina[37]. Se estima que el 0,85% del Producto Interior Bruto (PIB) de todo el mundo se ve afectado por este grupo de actores[38].

Respecto de los métodos más usados, a la cabeza se encuentra la propagación de código dañino a través de los **correos electrónicos**[39]: más del 60% del tráfico mundial de correo electrónico en 2018 contenía carga dañina y estuvo involucrado en más del 90% de los ciberataques.

Por otro lado, en 2018 ha aparecido un nuevo desarrollo vinculado a la monetización directa: el uso de malware de criptojacking/cryptomining[40] o contra criptomonedas que, según estimaciones, ha podido provocar pérdidas de 880 millones de dólares[41]. No obstante, y pese a que en 2018 el cryptojacking/cryptomining parece estar reemplazando al ransomware[42], su monetización no es todavía muy alta[43].

Otra tendencia clara en los ciberataques delincuenciales de 2018 ha sido el refinamiento del phishing mediante el uso de técnicas de ingeniería social[44] y la

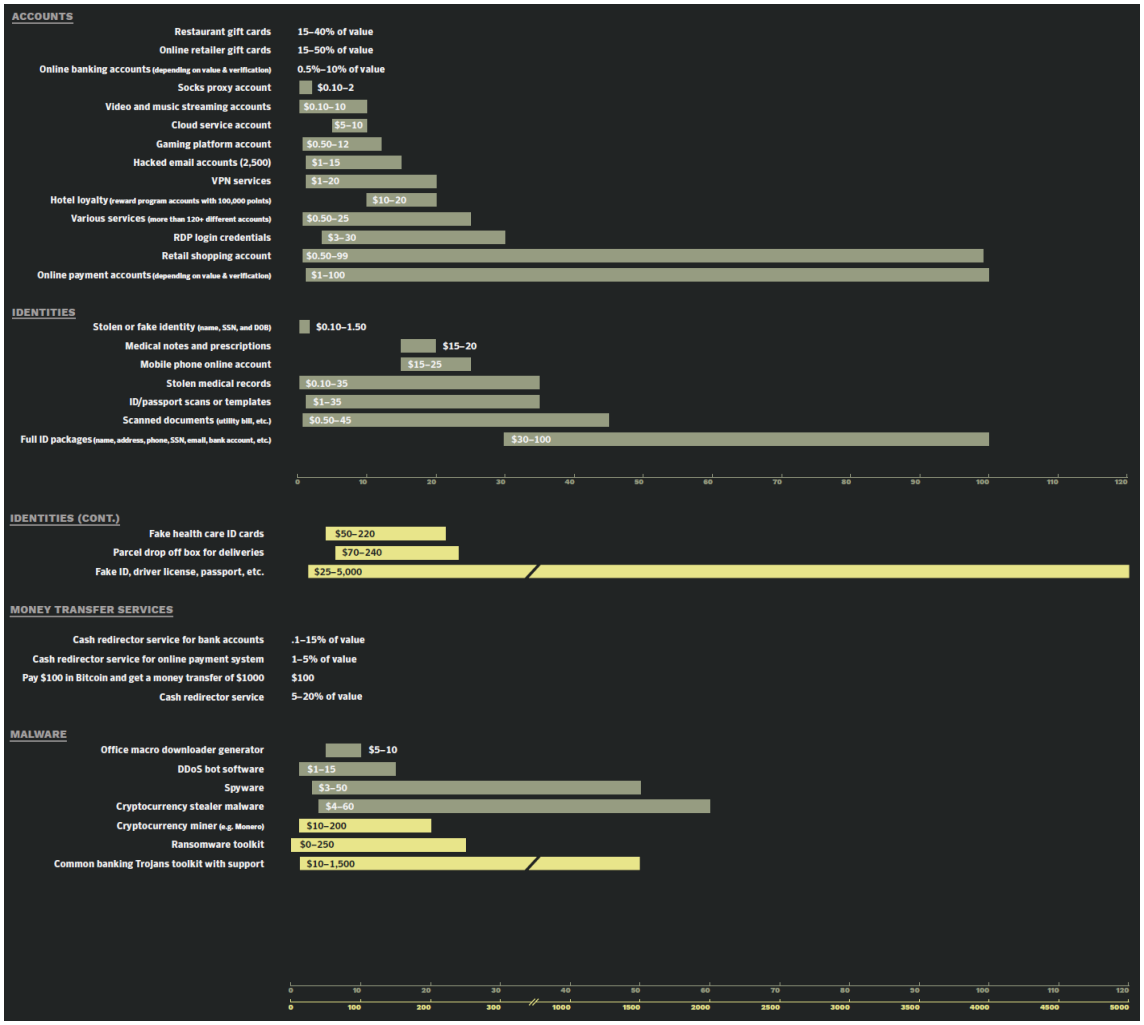
[37] Véase: https://www.hackmageddon.com/category/security/cyber-attacks-statistics/
[38] Ver: https://www.computerweekly.com/news/252435439/Economic-impact-of-cyber-crime-is-significant-and-rising
[39] Ver: https://brica.de/alerts/alert/public/1229120/malware-less-email-attacks-increasingly-common-fireeye-finds/
[40] Véanse: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018 y https://cio.economictimes.indiatimes.com/news/digital-security/crypto-thefts-drive-growth-of-global-coin-money-laundering/64881793
[41] Ver: https://securityaffairs.co/wordpress/77213/hacking/cyber-attacks-crypto-exchanges.html
[42] Ver: https://www.bankinfosecurity.com/cryptojacking-displaces-ransomware-as-top-malware-threat-a-11165
[43] Ver: https://www.theregister.co.uk/2018/08/30/cryptojacking_pays_poorly/
[44] Ver: https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf

innovación permanente para persuadir a los usuarios de la autenticidad de las estafas[45].

También se debe mencionar la tendencia a la innovación en las plataformas del Ciberdelito como Servicio (*Crime as a Service*)[46]. Además de las mejoras en los servicios ofertados, estos desarrollos ofrecen una mayor facilidad de uso, lo que contribuye a extender su popularidad y propiciar ataques más eficientes.

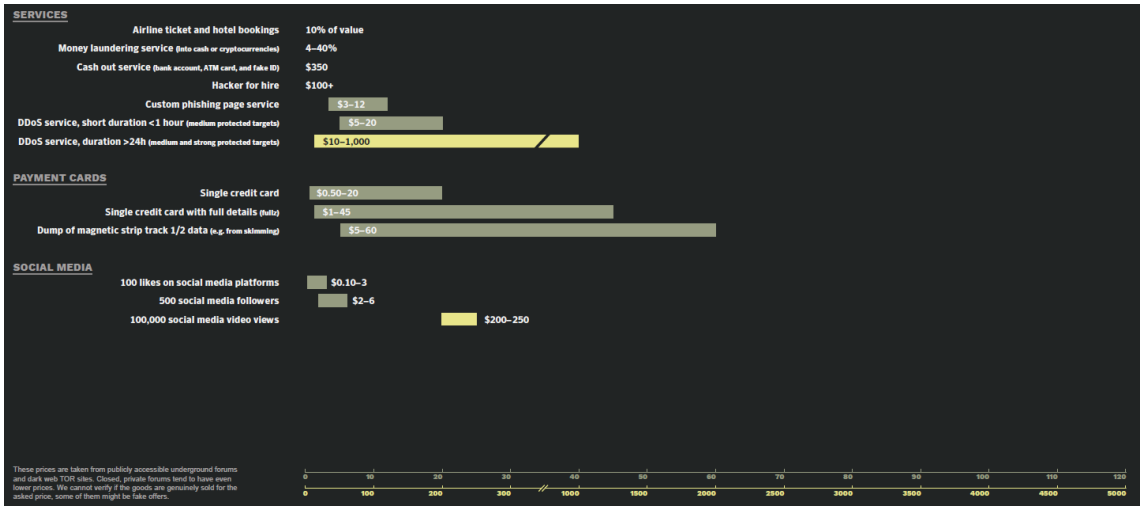
Finalmente, hay que recordar que los riesgos de operar en el ciberespacio, si se usan las herramientas adecuadas, son muy bajos, al contrario que los beneficios, que pueden llegar a ser muy elevados.

Los cuadros siguientes muestran la actividad de monetización de las actividades delincuenciales, de lo que se ha dado en llamar *economía underground*.



[45] Ver: https://blog.trendmicro.com/trendlabs-security-intelligence/phishing-campaign-uses-hijacked-emails-to-deliver-ursnif-by-replying-to-ongoing-threads/

[46] Ver: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018



1.6. Ciberterrorismo y Ciberyihadismo

En 2018 no se han encontrado evidencias especialmente significativas de acciones de ciberyihadistas aislados, es decir, personas o pequeños grupos motivados por motivos religiosos. En la actualidad, el ciberterrorismo parece asociado a comportamientos muy definidos de grupos terroristas convencionales o, incluso, de actores patrocinados por Estados[47].

Pese a todo, en 2018, la convergencia entre el ciberespacio y el terrorismo permanece: los terroristas continúan utilizando servicios legítimos para diseminar propaganda a nivel mundial, reclutar nuevos miembros o realizar captaciones de fondos con los que financiar sus operaciones. Así, la monetización y el reclutamiento son los objetivos principales de este grupo de agentes de las amenazas[48], que viene exigiendo una estrecha cooperación entre los cuerpos policiales y los servicios de inteligencia de todo el mundo.

Una de las actividades más importantes para contrarrestar esta amenaza es lograr un mejor control de las redes sociales (utilizadas para el reclutamiento y la financiación), persiguiendo la identificación de los actores dañinos[49]. Otro elemento importante es la observación de los flujos de dinero, especialmente los realizados con criptomonedas[50].

[47] Ver: https://www.recordedfuture.com/iran-hacker-hierarchy/

[48] Ver: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

[49] Ver: https://www.thenational.ae/world/europe/eu-plans-new-laws-to-target-terror-on-social-media-sites-1.762013

[50] Ver: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

Por lo que respecta a las capacidades de los terroristas para la realización de ciberataques, se ha evidenciado que, a pesar de la existencia de poderosas herramientas en la *dark web*, este grupo de actores aún mantiene bajas capacidades de acción[51], lo que no ha sido obstáculo para que varios Estados hayan incluido la protección contra el ciberterrorismo en sus agendas para la defensa nacional[52].

Por otro lado, dada la disponibilidad del *Crime-as-a-Service* y el potencial para reclutar elementos humanos, los análisis internacionales muestran que el ciberterrorismo aumentará significativamente en los próximos años[53]. Estas predicciones, observadas desde el punto de vista de las vulnerabilidades de los sistemas de control industrial (ICS), parecen bastante plausibles[54].

1.7. Los hacktivistas

Los hacktivistas han continuado su actividad en 2018 a un ritmo similar al de años anteriores[55], en base a campañas de desfiguración de páginas web[56] y ataques DDoS, con el objetivo de llamar la atención de los medios, sin perseguir, en general, la monetización de sus acciones.

Motivados las más de las veces por desarrollar operaciones de protesta contra decisiones políticas que afectan a asuntos nacionales o internacionales, a través de células independientes o con bajo nivel asociativo[57], los hacktivistas han concentrado su atención en 2018 en los derechos de las mujeres y la violencia con armas de fuego[58].

Desde el punto de vista técnico, Linux y Apache han sido las principales plataformas web comprometidas en sus acciones[59].

---

[51] Ver: https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2018.html

[52] Véanse: https://www.justice.gov/ag/page/file/1076696/download , https://www.defense.gouv.fr/english/actualites/articles/les-manipulations-de-l-information-un-defi-pour-nos-democraties y http://www.basicint.org/publications/stanislav-abaimov-paul-ingram-executive-director/2017/hacking-uk-trident-growing-threat

[53] Ver: https://www.raytheon.com/sites/default/files/2018-02/2018_Global_Cyber_Megatrends.pdf

[54] Véanse: https://www.darkreading.com/risk/take-(industrial)-control-a-look-at-the-2018-ics-threat-landscape/d/d-id/1332754 y https://securelist.com/threat-landscape-for-industrial-automation-systems-in-h1-2018/87913/

[55] Ver: https://www.hackmageddon.com/category/security/cyber-attacks-statistics/

[56] Véase el compendio de técnicas usadas en https://blog.trendmicro.com/graffiti-in-the-digital-world-how-hacktivists-use-defacement/ y https://blog.trendmicro.com/trendlabs-security-intelligence/hacktivism-web-defacement/

[57] Ver: https://www.pwc.com/m1/en/publications/a-practical-method-of-identifying-cyberattacks.html

[58] Ver: https://blog.trendmicro.com/graffiti-in-the-digital-world-how-hacktivists-use-defacement/

[59] Ver: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/web-defacements-exploring-the-methods-of-hacktivists

Además de la desfiguración, los hacktivistas siguen activos en la divulgación de información confidencial recabada en los sitios web atacados, así como desarrollando acciones DDoS. De hecho, el hacktivismo ha sido el segundo motivo en lo relativo al uso de vectores de ataque relacionados con DDoS[60].

1.8. Actores internos

Este grupo, al que suele denominarse *insiders*, está formado por personas maliciosas y/o negligentes, que pueden ser meros usuarios de los sistemas de información, usuarios privilegiados e, incluso, proveedores o contratistas de productos o servicios. Según los informes analizados en 2018, este grupo es también una importante fuente de compromiso en el panorama de las amenazas[61].

Las estadísticas muestran que alrededor del 25% de los incidentes en entornos corporativos se atribuyen a *insiders*[62], aunque las empresas siguen percibiendo este tipo de amenaza como una de las más altas, de suerte tal que un 64% de las organizaciones dice estar invirtiendo en medidas de disuasión frente a personas con información privilegiada[63] que, efectivamente, constituye la segunda fuente de incidentes[64].

Aunque la monetización deliberada es el principal motivo de este grupo de actores, la mayor parte del daño parece ser causado por acciones no intencionadas de los empleados[65]: como la divulgación accidental de datos (por ejemplo, el uso de direcciones de correo electrónico incorrectas), fallos en el reconocimiento de ataques de phishing o errores debidos a una configuración errónea[66].

Finalmente, hay que señalar que las amenazas internas pueden materializarse también de forma indirecta, con ataques a la cadena de suministro[67].

---

[60] Ver: https://www.netscout.com/report/

[61] Véanse: https://www.trustwave.com/Resources/Library/Documents/2018-Trustwave-Global-Security-Report/ , http://www.isaca.org/chapters1/puget-sound/education/Documents/2018%20Emerging%20Trends%20in%20Cybersecurity%20-%20EY%20ISACA%20Presentation%20-%2020MAR.pdf y https://isaca.nl/images/Presentatie_Raef_Meeuwisse_19-4-2018.pdf

[62] Ver: http://www.isaca.org/chapters1/puget-sound/education/Documents/2018%20Emerging%20Trends%20in%20Cybersecurity%20-%20EY%20ISACA%20Presentation%20-%2020MAR.pdf

[63] Ver: https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf

[64] Ver: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

[65] Ver: https://www.doxnet.com/2018/04/insider-use-and-abuse-identifying-internal-threats-and-how-to-mitigate-them/

[66] Ver: https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2017

[67] Ver: https://www.ncsc.gov.uk/guidance/example-supply-chain-attacks y https://www.wired.com/story/supply-chain-hacks-cybersecurity-worst-case-scenario/

6. VULNERABILIDADES

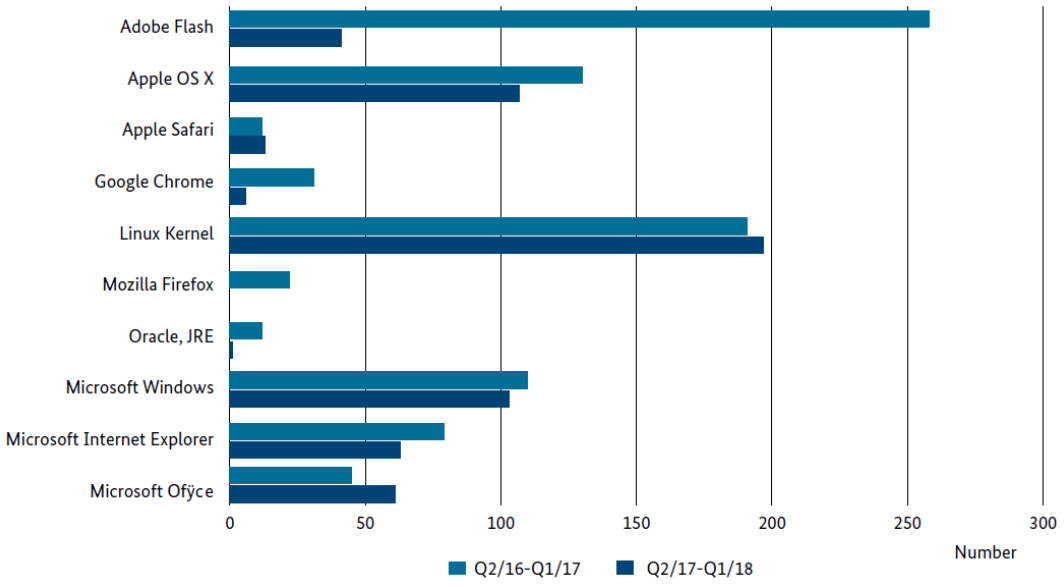
Se desarrollan seguidamente las vulnerabilidades más significativas de 2018.

1.9. Vulnerabilidades en el software y en el hardware

Durante 2018 el número de vulnerabilidades conocidas en los productos de software ha sido alto y no hay indicios de que esta situación cambie en los próximos años. Esto también se aplica a productos combinados hardware-software. Si bien las herramientas de desarrollo de software (compiladores, IDE, analizadores de código fuente) han mejorado notablemente y pueden alertar a los desarrolladores sobre elementos de riesgo, son claras ciertas tendencias en el software que afectan a la seguridad del producto final, a saber:

- Mayor complejidad de las aplicaciones de usuario final.
- Agrupación de componentes software, parcialmente actualizados.
- Integración incontrolada de elementos de origen externo.
- Optimizaciones de velocidad a expensas de la seguridad.
- Abandono de la resolución de problemas con referencia a medidas de mitigación
- Rechazo de actualizaciones de seguridad por parte de muchos fabricantes.

La figura siguiente muestra las CVE críticas del software más utilizado en el periodo que se muestra.



Parece claro que, en el momento de la adquisición de un producto software o un producto combinado software/hardware, casi siempre es imposible hacer una declaración cualificada sobre la seguridad o la cantidad de vulnerabilidades presentes en dicho producto, antes de materializar la compra y, a menudo, también después.

En 2018 se evidenció que el kernel de Linux parece tener un número de vulnerabilidades significativo, habiéndose encontrado muchas de ellas en módulos de controladores que también se utilizan en los smartphones Android. A diferencia de Windows, estas vulnerabilidades se incorporan al kernel de Linux puesto que están parcheadas al mismo tiempo. Con Windows, el fabricante del controlador está obligado a publicar las actualizaciones necesarias que también deben instalarse individualmente de forma manual por parte del usuario.

Como en años anteriores, las **actualizaciones** de seguridad en los entornos operativos sufrieron importantes retrasos (o no se implementaron). Esta realidad también aparece en sectores donde la vida humana depende, directa o indirectamente, del producto software en cuestión (sistemas de seguridad, dispositivos médicos, etc.) o en procesos industriales en los que los errores durante las actualizaciones generan altos costes.

Por otro lado, muchos dispositivos se utilizan durante tanto tiempo que el fabricante deja de ofrecer soporte en un momento dado. Aún más graves son los casos en los que el fabricante ya no está activo en el mercado, no se puede identificar o se niega a prestar asistencia. Además, pueden aparecer problemas adicionales cuando las actualizaciones no pueden instalarse en el sistema operativo porque otro software dependiente de él ya no funcionará correctamente.

***Spectre* y *Meltdown* – problemas en las arquitecturas hardware**

A principios de 2018 se conoció una nueva clase de ataques contra ciertas arquitecturas de CPU. Las vulnerabilidades conocidas por los nombres de *Meltdown* y *Spectre* fueron novedosas porque combinaron las propiedades arquitectónicas de las CPU modernas para leer áreas protegidas de memoria. Casi todas las de los fabricantes Intel, AMD y ARM se han visto afectadas.

Las vulnerabilidades explotan características del hardware que se han venido incorporando a los procesadores desde mediados de los años noventa, siendo su objetivo principal aumentar el rendimiento y minimizar el gasto asociado de recursos, tales como la ejecución de comandos o la ejecución arbitraria de código.

Dependiendo de la vulnerabilidad explotada, un atacante podría superar los mecanismos de seguridad provistos por el sistema operativo y/o el hardware, y leer los datos. Si los problemas ocurren en sistemas basados en hardware, las medidas de mitigación necesarias son, frecuentemente, muy costosas.

Sea como fuere, debido a sus profundas raíces estructurales, esta clase de problema persistirá. Por el momento, no está claro qué

La falta de voluntad de los fabricantes para proporcionar información sobre el estado de seguridad de sus productos -y mantenerla actualizada, al menos durante el período de garantía-, contribuye a sufrir una situación de seguridad precaria. Con carácter general, los compradores carecen de los recursos económicos, el tiempo o la experiencia para evaluar la seguridad IT de un producto, confiando en las declaraciones del fabricante o en las pruebas de terceros. Frecuentemente, las manifestaciones del fabricante sobre la seguridad IT de los productos SoHo (Small Office – Home Office), suelen estar incompletas[68].

cambios adoptarán los fabricantes de CPU para eliminar estas vulnerabilidades. El hardware recién adquirido seguirá siendo vulnerable.

Los procesadores modernos son muy complejos, y muchos mecanismos internos son considerados secretos por el fabricante. Esta realidad tiene como resultado que no es posible confiar plenamente en estos componentes, siendo muy difícil estimar el riesgo futuro.

Hasta que los fabricantes de hardware proporcionen o fabriquen soluciones adecuadas y suficientemente transparentes, los efectos en los sistemas instalados pueden mitigarse o eliminarse en parte en base a cambios de software, lo que se logra instalando rápidamente los parches disponibles para el firmware, el microcódigo, el sistema operativo y los programas de aplicación.

De todo ello debe extraerse una conclusión: un producto que contiene vulnerabilidades conocidas en el momento de la compra debe considerarse defectuoso -desde la perspectiva de seguridad IT- si las vulnerabilidades no se identifican expresamente o si no hay disponible una actualización de seguridad. Lo mismo se aplica a las vulnerabilidades que se conocen durante el período de garantía del producto. El mantenimiento del software por parte del fabricante, incluida la eliminación de vulnerabilidades, no solo debe ser el procedimiento habitual y el mecanismo para satisfacer la normativa legal aplicable, sino que también debe ser solicitado por el consumidor, como parte del servicio.

[68] Esto es aplicable, particularmente, como señala la BSI alemana, a la creación de actualizaciones de seguridad y no solo a las declaraciones sobre las vulnerabilidades actuales del producto o la existencia de debilidades públicamente conocidas. Las pruebas de productos de terceros, frecuentemente, se centran en la funcionalidad y no en la seguridad del producto. No hay una descripción general de la actualización real y la situación de la seguridad para todos los dispositivos relevantes para el mercado de una determinada clase de dispositivo (por ejemplo, teléfonos inteligentes, reproductores, etc.). Por lo tanto, los clientes no tienen una forma realista de usar la seguridad del producto como criterio para una decisión de compra, lo que significa que los fabricantes con productos más seguros no tienen ventajas en el mercado.

Características específicas de Mozilla Firefox y Google Chrome. Se han observado anomalías en los dos productos de software: Mozilla Firefox y Google Chrome. Desde octubre de 2016, Mozilla no parece haber mantenido ninguna entrada en la base de datos de MITRE CVE para Firefox. Las entradas de CVE están referenciadas en sus propias publicaciones (Avisos de seguridad de la Fundación Mozilla), pero no se anotan en la base de datos pública. No se proporciona una descripción de la vulnerabilidad, ni se hace referencia alguna al navegador Firefox como producto afectado. No hay evaluación de la vulnerabilidad o una puntuación de base. Google parece haber estado procediendo de manera similar con su navegador Chrome desde finales de octubre de 2017 y tampoco ha mantenido las entradas en la base de datos de CVE, aunque todavía proporciona números de CVE como lo hizo anteriormente en las actualizaciones de lanzamiento de Chrome. Sin embargo, las entradas correspondientes en la base de datos de MITRE CVE están vacías. Google tampoco proporciona una descripción de las vulnerabilidades, ni se refiere al navegador Chrome como el producto afectado. La evaluación de la vulnerabilidad y una puntuación de base también están ausentes. Además, es sorprendente que las entradas de CVE mantenidas para Google Chrome durante el período analizado estén calificadas casi exclusivamente con una puntuación base de CVSS v2.0 de 6,8 por ciento. Por lo tanto, las vulnerabilidades informadas no parecen ser vulnerabilidades críticas, que son aquellas que se basan en una puntuación base CVSS v2.0 de 7.0 o superior.	**Capacidad de actualización de los teléfonos inteligentes** Los teléfonos inteligentes con vulnerabilidades públicamente conocidas se venden como nuevos sin disponer de las actualizaciones de seguridad adecuadas, lo que da como resultado que, en muchas ocasiones, los usuarios deben arrostrar graves problemas de seguridad. Un ejemplo son los agujeros de seguridad "Stagefright" en el marco multimedia del mismo nombre en el sistema operativo Android de Google, que salió a la luz en julio de 2015. Es prácticamente imposible para los consumidores comprobar si el software está actualizado y si hay cualquier opción de actualización. Es necesaria, por tanto, una información transparente para tomar una decisión de compra informada, que, frecuentemente, los proveedores no ofrecen. Por ejemplo, después de que la BSI alemana encontrara agujeros de seguridad en un teléfono inteligente, la Asociación de Consumidores de Renania del Norte-Westfalia utilizó su representación asociativa para emprender acciones legales, presentando una demanda contra el vendedor del dispositivo afectado, basada en una información insuficiente al consumidor. La acción legal sigue en curso y el acuerdo de coalición entre la CDU, la CSU y la SPD pretende que la protección del consumidor se establezca como una tarea adicional entre las competencias de la BSI alemana.

Vulnerabilidades en implementaciones de OpenPGP y S/MIME

Investigadores de seguridad de la Universidad de Ciencias Aplicadas de Münster, Ruhr University Bochum y KU Leuven (Bélgica) encontraron serios puntos débiles en la implementación de los estándares de cifrado de correo electrónico OpenPGP y S/MIME, que publicaron el 14 de mayo de 2018 en https://efail.de/ En base a tales vulnerabilidades, los atacantes podrían manipular correos electrónicos cifrados de tal manera que el contenido del mensaje se reenvíe en texto plano después de ser descifrado por el destinatario.

Para explotar las vulnerabilidades, el atacante debe tener acceso a la ruta de transporte, el servidor de correo o el buzón del destinatario. Además, debe permitirse el contenido activo en el lado del destinatario, como la ejecución de código HTML y, en particular, la descarga posterior de contenido externo. Esta es actualmente la configuración predeterminada, especialmente, en dispositivos móviles.

Los estándares de cifrado de correo electrónico mencionados pueden, en opinión de la alemana BSI, seguir utilizándose de forma segura si se implementan y configuran correctamente. La mayoría de los proveedores de clientes de correo electrónico ya han tomado medidas contra la vulnerabilidad, así como contra la extracción directa de datos -es decir, sin cifrado-, en sus productos.

Los fabricantes explican en los siguientes sitios web cómo los usuarios de programas de correo electrónico más habituales pueden evitar que el contenido remoto se vuelva a cargar:

- Microsoft Outlook - Block automatic picture downloads in e-mail messages
  https://support.office.com/en-us/article/block-or-unblock-automatic-picture-downloads-in-email-messages-15e08854-6808-49b1-9a0a-50b81f2d617a?ui=en-US&rs=en-US&ad=US
- Mozilla Thunderbird - Block remote content in messages
  https://support.mozilla.org/en-US/kb/remote-content-in-messages
- Apple Mail - Show or hide remote images
  https://support.apple.com/kb/PH4873?locale=en_US

Independientemente de las vulnerabilidades encontradas, el tipo de conexión es importante en el contexto de la comunicación con el proveedor de servicios de correo electrónico. Por ejemplo, si se utiliza IMAP, los datos se sincronizan entre el servidor y el cliente en el dispositivo móvil.

La peculiaridad de Cisco Smart Install

Cisco Smart Install (SMI) es una función de configuración automática para los conmutadores de red de Cisco, instalada en los dispositivos nuevos, de forma predeterminada. SMI no proporciona protección de acceso; no se requiere autenticación y, por lo tanto, el acceso a SMI solo debe permitirse desde redes confiables y nunca abiertamente desde Internet.

En agosto de 2017 se evidenció que ciertos actores se habían valido de esta peculiaridad para atacar a varias organizaciones australianas, leyendo los archivos de configuración de dispositivos (https://acsc.gov.au/news/routers-targeted.html). En noviembre, se

descubrieron cientos de otros archivos de configuración que, según informes de prensa, los atacantes habían extraído anteriormente en los dispositivos afectados de todo el mundo.

A principios de abril de 2018, los atacantes utilizaron esta misma peculiaridad del SMI para comprometer a miles de conmutadores de Cisco en diferentes países. En Rusia e Irán, los agentes de las amenazas dejaron sin servicio los dispositivos afectados, lo que provocó que grandes áreas de las redes de estos países quedaran desconectadas de Internet durante varias horas.

Desde entonces, el número de dispositivos afectados ha disminuido considerablemente.

1.10. Nuevas formas de explotación

Aunque, a finales de 2017 y principios de 2018, se pusieron de manifiesto una serie de vulnerabilidades técnicas de gran peligrosidad, no han derivado en explotaciones significativas, debido, fundamentalmente -como ha señalado el CSAN holandés[69]-, a que las técnicas de ataque requeridas eran muy complejas o requerían de especiales condiciones adicionales, tales como la cercanía física del objetivo.

En julio de 2017 se detectó una vulnerabilidad -conocida como ***Broadpwn***- en los chips Wi-Fi de Broadcom que utilizan los teléfonos y otros equipos de fabricantes como Samsung, Google y Apple; en virtud del cual un agente podría obtener el control del dispositivo, ejecutar el código en el chip Wi-Fi y obtener acceso al tráfico inalámbrico de datos[70]. Sin embargo, explotar esta vulnerabilidad requería que el atacante estuviera físicamente próximo a la víctima. Las vulnerabilidades afectaron a Apple y Google, y se resolvieron de manera coordinada en las nuevas versiones de sus sistemas operativos iOS y Android, respectivamente.

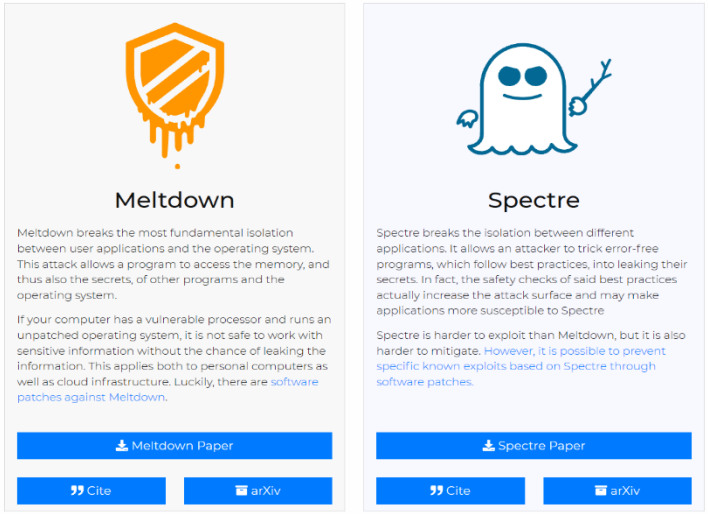
En octubre de 2017, investigadores de la Universidad Católica de Lovaina publicaron un informe sobre ciertas técnicas de ataque que hacían vulnerables a los dispositivos que usan Wi-Fi con cifrado WPA o WPA2: el llamado ataque ***Krack***[71]. Como quiera que el éxito del ataque exige que el agente de la amenaza ha de estar físicamente cerca de la red Wi-Fi que desea atacar, las técnicas de agresión son difíciles de usar de manera eficiente a gran escala.

[69] Cyber security Assessment Netherlands, 2018.

[70] Véase: Exodus Intelligence: Broadpwn: Remotely Compromising Android and iOS via a Bug in Broadcom's Wi-Fi Chipsets (en http://blog.exodusintel.com/2017/07/26/broadpwn/)

[71] Véase: Key Reinstallation Attacks - Breaking WPA2 by forcing nonce reuse (en https://www.krackattacks.com/). Hay un video explicativo en https://youtu.be/Oh4WURZoR98

Como se ha dicho, en enero de 2018, equipos de investigación revelaron dos nuevas familias de vulnerabilidades hardware (denominadas *Spectre* y *Meltdown)* que permitirían a los atacantes obtener información confidencial ejecutando el código del programa en el ordenador de la víctima[72].



En mayo de 2018, se descubrió una nueva vulnerabilidad con un efecto similar al de ***Spectre***. A mediados de noviembre de 2018, un equipo de investigadores descubrió siete nuevos ataques de bajo impacto a los procesadores. Dos de ellos fueron variaciones del ataque *Meltdown*, y los cinco restantes, variaciones de *Spectre*[73].

En marzo de 2018, investigadores de la empresa de seguridad CTS Labs publicaron en un sitio web un estudio en relación con 13 puertas traseras y vulnerabilidades graves que, según afirmaron, habían descubierto en los procesadores de **AMD** (entidad que fue informada de las brechas tan solo 24 horas antes de hacerse públicas), conocidas como *AMDflaws*[74]. Aunque los medios de comunicación manifestaron dudas sobre la verosimilitud de la información, AMD confirmó que los problemas existían y estaban trabajando en los correspondientes parches, aunque -así lo afirmaron-, dichas vulnerabilidades suponían un riesgo limitado porque solo podían explotarse si un atacante ya había comprometido el sistema y había alcanzado privilegios de administrador[75].

Finalmente, en mayo de 2018, investigadores de la Universidad Libre de Ámsterdam revelaron la vulnerabilidad ***GLitch***, una nueva forma de perpetrar lo que se conoce como ataques de *Rowhammer* a través del procesador gráfico de un ordenador[76].

En otro orden de cosas, como se ha señalado, una buena parte de las fugas de datos son resultado de deficiencias en la configuración de los sistemas y en la ausencia

[72] Véase: Meltdown and Spectre: Vulnerabilities in modern computers leak passwords and sensitive data (en https://meltdownattack.com/)
[73] Fuente: PandaLabs Annual Report 2018.
[74] Véase: CTS: Amdflaws (en http://cts-labs.com/)
[75] Véase https://blog.trailofbits.com/2018/03/15/amd-flaws-technical-summary/
[76] Véase VUSec: GLITCH (en https://www.vusec.net/projects/glitch/)

de medidas de seguridad adecuadas. Los datos obtenidos de tales fugas -especialmente, cuando son personales o sensibles- pueden utilizarse para desarrollar campañas de phishing dirigidas a la sustracción de credenciales o identidades, siendo muy difícil establecer a priori su impacto.

En septiembre de 2017, la agencia de calificación crediticia **Equifax** anunció una fuga de datos que involucró a 143 millones de norteamericanos. En octubre de 2017 y marzo de 2018, Equifax informó que los atacantes habían sustraído los datos de otros 4,9 millones de norteamericanos[77], explotando una vulnerabilidad de Apache Struts, y que, pese a la emisión del parche, fue explotada con enorme rapidez. El coste del ataque representó para Equifax 87,5 millones de dólares[78].

Más ejemplos:

- En noviembre de 2017, se reveló que **Uber** había ocultado un ataque ocurrido en 2016 a su aplicación, en el que se habían hecho públicos datos de 57 millones de personas[79]. En diciembre se anunció que los datos de aproximadamente 174.000 pasajeros y conductores de Uber habían sido sustraídos, a raíz -según parece- de que Uber colocara en GitHub las claves que brindan acceso a la nube de Amazon y que contenía toda la información personal de los pasajeros y conductores. Esta circunstancia fue notificada a la empresa por parte de su descubridor, que recibió 100.000 dólares a condición de que firmara un acuerdo en el que se comprometiera a borrar todos los datos. La compañía decidió finalmente no informar públicamente de esta fuga porque -según afirmaron-, así estaba contemplado en su Programa de Divulgación de Vulnerabilidades[80].
- En el mismo mes, se reveló que, como resultado de una fuga de datos, el consumo de **energía de los hogares holandeses** se podía obtener por

[77] Véanse:
Bloomberg: Equifax Says 2.5 Million More Americans May Be Affected by Hack (en https://www.bloomberg.com/news/articles/2017-10-02/urgent-equifax-2-5-million-more-americans-may-be-affected-by-hack) y
Equifax: Equifax Releases Updated Information on 2017 Cybersecurity Incident (en https://investor.equifax.com/news-and-events/news/2018/03-01-2018-140531340)

[78] Véase: Equifax: Equifax Releases Third Quarter Results (en https://investor.equifax.com/news-and-events/news/2017/11-09-2017-211550295)

[79] Véase https://www.nu.nl/internet/5017448/uber-verzweeg-datalek-van-57-miljoen-accounts.html

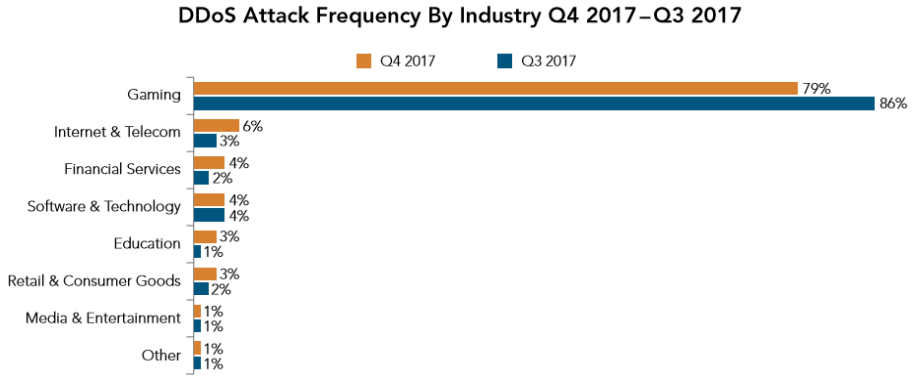
[80] Véase: Reuters: Exclusive: Uber paid 20-year-old Florida man to keep data breach secret – sources (en https://www.reuters.com/article/us-uber-cyber-payment-exclusive/exclusive-uber-paid-20-year-old-florida-man-to-keep-databreach-secret-sources-idUSKBN1E101C). Finalmente, los abogados involucrados en ocultar el hecho fueron despedidos cuando el incidente se hizo público y muchas personas expresaron preocupación al respecto.

código postal y número de edificio en el sitio web de un proveedor de energía[81].

- En febrero de 2018, la empresa de seguridad alemana Kromtech descubrió un repositorio de **Amazon S3** (un tipo de servidor de almacenamiento en la nube) configurado incorrectamente[82]. Dicho servidor contenía más de 119.000 documentos escaneados, incluidos documentos de identidad. La brecha se resolvió el día siguiente. Sin embargo, en abril de 2018, se reveló que los documentos de identidad escaneados y los detalles de la dirección postal de 3.000 ciudadanos holandeses se encontraban entre ellos, incluyendo documentos de identidad de los empleados del Ministerio de Defensa.

1.11. Ataques DDoS a través de sistemas públicamente accesibles

Mientras que el primer tercio del año 2017 fue especialmente pródigo en ataques DDoS, durante el último trimestre, la frecuencia de este tipo de acciones se moderó[83], salvo en la industria del videojuego.



Si bien 2017 fue testigo del uso masivo de dispositivos IoT como elementos facilitadores de ataques DDoS, 2018 ha dejado claro que con otros tipos de dispositivos también pueden desarrollarse tales acciones, muy especialmente si los equipos involucrados no son seguros o no están protegidos adecuadamente.

---

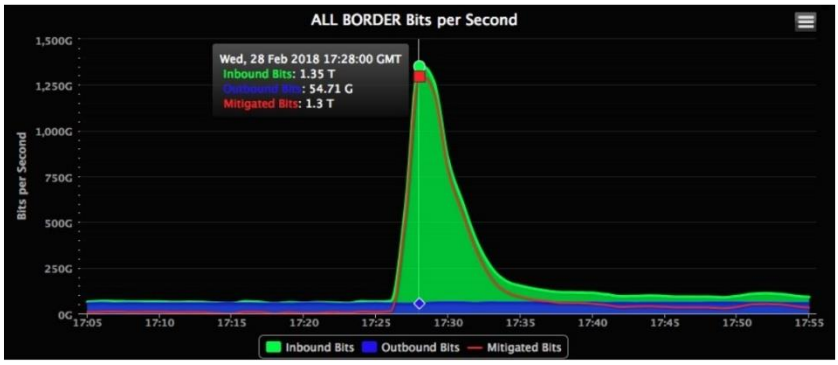
[81] Véase https://www.nu.nl/internet/4989794/energieverbruik-alle-nederlandse-huishoudens-was-in-zien-datalek.html

[82] Véase: Kromtec: FedEx Customer Records Exposed (en https://kromtech.com/blog/security-center/fedex-customer-records-exposed)

[83] Véanse: Fuente: Akamai.
https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/q2-2017-state-of-the-internet-securityreport.pdf
https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/q3-2017-state-of-the-internet-security-report.pdf
https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf

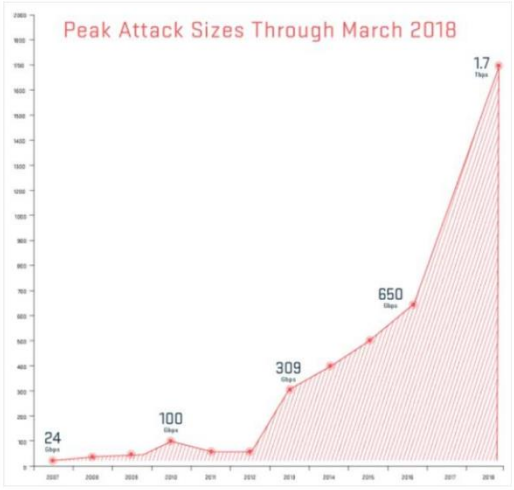
Así, a partir de febrero de 2018, se evidenció en las acciones DDoS el uso de los llamados ataques "*Memcached*", a través de sistemas accesibles al público[84]. Como es sabido, los sistemas *Memcached* están diseñados para almacenar temporalmente pequeñas cantidades de datos de otras fuentes tales como bases de datos y APIs, para hacer que los sitios web sean más rápidos. Los sistemas no requieren autenticación para las comunicaciones y no han sido desarrollados para ser de acceso público, posibilitando por tanto ataques por amplificación.

Según la compañía Panda, el 28 de febrero de 2018 tuvo lugar el ataque DDoS más potente de la historia: 1,35 terabits por segundo de tráfico dirigido a GitHub, la plataforma web de proyectos de desarrollo colaborativos[85].



Real-time traffic from the DDoS attack. AKAMAI

Unos días más tarde, se superó el record con un ataque con picos de tráfico de 1,7 Tbps[86].



[84] Véase: Panda: Memcached, el ataque DDoS de moda, (en https://www.pandasecurity.com/spain/mediacenter/seguridad/memcached-ataque-ddos/)

[85] Fuente: Wired: GitHub Survived the Biggest DDoS Attack Ever Recorded (en https://www.wired.com/story/github-ddos-memcached/)

[86] Fuente: The Register: World's biggest DDoS attack record broken after just five days (en https://www.theregister.co.uk/2018/03/05/worlds_biggest_ddos_attack_record_broken_after_just_five_days/)

En estas acciones, el atacante envía lo que simula ser una solicitud en nombre del objetivo, falsificando su dirección IP. Puesto que las respuestas son más largas que la solicitud, el actor puede usar un ancho de banda relativamente pequeño para configurar un ataque mayor.

Un sistema de acceso público con un factor de amplificación muy alto, tal como un sistema *Memcached* no protegido, representa para los atacantes una herramienta muy atractiva[87].

Los ataques DDoS se están volviendo cada vez más complejos, incrementándose los tipos de origen, que podrían ubicarse en cualquier parte del mundo, pudiendo atacar simultáneamente múltiples objetivos. Como hemos dicho, algunos ejemplos son los dispositivos IoT inseguros, los sistemas *Memcached* abiertos (sin protección) o los *Booter Sites*, lugares donde pueden adquirirse servicios de ataque DDoS, a muy bajo coste[88].

La figura muestra un cuadro con algunos precios de estas herramientas de ataque[89].

[87] Comentario de Panda, en relación con los ataques Memcached: Alrededor de 100.000 servidores *Memcached* están expuestos sin ninguna protección de autenticación. Esto quiere decir que un ciberdelincuente puede acceder a ellos y enviarles grandes volúmenes de datos con el fin de saturar los servidores y maximizar sus índices de respuesta. El resultado: el sistema responde devolviendo miles de veces los datos de las solicitudes a la víctima. Con grandes cantidades de datos enviados – en torno a 10 paquetes de datos por segundo – el servidor *Memcached* amplifica considerablemente el volumen de datos que pueden enviarse contra un objetivo. Por eso, si el sistema carece de un filtro adecuado que permita una gestión eficaz de la red, la oleada de datos puede ser más que suficiente para dejar fuera de servicio a algunos proveedores de Internet.

[88] Fuente: Armors: THE BLACK MARKET REPORT (en https://cdn.armor.com/app/uploads/2018/03/27222933/2018-Q1-Reports-BlackMarket-DIGITAL-min.pdf)

[89] Fuente: The Black Market Report: a look inside the dark web (Marz., 2018)

HACKING TOOLS & SERVICES	
Account Hacking Program	$12.99 (See more details on page 10)
Hacked Instagram Accounts in Bulk	1,000 - 10,000 accounts $15 - $60
Botnet: Blow-Bot Banking Botnet	Monthly Basic Rental $750 | Monthly Full Rental $1,200 | Monthly Support $150
Disdain Exploit Kit	Day $80, Week $500, Month $1,400
Stegano Exploit Kit: Chrome , FireFox, Internet Explorer, Opera, Edge	Unlimited Traffic, Day $2,000 Unlimited Traffic, Month $15,000
Microsoft Office Exploit Builder	Lite exploit builder $650 Full Version $1,000
WordPress Exploit	$100
Password Stealer	$50
Android Malware Loader	$1,500
Western Union Hacking Bug For World Wide Transfer	$300
DDoS Attacks	Week long attack $500 - $1,200
ATM Skimmers: Wincor, Slimm, NCR, Diebold	$700 - $1,500
Hacking Tutorials	Multiple Tutorials $5 - $50

1.12. La seguridad de los dispositivos médicos y sanitarios

Cada vez es mayor el desarrollo de dispositivos médicos y sanitarios que se conectan a Internet. Estos productos tienen diferentes tipos de interfaces que permiten su integración en las redes informáticas, pudiendo vincularse, en ocasiones, a aplicaciones móviles, para gestionar los datos personales de los pacientes. Las tecnologías inalámbricas hacen que sea mucho más fácil para los facultativos acceder a los datos del paciente y comunicarse con el sistema. Dispositivos médicos que se implantan, tales como marcapasos, desfibriladores ICD, neuro-estimuladores e implantes cocleares presentan claras ventajas sobre los sistemas anteriores, toda vez que la comunicación inalámbrica hace innecesaria una intervención quirúrgica para, por ejemplo, ajustar los parámetros del dispositivo.

Lógicamente, estos equipos tienen importantes exigencias de seguridad, ya que, normalmente, tienen una vida útil relativamente larga o han de alojarse durante un tiempo significativo en el cuerpo del paciente, desempeñando en ocasiones funciones de vital importancia. Por lo tanto, es imprescindible identificar y evaluar posibles amenazas en una etapa temprana que permita el desarrollo de las contramedidas adecuadas para garantizar la seguridad durante la vida del equipo.

Varias pruebas en laboratorio, realizadas en los Estados Unidos, han demostrado que una porción de dispositivos médicos (marcapasos, desfibriladores, respiradores, bombas de infusión) son vulnerables a ciberataques. Por ejemplo, un desfibrilador se pudo controlar y reprogramar de forma remota para liberar electricidad no deseada. En consecuencia, la ciberseguridad debe ser integrada e implementada desde el principio del desarrollo y la fabricación de estos dispositivos ("seguridad por diseño" y "seguridad por defecto"), con el fin de garantizar su uso durante un período tan largo como sea posible.

A menudo, los mecanismos de autenticación en dispositivos médicos digitales no están suficientemente protegidos y/o las técnicas de cifrado de datos para la comunicación y el almacenamiento son débiles o, incluso, inexistentes. En estas circunstancias, sería posible obtener acceso no autorizado y manipular el dispositivo sin el conocimiento del paciente[90].

1.13. La seguridad del mobile-banking

Aunque hay una gran variedad de servicios de pago para comercios y consumidores (Paypal, 3D-Secure, Giropay, iDeal, etc.), los pagos por Internet ya no se limitan a los ordenadores personales, sino que, cada vez con más frecuencia, se llevan a cabo usando dispositivos móviles (smartphones o tabletas), lo que alienta a las entidades financieras a ofrecer apps de banca on-line para estos dispositivos, incluso aplicaciones que permiten la administración de cuentas de diferentes entidades. Tales aplicaciones bancarias se complementan con una segunda aplicación, conocida como "aplicación TAN" que genera un número (TAN) para asegurar la transacción ejecutada en la app bancaria.

[90] Sin embargo, para dar a los médicos el acceso más rápido posible en caso de emergencia a dispositivos tales como los desfibriladores implantados, los mecanismos de seguridad han mostrado un perfil deliberadamente bajo. La utilización de procedimientos de acceso más seguros consumirían un tiempo mayor y cualquier demora podría ser perjudicial para el paciente. Además, siguiendo con el ejemplo de los desfibriladores implantables, puede ser problemático implementar características de seguridad más fuertes. Estos desfibriladores tienen el tamaño de una caja de cerillas y funcionan con baterías con una carga útil entre cuatro y seis años, por lo que los pacientes con ICD tienen que someterse a intervenciones quirúrgicas regulares para la sustitución de la batería. Si se utilizara más espacio de almacenamiento o mejores técnicas de cifrado, sería a expensas del tamaño del desfibrilador y la duración de la batería, por lo que el tiempo de permanencia del dispositivo se acortaría, requiriendo cirugías adicionales, con lo que nos encontramos ante una solución de compromiso entre la funcionalidad del dispositivo y su seguridad.

El método de inicio de sesión en una aplicación y el tipo de seguridad de la transacción son determinantes. Por razones de comodidad, suele utilizarse un único dispositivo en el que se ejecutan la aplicación bancaria y la aplicación que genera el TAN, lo que constituye un riesgo significativo si el dispositivo se ve comprometido, porque el atacante podría obtener el control de ambas aplicaciones.

Todo ello deriva en el enorme tráfico ilegal actual de credenciales. El cuadro de la derecha muestra una tabla con los precios en el mercado negro de credenciales bancarias sustraídas[91].

BANKING & ONLINE PAYMENT ACCOUNTS CREDENTIALS	
ACCOUNTS (U.S.) BANK OF AMERICA, JPMORGAN CHASE, WELLS FARGO...	
Balance $2,000 - $5,000	$100 - $400
Balance $12,000 - $15,000	$600 - $1,000
Balance $20,000 +	$1,000 +
ACCOUNTS (UK) LLOYDS BANK, BARCLAYS, HSBC...	
Balance 3,000 - 6,000 GBP	$150-$600
Balance 10,000 - 16,000 GBP	$600 - $1,000
Balance 20,000 GBP +	$800-$1,500
ATM CARDS WITH BALANCES AND PIN	
Balance $2,000 - $8,000	$100-$500
LARGE U.S. ONLINE PAYMENT ACCOUNT CREDENTIALS	
Verified Balance $1,500 - $5,000	$100 - $450

1.14. Domótica e Internet of Things (IoT)

Como es sabido, el Internet de las Cosas (IoT) permite la conexión de múltiples elementos entre sí y con las personas, usando un hardware cada vez más asequible, con un menor consumo y, en consecuencia, una mayor duración de la batería. Las áreas de aplicación más frecuentes de los dispositivos IoT son los electrodomésticos, la vigilancia del hogar (videovigilancia y audiovigilancia) y la gestión de la salud (los werarables, por ejemplo).

Esta realidad ha provocado el crecimiento de nuevas soluciones IoT en las que el usuario busca la funcionalidad, idoneidad y precio, relegando la seguridad a un segundo plano.

Sin embargo, frecuentes informes en torno a incidentes asociados a estos dispositivos han contribuido a concienciar a los consumidores de los riesgos que plantea su uso, lo que ha provocado que muchos protocolos utilizados actualmente en IoT ofrezcan funciones de seguridad mejoradas y una respuesta más rápida a las vulnerabilidades del dispositivo.

Pese a todo, sin embargo, la gran cantidad de dispositivos conectados a Internet que no están adecuadamente protegidos hace que sigan siendo un objetivo lucrativo

[91] Fuente: The Black Market Report: a look inside the dark web (Marz., 2018)

para los atacantes. Además de ser más fáciles de comprometer, la detección de incidentes en dispositivos IoT también es mucho más difícil. Frecuentemente, los propietarios de estos equipos infectados no perciben ninguna anomalía en el funcionamiento, pudiendo utilizarse para, por ejemplo, desarrollar botnets.

Interfaz OBD-II en vehículos.
La OBD-II (diagnóstico a bordo) es una interfaz que está disponible en todos los vehículos motorizados fabricados y registrados en Europa desde 2003. Proporciona acceso a los buses CAN que conectan todos los componentes electrónicos del vehículo. La función original de la interfaz fue monitorizar la regulación de las emisiones. Desde entonces, ha sido utilizado para inspecciones adicionales, por ejemplo, para diagnóstico de fallos en talleres, pudiéndose también utilizar para instalar adaptadores específicos (*dongles*), que se conectan a la interfaz OBD-II y, a través del teléfono móvil, envían datos de diagnóstico a las aseguradoras o a las compañías de alquiler de automóviles, por ejemplo.

Debido a su diseño, OBD-II no solo puede leer datos del vehículo, sino también importar comandos a la red interna. Sin embargo, los *dongles* no están sujetos a ninguna verificación de autorización ni ofrecen interfaces cubiertos por la responsabilidad del fabricante del vehículo, lo que genera riesgos adicionales. En 2015, los investigadores demostraron que podían enviar SMS manipulados a ciertos *dongles*, que influían en las funciones de frenado a baja velocidad. En 2017 se demostró que la conexión Bluetooth de un *dongle* podía ser atacada, lo que podía alterar las funciones de conducción.

En relación con los dispositivos IoT, caben dos escenarios de amenaza: en un primer escenario, el equipo se compromete para causar daños directos o indirectos al usuario, como los mostrados en el cuadro siguiente.

• Manipulación de datos: El atacante podría modificar el control de accesos para obtener acceso no autorizado a un edificio o causar daños al sistema de aire acondicionado.	• Espionaje de datos: Los dispositivos IoT pueden equiparse con varios sensores. Un dispositivo comprometido podría enviar datos al atacante, proporcionando acceso a información confidencial.
• Sabotaje de dispositivos IoT: El atacante podría dejar el dispositivo fuera de servicio o limitar sus funcionalidades.	• Uso de dispositivos IoT como puerta trasera: Los dispositivos IoT con medidas de seguridad inadecuadas podrían usarse como puertas traseras para obtener acceso a redes domésticas o corporativas.

En un segundo escenario de amenazas, el dispositivo IoT se compromete para ser utilizado como medio para atacar otros objetivos, por ejemplo, servicios web o infraestructuras de terceros. En estos casos, como el equipo no ve alterada su funcionalidad, el ataque suele pasar desapercibido. Algunos ejemplos son:

• Construcción de botnets: El secuestro masivo de dispositivos de IoT con deficiente seguridad permite la creación de grandes redes de bots que	• Ocultamiento de la identidad: Los dispositivos comprometidos pueden usarse como servidores proxy para ocultar nuevos ataques.

pueden propiciar ataques DDoS.	
• Minería de criptomonedas: Como hemos visto con anterioridad, es posible utilizar la potencia de cómputo colectivo de los dispositivos IoT comprometidos para la minería de criptomonedas. En este caso, el ataque es más fácil de detectar, porque se ralentiza el normal funcionamiento del equipo.	• Clic-Fraud con banners publicitarios: El atacante usa muchas direcciones IP diferentes de dispositivos IoT secuestrados para generar clics en banners publicitarios, videos o contenido de redes sociales. De esta manera, se puede obtener un beneficio económico con la facturación basada en clics. Además, el anunciante sufre daños directos a través del pago de una comisión por clics simulados.

Los posibles efectos de los ataques en los dispositivos de IoT son tan diversos como puedan serlo en los ordenadores convencionales: todas las dimensiones de la seguridad (confidencialidad, disponibilidad e integridad) pueden verse comprometidas.

1.15. Vulnerabilidades en chips

Los componentes que almacenan claves criptográficas o implementan algoritmos criptográficos son esenciales en las aplicaciones de seguridad más importantes, tales como la autenticación segura, la comunicación cifrada o las firmas electrónicas.

Mientras que los algoritmos utilizados pueden probarse e, incluso, verificarse matemáticamente, el almacenamiento seguro de la clave y, en particular, el procesamiento de claves sigue siendo un gran desafío, ya que, inevitablemente, surgen fenómenos físicos medibles que permiten extraer conclusiones sobre las claves. Con las generaciones de chips más antiguas, por ejemplo, el contenido de la ROM podía leerse simplemente con la ayuda de un microscopio digital, puesto que el almacenamiento de un "1" es ópticamente diferente de un "0". La medición del consumo de energía durante el proceso también podía utilizarse para atacar una clave, ya que el consumo de energía varía según las diferentes secuencias de bits. Si bien los elementos de seguridad actuales implementan numerosas medidas contra tales acciones, los resultados de las investigaciones evidencian que también las técnicas de ataque han mejorado. Por eso, aunque las acciones dañinas son relativamente fáciles de implementar, los ataques invasivos o las manipulaciones en el hardware mediante, por ejemplo, bombardeo con láser o incluso la modificación de los circuitos no son acciones generalizadas, debido al esfuerzo requerido para su acometimiento.

Las debilidades algorítmicas constituyen otro problema. Aunque los métodos utilizados hayan sido probados, a veces no se pueden implementar algoritmos criptográficos seguros debido a la limitada capacidad de almacenamiento y proceso de los elementos de seguridad.

Los recursos limitados implican que las operaciones criptográficas complejas deben acelerarse mediante funciones implementadas en hardware. Sin embargo, las operaciones muy complejas, tales como la generación de claves en RSA, siguen consumiendo mucho tiempo dependiendo de la longitud de la clave, puesto que los grandes números primos deben buscarse aleatoriamente. El uso de FastPrime, un algoritmo propietario para construir grandes números primos acelera la generación de claves. Sin embargo, se ha demostrado que las claves generadas de esta manera son criptográficamente más débiles de lo esperado.

Los procesos propietarios, aunque son considerablemente más rápidos, no están sujetos a pruebas y evaluaciones de seguridad. Una certificación de seguridad en línea con **Common Criteria**, por ejemplo, solo evalúa la implementación segura (resistencia al canal lateral) en el chip. No evalúa la fuerza matemática de un proceso criptográfico en sí.

La vulnerabilidad ROCA (ver epígrafe 7.14), revelada a finales de 2017 por un equipo de investigación, se refiere a un procedimiento de este tipo que se utilizó en una librería criptográfica de Infineon para tarjetas inteligentes, y que implicaba que la clave privada RSA podía reconstruirse a partir de la clave pública.
ROCA no es un problema nuevo. Es más bien el resultado de una generación de

Key Reinstallation AttaCK (KRACK) en vulnerabilidad WLAN

En octubre de 2017, el investigador de seguridad Mathy Vanhoef publicó un trabajo que describe un ataque a los protocolos de acceso protegido a Wi-Fi (WPA, WPA2) llamado Key Reinstallation AttaCK (KRACK). WPA2 es el actual estándar de seguridad para redes inalámbricas, que se integra en casi todos los dispositivos habilitados para WLAN. La vulnerabilidad subyacente es un fallo de diseño en el estándar IEEE 802.11i cuyas características de seguridad se han implementado en WPA2.

El actual estándar de seguridad IEEE 802.11i ha definido un procedimiento de negociación multinivel como un protocolo de autenticación de red que proporciona una mayor seguridad para configurar y usar redes WLAN. Los pasos del procedimiento de negociación consisten en una comunicación entre el cliente y el punto de acceso, en el contexto de la cual se calculan e intercambian importantes elementos criptográficos. El objetivo principal de este intercambio es que el cliente pueda autenticarse en el punto de acceso y garantizar un cifrado seguro. El procedimiento generará e instalará una clave de sesión común para ambas partes. Los datos se pueden cifrar con tal clave para garantizar su confidencialidad e integridad.

KRACK comienza en el punto posterior a la "instalación" de la clave de sesión. Una vez que el mensaje del punto de acceso a la clave de sesión ha sido enviado, el cliente instala la clave generada conjuntamente y confirma este paso al punto de acceso. Sin embargo, dado que los mensajes en la red podrían

claves RSA fundamentalmente compleja. Con la ayuda del ataque *Coppersmith*, un módulo RSA se puede factorizar de manera eficiente si se conocen los bits más altos de uno de los números primos. Este efecto se produce no solo debido a la forma en que se construyen los números primos con el algoritmo de *FastPrime*, sino también cuando se utilizan malos generadores de números aleatorios.

El problema de los números aleatorios pobres, por ejemplo, propició un ataque exitoso a algunas tarjetas de identificación taiwanesas en 2015.

eventualmente perderse, el punto de acceso envía nuevamente el mensaje si el cliente no confirma. En este caso, el cliente también puede reinstalar la clave de sesión. Al mismo tiempo, se reinician el número de paquete de transmisión incremental (conocido como *nonce*) y el contador de reproducción usado por el protocolo de confidencialidad de datos. Con KRACK, el atacante fuerza las repeticiones del mensaje desde el punto de acceso para iniciar el restablecimiento del *nonce*. De esta manera, se puede forzar un nuevo cifrado con la misma clave (porque depende de la fuente), a través del cual los paquetes de datos se pueden reproducir, descifrar y/o falsificar, por ejemplo, si el atacante está dentro del alcance de la red inalámbrica. El ataque funciona de manera similar con otros métodos de negociación WLAN (Peerkey, Group Key o Fast BSS Transition).

Por otro lado, el análisis de canales laterales (side channel) en el campo de los algoritmos simétricos (AES) y la criptografía asimétrica clásica (RSA) son un tema constante de investigación. Los elementos de seguridad más antiguos evidencian frecuentemente debilidades en la resistencia al side channel. Incluso si su seguridad ha sido originariamente certificada conforme a Common Criteria, dicha certificación es solo una instantánea del estado de la tecnología en ese momento. Esto significa que los ataques de canal lateral también representan una amenaza práctica para los elementos de seguridad certificados a medida que el hardware envejece. Por esta razón, la validez de los certificados de seguridad se limita, generalmente, a cinco años para las tarjetas con chip y productos similares. Para las aplicaciones relevantes de seguridad que deban estar operativas durante un período de tiempo más largo, deben usarse mecanismos de actualización para la implementación de los procedimientos criptográficos.

7. MÉTODOS Y OBJETIVOS DE ATAQUE

Este epígrafe describe los desarrollos en los métodos, procedimientos y herramientas que los actores de las amenazas han venido utilizando en el período considerado.

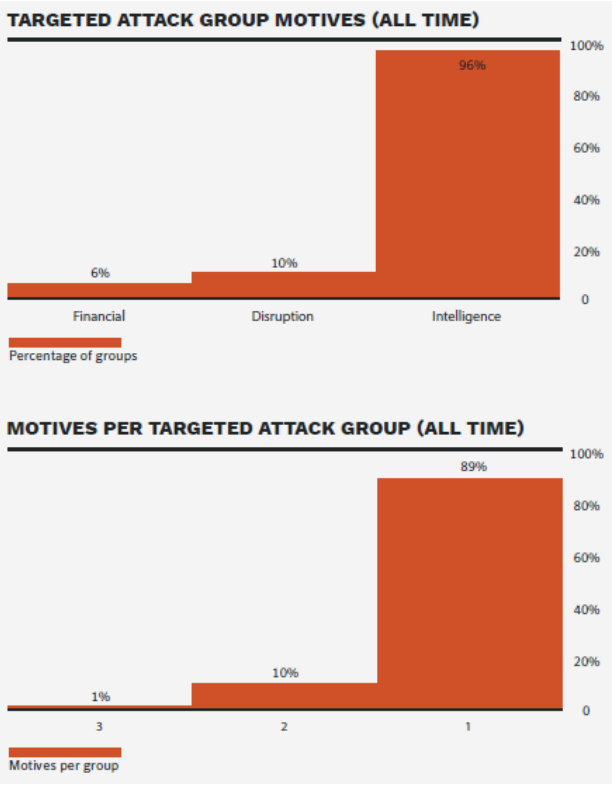
1.16. Amenazas Persistentes Avanzadas (APT)

Como es sabido, las Amenazas Persistentes Avanzadas (APT) son ciberataques dirigidos a instituciones y organizaciones concretas, persiguiendo obtener acceso a largo plazo a una red, exfiltrando información y propagando el ataque a otros sistemas. En comparación con otros vectores de ataque, las APT, generalmente, utilizan las más modernas técnicas para evadir las contramedidas y alcanzar sus objetivos.

El uso de instaladores dañinos y el secuestro de actualizaciones han aumentado en la fase inicial de tales ataques. Los archivos de instalación con código dañino se colocan en los sitios web o servidores de actualización de los fabricantes de software, de forma que cuando los usuarios descargan e instalan los programas, también se ejecuta un programa dañino que, posteriormente, puede descargar módulos adicionales. Se trata de un método muy eficiente para los atacantes, porque las víctimas instalan el malware sin saberlo, pudiéndose comprometer una gran cantidad de objetivos, según el tipo de programa. No obstante, los riesgos de este método de ataque pueden mitigarse por parte de los fabricantes de software, protegiendo sus sitios web, firmando electrónicamente el software y almacenando las claves de firma en sistemas aislados y protegidos.

Algunos ejemplos recientes de ataques por secuestro de mecanismos de instalación son *Shadowpad*, *NotPetya*, *CCleaner* y algunos otros programas legítimos. A este vector de ataque también se le conoce como un ataque a la cadena de suministro, en el que se ataca primero a los proveedores del objetivo real, para utilizarlos como puente para alcanzar a la red del objetivo último. Este es otro mecanismo utilizado por grupos como APT10 como parte de la campaña *Cloud Hopper*[92].

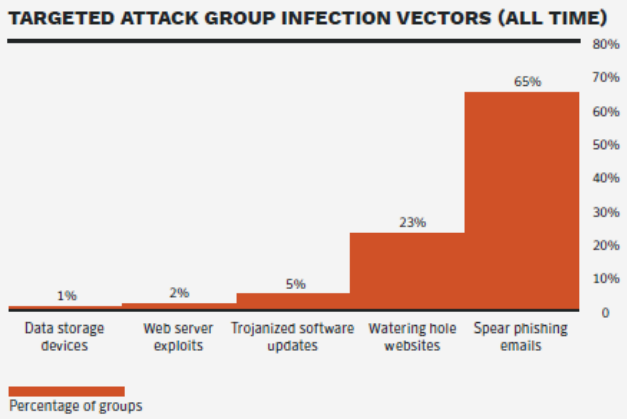
Las figuras de la derecha muestran la motivación de los atacantes (propósitos financieros, disrupción o inteligencia) desde 2016 hasta 2018[93].



[92] Véase. Panda: 'Cloud Hopper', la campaña de ciberespionaje dirigida a MSPs (en https://www.pandasecurity.com/spain/mediacenter/noticias/cloud-hopper-ciberespionaje/)

[93] Fuente: Symantec: ISTR. Vol. 24 (Feb., 2019)

Además de estas tendencias, los correos electrónicos fraudulentos con enlaces (a código dañino o a sitios de phishing para obtener datos de acceso de buzones de correo web o VPN) o archivos adjuntos dañinos, siguen siendo muy habituales en la fase inicial de un ataque, como se observa en la figura de la derecha[94].



La BSI alemana[95] ha descrito algunos casos de 2018 en Oriente Medio, en los que se evidenciaron infecciones de aplicaciones legítimas para teléfonos inteligentes en tiendas de aplicaciones de terceros.

Una fase posterior de las APT es el movimiento lateral, durante el cual los atacantes extienden su influencia dentro de la red de la víctima, utilizando herramientas de administración legítimas (tales como PowerShell o Windows Management Instrumentation, WMI), lo que hace que sus acciones sean menos sospechosas. Otra tendencia es el uso de herramientas disponibles públicamente que, a diferencia de las herramientas de administración, no existen en las instalaciones estándar. Por ejemplo, varios grupos de atacantes han utilizado versiones públicas de la herramienta de prueba de pentest *Cobalt Strike*. Otras herramientas, públicamente disponibles, son *Powershell Empire* y *Koadic,* lo que representa dos ventajas para los atacantes: evitan esfuerzos de desarrollo y hacen que sea más difícil clasificar los ataques[96].

Parece claro que la única protección posible contra las APT es adoptar un concepto de seguridad holístico que incluya algunas de las siguientes medidas clave:

- Usar autenticación de dos factores para VPN y webmail, como mecanismo de protección contra el phishing.
- Emplear directorios de lista negra para dificultar la ejecución inicial de código dañino de los archivos adjuntos del correo o del navegador.

[94] Fuente: Symantec, op.cit.

[95] Véase: Federal Office for Information Security (BSI): The State of IT Security in Germany 2018.

[96] Sin embargo, esta tendencia no debe exagerarse. Según el BSI alemán, el software disponible públicamente nunca podrá reemplazar completamente los programas hechos a medida. Los agentes de las amenazas manejan requisitos especiales para llevar a cabo ataques dirigidos de la manera más eficiente posible. Por otro lado, el uso de malware conocido aumenta la probabilidad de detección por parte de los productos de seguridad. En respuesta, los actores dañinos continuarán desarrollando su propio malware y lo utilizarán en paralelo con las herramientas disponibles públicamente.

- Restringir la comunicación entre los clientes a funciones esenciales hace que el movimiento lateral sea más difícil para los atacantes.
- El modelo de capas en Active Directory garantiza que los datos de acceso con privilegios elevados no se utilicen en sistemas con bajo privilegio, lo que exige de los atacantes un esfuerzo adicional para obtener datos de acceso con alto privilegio.

Por otro lado, los medios de comunicación suelen informar frecuentemente de ataques que tienen relevancia política, recibiendo poca atención aquellos otros relativos a espionaje industrial. Hay que tener en cuenta que la información que se publica no es, necesariamente, representativa o exhaustiva de todos los ataques.

El siguiente cuadro ofrece una descripción general de los grupos de atacantes más relevantes en diferentes industrias[97].

[97] Fuente: Federal Office for Information Security (BSI): The State of IT Security in Germany 2018.

Gov. organis.	Milit./ armaments	Opposition	Media	Energy	Finances	Video conf.	NGO	Univer-sities	High tech	Trans./ logistics	Aeron. & aerospace	Health	Law offices
APT12/ Num-beredP. APT28/ Sofacy APT29/ CozyBear APT32/ Ocean-Lotus APT37/ Reaper Bahamut BlueMush-room Cadelle/ Chafer Callisto Charming-Kitten Dark-Caracal DarkHotel Dropping-Elephant Emissary-Panda Extreme-Jackal Gamare-don Gaza-Cybergang Greenbug Hammer-Panda Infy KeyBoy Lapis/ Trans-parentTr. Longhorn Lotus-Panda Machete Micropsia Muddy-Water Naikon/ OverrideP. Leviathan OilRig Operati-onCleaver Project-Sauron Shamoon Snake Sowbug Tick TidePool/ Ke3chang Tonto Transpa-rentTribe Tropic-Trooper/ PirateP. Vermin Viceroy-Tiger	APT28/ Sofacy APT37/ Reaper AridViper BlueMush-room Callisto Charming-Kitten C-Major/ PureStrike Dark-Caracal Dropping-Elephant Gamare-don Gaza-Cybergang Hammer-Panda HelixKitten Lotus-Panda Machete Naikon/ OverrideP. Leviathan OilRig Operation-Cleaver Project-Sauron Snake	Ahtapot APT32/ Ocean-Lotus Bahamut BlackOasis Bookworm Charming-Kitten Dark-Caracal Ener-geticBear Flying-Dragon Group5 Infy Neo-dymium Operation-Cleaver Operation Manul Prome-thium ScarCruft Sima Stealth-Falcon SunTeam Temper-Panda ZooPark	APT28/ Sofacy APT32/ Ocean-Lotus Bahamut BlackOasis BugDrop Callisto Charming-Kitten Dark-Caracal DarkHotel Dropping-Elephant GazaCy-bergang Infy Olympic-Destroyer Operation Manul Sandworm ScarCruft Shrouded-Crossbow Stealth-Falcon SunTeam Tick	APT10 APT18/ Wekby APT29/ CozyBear Charming-Kitten Electric-Powder Emissary-Panda Energetic-Bear Gaza-Cybergang Greenbug HelixKitten Kraken/ Laziok Longhorn Machete Muddy-Water OnionDog Operation-Cleaver Sandworm Shamoon Tropic-Trooper/ PirateP.	APT18/ Wekby APT29/ CozyBear BlueMush-room Dark-Caracal Dropping-Elephant Emissary-Panda Energetic-Bear Equation-Group Gaza-Cybergang Hammer-Panda Longhorn OilRig Sandworm	APT18/ Wekby Codoso Emissary-Panda Hammer-Panda HelixKitten Longhorn Machete Muddy-Water OilRig Project-Sauron Thrip	APT29/ CozyBear APT37/ Reaper Callisto Charming-Kitten DarkHotel Hammer-Panda Honeybee Infy NilePhish Operation-Cleaver Rocket-Kitten	APT10/ menuPass BugDrop Charming-Kitten Codoso Dark-Caracal DarkHotel Greenbug DarkHotel Longhorn Leviathan Rocket-Kitten	APT18/ Wekby Charming-Kitten Codoso LEAD/ Winnti Tick	Cadelle/ Chafer NanHaiShu OilRig OnionDog Project-Sauron Shamoon	APT28 Dropping-Elephant Emissary-Panda Leviathan Hammer-Panda Greenbug Longhorn	APT10/ menuPass Leviathan LEAD/ Winnti	APT29/ CozyBear Codoso Dark-Caracal DeepPanda Leviathan

Lista de Grupos APT activos en diferentes industrias (entre el 1 de enero de 2017 y el 31 de mayo de 2018)

1.17. Ciberespionaje

Como ha señalado ENISA[98], varios informes de organizaciones de investigación de seguridad global revelaron que el ciberespionaje se está convirtiendo en una práctica habitual de ciertos Estados[99]. Estos se dirigen habitualmente contra sectores industriales, infraestructuras críticas y estratégicas en todo el mundo, incluidas entidades gubernamentales, ferrocarriles, proveedores de telecomunicaciones, compañías de energía, hospitales y entidades financieras[100], con el objetivo de obtener beneficios geopolíticos, secretos de Estado y/o comerciales, propiedad intelectual o

[98] Fuente: ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends. FINAL VERSION. 1.0. ETL 2018. JANUARY 2019

[99] Ver: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

[100] Véase: https://www.blackhat.com/docs/us-18/black-hat-intel-where-cybersecurity-stands.pdf

industrial, así como datos e informaciones de sectores estratégicos. El número de actores que se ven involucrados (desde organizaciones económicas a servicios de inteligencia, pasando por actores interpuestos) es muy amplio[101].

Durante el período que abarca el informe, el número de ciberataques patrocinados por Estados, centrados en la economía, ha aumentado. Estas acciones, dirigidas también al uso de IoT, están también incrementando en los servicios públicos, petróleo, gas natural y fabricación. Además, el uso de APT indica que muchos ataques dirigidos contra el sector financiero tienen su origen en las tácticas, técnicas y procedimientos del ciberespionaje (usadas por actores tales como *Cobalt Group, Carbanak* y *FIN7*).

Mostramos seguidamente las iniciativas de mayor interés en relación con este tipo de ataques:

- La Comisión de Asuntos Exteriores del Parlamento Europeo ha pedido a los Estados miembros que establezcan una Unidad de Defensa Cibernética[102] y trabajen conjuntamente en una defensa común[103]. Por su parte, el Presidente norteamericano Trump ha llamado al despliegue de "tácticas ofensivas proactivas", en relación con la seguridad nacional[104].
- Las vulnerabilidades introducidas por tecnologías emergentes, tales como la Inteligencia Artificial (IA) o el Internet de las Cosas (IoT), generan interés entre los Estados atacantes para apoyar actividades de ciberespionaje a través de su explotación.
- La infiltración de sw en la cadena de suministro constituye una amenaza clara para todos los sectores, en especial para las infraestructuras críticas.
- La debilidad de determinadas legislaciones nacionales podría permitir la sustracción de propiedad intelectual. Este es el caso, por ejemplo, de las relaciones comerciales entre EE.UU. y China, donde se exige la

[101] Véanse: https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf , https://www.accenture.com/t20180803T064557Z__w__/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf , https://www.nytimes.com/2018/11/06/opinion/midterm-elections-russia.html?rref=collection%2Ftimestopic%2FCyberwarfare&action=click&contentCollection=timestopics&region=stream&module=stream_unit&version=latest&contentPlacement=3&pgtype=collection y https://www.theguardian.com/technology/2018/oct/17/theresa-may-to-urge-eu-leaders-to-take-action-on-cyber-attacks

520 https://www.wired.co.uk/article/china-hacking-cyber-spies-espionage, accessed November 2018.

521 https://www.politico.eu/article/europe-raises-red-flags-on-chinas-cyber-espionage/, accessed November 2018.

[102] Ver: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0492+0+DOC+PDF+V0//EN

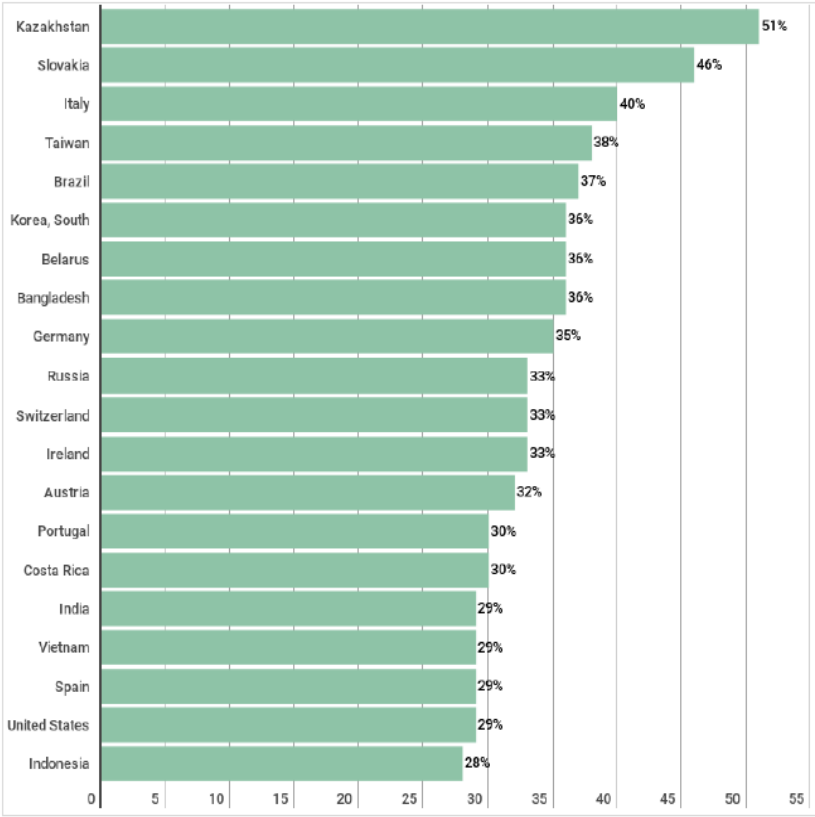
[103] Ver: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-625.376+01+DOC+PDF+V0//EN&language=EN

[104] Ver: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

aprobación del gobierno antes de transferir los datos fuera del país. En Rusia, por ejemplo, se exige el código fuente para toda la tecnología extranjera que se venda dentro del país.

- Es probable que las nuevas sanciones impuestas a Irán presionen al país para intensificar las ciberamenazas patrocinadas por el Estado para lograr sus objetivos geopolíticos y estratégicos a nivel regional, especialmente, si no mantiene a sus homólogos europeos comprometidos con el Plan de Acción Integral Conjunto (Acuerdo JCPOA).

Las redes de tecnología operacional (OT) de las industrias son un campo de acción idóneo para los actores de las ciberamenazas. Estos agentes utilizan herramientas de administración remota (RAT) que ya están instaladas en los sistemas de control industrial (ICS). Un informe reciente[105] señala los 20 países en los que se utilizaron RAT en incidentes de espionaje, durante el primer semestre de 2018.



[105] Ver: https://securelist.com/threats-posed-by-using-rats-in-ics/88011/

Por su interés, se reproduce un cuadro generado por el gobierno holandés, con las precauciones básicas para prevenir el ciberespionaje, incluyendo su grado de efectividad y coste asociado[106].

	Ref.	Precaution	Overall effectiveness	Impact on work rocesses	Initial costs	Ongoing costs
Essential precautions						
1	3.1	Compartmentalise and segment networks and systems.	Very high	Low	High	Low
2	1.1	Strengthen basic security of servers and workstations.	Very high	Low	Average	Average
3	1.5	Introduce "whitelisting" of trusted applications.	Very high	Low	High	Average
4	1.4	Apply end-to-end encryption on public infrastructure.	Very high	Low	Average	Average
Important precautions						
5	3.2	Minimise use of enhanced rights.	High	Average	Average	Average
6	2.1	Apply intrusion detection and prevention to known indicators of compromise (IoCs).	High	Low	High	Average
7	1.2	Scan incoming e-mail for security risks.	High	Average	Average	Low
8	3.3	Enforce use of strong authentication.	High	High	High	Average
9	1.3	Improve users' security awareness.	High	Average	Low	Low
10	2.2	Conduct security tests regularly (penetration tests, vulnerability scans, red teaming and so on).	High	Low	Average	Average
11	2.3	Check websites visited by staff for malware.	High	Low	Average	Low
12	2.4	Use anomaly detection in the "crown jewels" compartment.	High	Low	High	Low
13	2.5	Use "honeypots" and "honeytokens".	Average	Low	Average	Low

1.18. Amenazas híbridas

Las denominadas "amenazas híbridas", tal y como se recoge en la **Estrategia de Seguridad Nacional**[107]**,** de 2017, "son acciones combinadas que pueden incluir, junto al uso de métodos militares tradicionales, ciberataques, operaciones de manipulación de la información, o elementos de presión económica o campañas de influencia en redes sociales, que se han manifestado especialmente en procesos electorales. La finalidad última que se persigue es la desestabilización, el fomento de movimientos subversivos y la polarización de la opinión pública"

La definición del Gobierno de España reconoce también que este tipo de amenaza puede venir tanto por parte de "agentes estatales" como "no estatales", donde se atacan deliberadamente vulnerabilidades sistémicas de los estados y sus instituciones, utilizando el ciberespacio como la herramienta más versátil y adecuada

[106] Fuente: Cyberespionage. Are you aware of the risks? (A publication by the AIVD and MIVD – Oct. 2017)

[107] En esta Estrategia se incluye de manera explícita la amenaza de acciones híbridas como uno de los principales retos de seguridad a los que debe de hacer frente el país. GOBIERNO DE ESPAÑA. Departamento de Seguridad Nacional.

http://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf

para sus propósitos[108]. Constituye, por tanto, el fenómeno resultante de la convergencia e interconexión de diferentes elementos que, en conjunto, constituyen una amenaza más compleja y multidimensional[109].

La desinformación[110] representa, por su parte, una de las armas que configuran este tipo de amenazas. A la vista de su importancia, la UE ha identificado las siguientes cuestiones-clave[111]:

- Gracias a las tecnologías digitales, el acceso a las noticias se ha vuelto más fácil y barato, y su consumo ha tenido un crecimiento sin precedentes.
- Los intermediarios online han aumentado significativamente, en un marco regulatorio que los hace no responsables del control editorial y de la mala conducta de sus usuarios. En su consecuencia, frecuentemente, las noticias online se caracterizan por la falta de verificación de los hechos y su escasa originalidad.
- Producir y difundir desinformación es mucho más barato y más fácil gracias a la disponibilidad de una infraestructura de plataformas digitales, extremo a extremo, para el intercambio de información.
- Se rompe la correlación entre la divulgación de noticias y los controles de calidad. En la era anterior a Internet, solo los medios de comunicación con recursos suficientes podían llegar a las grandes audiencias. Hoy en día, cualquiera puede ser un editor con alcance global.
- El vínculo entre el contenido de las noticias y los medios de comunicación se ha roto: mientras las noticias falsas comporten tráfico, dinero (publicidad, por ejemplo) y no exista responsabilidad, no hay una razón sólida para esperar que las plataformas digitales tengan un incentivo para tomar decisiones contundentes contra la desinformación.
- En el mundo actual, ningún medio informativo está completamente protegido de una posible presión o dirección política, por lo que, tanto los

[108] Véase: "Amenazas Híbridas: nuevas herramientas para viejas aspiraciones". Dr. Carlos Galán. Real Instituto Elcano (Diciembre, 2018).

[109] Ver: European Parliament Research Service (EPRS): At a Glance: Understanding Hybrid Threats. (Junio, 2015).

[110] Véase el Informe de Buenas Prácticas del CCN-CERT: BP/13 Desinformación en el ciberespacio. https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3549-ccn-cert-bp-13-desinformacion-en-el-ciberespacio/file.html

[111] Ver: "The legal framework to address "fake news": possible policy actions at the EU level" Parlamento Europeo. (Junio, 2018). Este document, además, distingue cuatro formas distintas en relación con las fake news: Content bubbles (or echo chambers), Unintentional fakes/opinions ("misinformation"), Intentional fakes or amplifiers ("Disinformation") y Disinformation (or influence) operations.

canales tradicionales como los nuevos, deben considerarse más complementarios que alternativos.

- En un mundo rico en información, la respuesta más efectiva a la desinformación es la concienciación (que podría ayudarse de la Inteligencia Artificial).

Uno de los casos más significativos ocurridos durante el periodo del informe en relación con este tipo de amenazas se produjo en la aplicación WhatsApp, que se usó como herramienta para dirigirse a millones de votantes brasileños antes de las elecciones presidenciales de octubre de 2018, inundando el sistema de mensajes políticos. Un estudio realizado sobre más de 100.000 mensajes de WhatsApp reveló que más de la mitad contenía información engañosa o completamente falsa[112].

1.19. Ataques a Sistemas de Control Industrial (ICS)

Durante 2017 y 2018, los Sistemas de Control Industrial han sido víctimas frecuentes de ataques no dirigidos, infectando con ransomware estaciones de trabajo de operadores u otros componentes de control; incidentes que, en algún caso, se alargaron durante varias semanas[113].

Los vectores de entrada fueron, principalmente, correos de phishing y soportes extraíbles, aunque también se evidenciaron casos en los que la infección se produjo como resultado de la utilización de sistemas de mantenimiento remoto configurados incorrectamente. En todos los casos, el código dañino explotó vulnerabilidades conocidas de software obsoleto y una inadecuada segmentación entre las redes de oficina y las redes de producción. Todo parece apuntar a que este tipo de incidentes continuará representando una amenaza significativa para los ICS en los próximos años[114].

Los ataques dirigidos a ICS con el objeto de manipularlos constituyen, sin embargo, una excepción[115].

Finalmente, la progresiva introducción de lo que se ha denominado "Industria 4.0"[116] también ofrece nuevos puntos de partida para las actividades delictivas.

---

[112] Ver: https://www.independent.co.uk/news/world/americas/brazil-election-2018-whatsap-fake-news-presidential-disinformation-a8593741.html

[113] Así lo ha afirmado la BSI (Federal Office for Information Security alemana).

[114] Lo que obedece, en parte, a la utilización de sistemas muy antiguos para los cuales no hay actualizaciones o no se aprueban las actualizaciones disponibles proporcionadas por el fabricante o integrador.

[115] Se ha mencionado con anterioridad el ataque Triton, de finales de 2017, cuyo objetivo era reprogramar el sistema de control responsable de la seguridad funcional de una planta.

[116] Industria 4.0 y su sinónimo, Cuarta Revolución Industrial, son expresiones que denominan una hipotética cuarta etapa de la evolución técnica-económica de la humanidad, contando a partir de la Primera Revolución Industrial. Habría comenzado recientemente y su desarrollo estaría proyectado hacia la segunda década del siglo XXI. La

1.20. Correo electrónico

El año 2018 ha demostrado que el correo electrónico sigue siendo muy usado para perpetrar ciberataques. En concreto, el phishing suele ser la primera etapa de un ciberataque, constituyendo la herramienta más usada para establecer un primer punto de entrada en los sistemas de la víctima para desarrollar ulteriores acciones de espionaje o sabotaje[117]. Así, una vez que los atacantes han accedido a la red de la víctima, proceden a buscar la información deseada o exploran cómo está configurada la infraestructura digital de la organización para avanzar en su ataque.

Aunque la forma tradicional de phishing, mediante el uso de spam, aún existe, no se trata ya de la única forma en el panorama actual de amenazas: el número de ataques dirigidos de phishing continúa creciendo. Atacando a individuos influyentes o con acceso a activos financieros o datos sensibles de empresas o de las Administraciones Públicas, los actores persiguen obtener mayores beneficios que mediante campañas de spam aleatorias.

Aunque el número de evidencias de phishing se mantuvo estable en 2017, a finales de 2017[118] y principios de 2018, Microsoft detectó un número considerable de correos electrónicos de suplantación de identidad[119]. Durante 2018, las principales manifestaciones de ciberataques de este tipo fueron los casos de phishing o spear-phishing perpetrados por delincuentes, Estados o actores patrocinados por Estados. Según la empresa Verizon, los Estados utilizaron técnicas de phishing en el 70% de sus ciberataques[120].

Aunque este tipo de ataques no es algo nuevo, todavía hay muchas organizaciones que no implementan medidas adecuadas, tales como los estándares SPF, DKIM y DMARC[121].

---

inteligencia artificial es señalada como elemento central de esta transformación, íntimamente relacionada con la acumulación creciente de grandes cantidades de datos (big data), el uso de algoritmos para procesarlos y la interconexión masiva de sistemas y dispositivos digitales.

[117] Más del 90% de las infecciones por código dañino provienen del correo electrónico. Fuente: Verizon: 2018 Data Breach Investigations Report (en www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf)

[118] Véase: APWG: Phishing Activity Report 2017 (en file:///C:/Users/CARLOS/Dropbox/CCN%20-%20Documentos%20publicados%20en%202018/APWG%20-%20Phishing%20activity%20report%20h1_2017.pdf y http://docs.apwg.org/reports/apwg_trends_report_q3_2017.pdf)

[119] Véase: Microsoft: Microsoft Security Intelligence Report VOLUME 23 (en https://info.microsoft.com/rs/157-GQE-382/images/EN-US_CNTNT-eBook-SIR-volume-23_March2018.pdf)

[120] Verizon op. cit.

[121] No obstante, en 2017 se evidenció que las medidas de seguridad podían eludirse, a raíz de las vulnerabilidades detectadas en "Mailsploit", que permitirían que la dirección de correo electrónico de una persona pueda usarse con éxito como remitente, a pesar de las medidas de seguridad señaladas.

1.21. Ransomware

El término *ransomware* define cierto tipo de código dañino que impide o restringe el acceso a un ordenador, prometiendo (a través de un mensaje de texto) liberar los recursos una vez satisfecho un rescate (extorsión).

Hay dos tipos de ransomware: aquel que bloquea el acceso o uso del equipo, manipulando el sistema operativo y muestra el texto con la petición (pantalla de bloqueo); y aquel otro que cifra los ficheros de datos del usuario, ofreciendo la posibilidad de descifrado después del pago del rescate. En este último caso, la funcionalidad general del sistema no suele verse afectada.

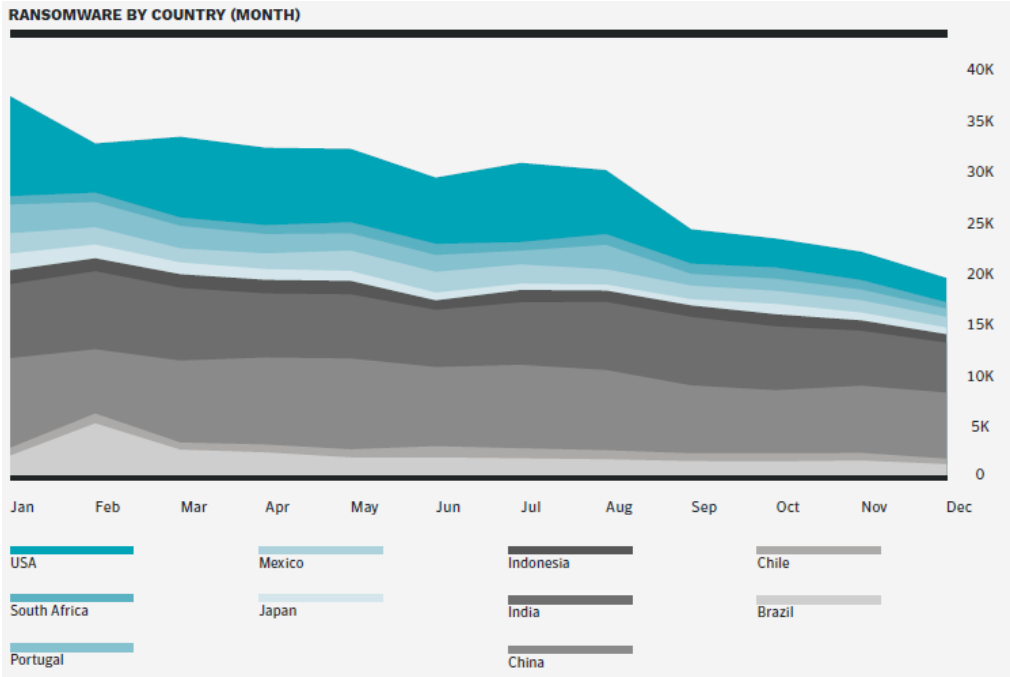
En la actualidad, el ransomware se presenta a través de varios vectores de ataque, entre ellos:

- Correos electrónicos de spam, que contienen código dañino adjunto o al que se hace referencia a través de una URL.
- Exploits drive-by que explotan vulnerabilidades de los navegadores, plugs-ins de navegadores o sistemas operativos, activándose al acceder a un sitio web infectado o a la publicidad insertada en él (en muchos casos, sin la interacción del usuario).
- Exploits-kits que explotan diversas vulnerabilidades en diferentes productos y que hacen que tanto el tipo de ataque como el transporte del código dañino estén disponibles para el actor dañino con solo tocar un botón.
- Explotando vulnerabilidades o adivinando contraseñas débiles en servidores web de acceso público. También hay software para espiar contraseñas en las redes internas.
- Las vulnerabilidades en las herramientas de administración remota (RAT) también se utilizan para acceder a los sistemas que están sujetos a mantenimiento, lo que significa, en muchas ocasiones, que el atacante dispone de privilegios de acceso desde el principio.
- En ocasiones, el código dañino, tras la infección, utiliza vulnerabilidades en el sistema operativo para hacerse pasar por un proceso legítimo y evitar la detección temprana.

Frecuentemente, los pagos de los rescates se realizan en criptomonedas, tales como bitcoin o ethereum, o a través de sitios web anónimos en la red TOR, lo que dificulta la persecución del delito.

Desde 2016, ha crecido el riesgo asociado al ransomware, como lo demuestran las principales campañas de 2017, como *WannaCry* y *NotPetya/ExPetr*[122].

La figura siguiente muestra la penetración de ransomware por país, durante 2018[123].



Pese a que los incidentes de 2018 no han tenido el impacto mediático de años anteriores, también han sido una fuente importante de riesgo. Estos son algunos ejemplos:

- El 26 de enero de 2018, se descubrió un nuevo software de este tipo, denominado *GandCrab*. Además de campañas localmente activas (*Magniber*), fue el primero en distribuirse de forma masiva a través de un exploit-kit.
- El ransomware *SamSam* ataca a través de vulnerabilidades en componentes de software de acceso público (servidores web) o adivinando contraseñas débiles en la gestión de usuarios. La ciudad de Atlanta, Georgia (EE. UU.), fue atacada con este ransomware el 22 de marzo de 2018, provocando la paralización de importantes servicios.
- El ransomware *XiaoBa* contiene también software que ejecuta minería de criptomonedas, es decir, altera los programas ejecutables para que

[122] El último de ellos debe considerarse más un acto de sabotaje que un ransomware real, ya que las personas afectadas no recibieron ningún mensaje de chantaje y los usuarios no tuvieron la oportunidad de descifrar los archivos cifrados.

[123] Fuente: Symantec: ISTR, Vol. 24 (Feb., 2019)

asuman las tareas de infraestructura para las criptomonedas y, por lo tanto, obtener beneficios económicos directos.

- En abril de 2018, se observó un ransomware que no exige dinero como rescate, aunque alienta a las personas a jugar juegos de ordenador. Otro utilizó vulnerabilidades en HPE Integrated Lights-Out para chantajear los pagos de bitcoin. El ransomware RanSIRIA afirma utilizar el dinero del rescate para apoyar a los refugiados sirios.El ransomware SynAck fue el primero en utilizar una técnica denominada "Proceso Doppelgänging", en mayo de 2018. También se utilizaron varias otras técnicas que dificultan tanto la detección como el análisis (eliminar protocolos, calcular direcciones de salto, usar un hash en lugar de la cadena original).

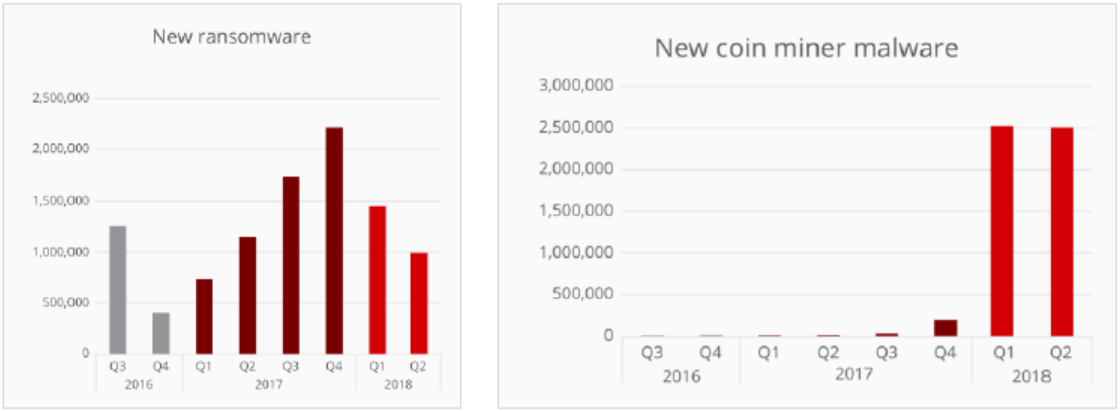
Estos incidentes y otras informaciones provenientes de la industria de seguridad IT apuntan a los siguientes desarrollos:

- De forma similar a los servicios de botnet disponibles para ataques DDoS, en la actualidad también hay ofertas de *Ransomware-as-a-Service*. El usuario del servicio ya no tiene que entender todos los detalles del vector de ataque y puede utilizar un enfoque modular para crear variaciones de ransomware existente.
- Hay signos de fragmentación en las familias de ransomware. Esto no hace necesariamente que los ataques individuales sean más peligrosos, sino que contribuye a la creación de un panorama confuso de amenazas, lo que hace más difícil excluir consecuencias graves. Además del hecho de que los procedimientos de ataque se vuelven cada vez más complejos, las precauciones para ocultarse o evitar la detección de los antivirus son cada vez más sofisticadas. Los procesos dañinos se disfrazan como procesos del sistema operativo, se eliminan los rastros en forma de entradas de registro o los archivos intermedios necesarios y las direcciones de salto se subcontratan o solo se generan en el proceso de cálculo, lo que dificulta la labor forense.
- Los grupos objetivo y los individuos son muy diversos. Los usuarios individuales son menos destacados como pagadores de rescate que en el pasado, por lo que la obtención de beneficios se vuelve más difícil para los atacantes. Por otro lado, las demandas de rescate están teniendo en cuenta el poder económico de la víctima y la relevancia de los datos alojados en el ordenador. Se están buscando nuevos grupos objetivo, por ej. personas receptivas a los problemas sociales. Independientemente de si la afirmación de usar el rescate para los refugiados, es o no cierta, el

ransomware demuestra una importante innovación que puede aumentar la superficie de ataque.

- Hay signos de diversificación en los vectores de ataque. Diferentes familias de ransomware se propagan a través de correo no deseado, exploits-kits, exploits drive-by, gusanos y software de mantenimiento remoto. El ransomware parece disminuir en la medida en la que otros modelos, como la minería de criptomonedas, son más rentables o prometen beneficios más constantes. Por otro lado, los cambios en la situación inicial podrían, a la inversa, provocar un aumento de nuevo del ransomware, tales como la caída de los tipos de cambio de las criptomonedas o la mayor disposición a aceptar pagos de rescate.

La figura siguiente muestra una correlación entre el volumen de detección de ransomware y de cryptojacking, desde 2016 hasta 2018[124].



1.22. Spam y phishing

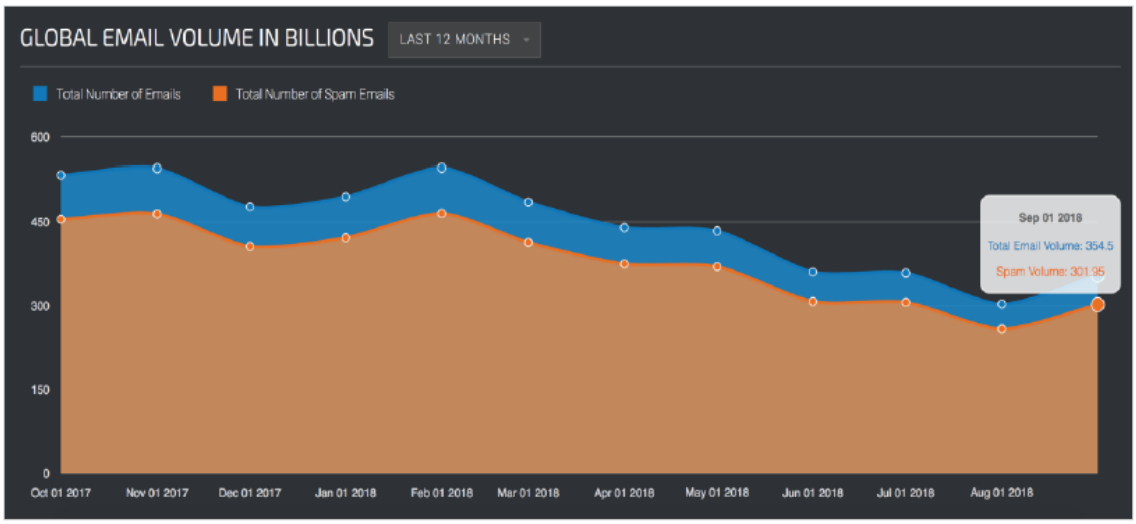
Suele denominarse *spam* a los correos electrónicos no solicitados, dividiéndose en tres categorías:

- Spam convencional: que, a menudo, se utiliza para anunciar productos, o servicios, así como en intentos de fraude.
- Malware spam ("malspam"): utilizado por los agentes de las amenazas para infectar los sistemas de los destinatarios con código dañino. El malware puede estar en un adjunto a un correo electrónico o introducirse indirectamente a través de un enlace en el cuerpo del correo o en los archivos adjuntos. Este enlace conduce al malware o a un sitio web que contiene exploits drive-by.

[124] Fuente: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-sep-2018.pdf

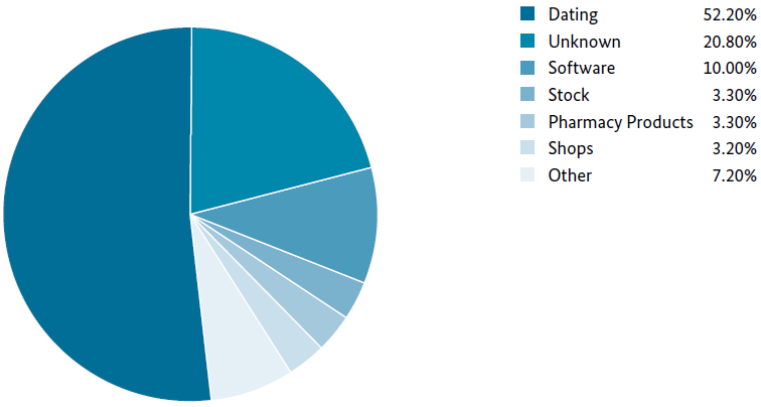
- Mensajes de suplantación de identidad (phishing): que alientan a los usuarios a entregar información, tal como el inicio de sesión (por ejemplo, para banca por Internet, servicios de pago, redes sociales o portales de compras) en sitios web controlados por los agentes de las amenazas.

La figura siguiente muestra la relación mundial entre email verdadero y spam, desde octubre de 2017 a septiembre de 2018[125].



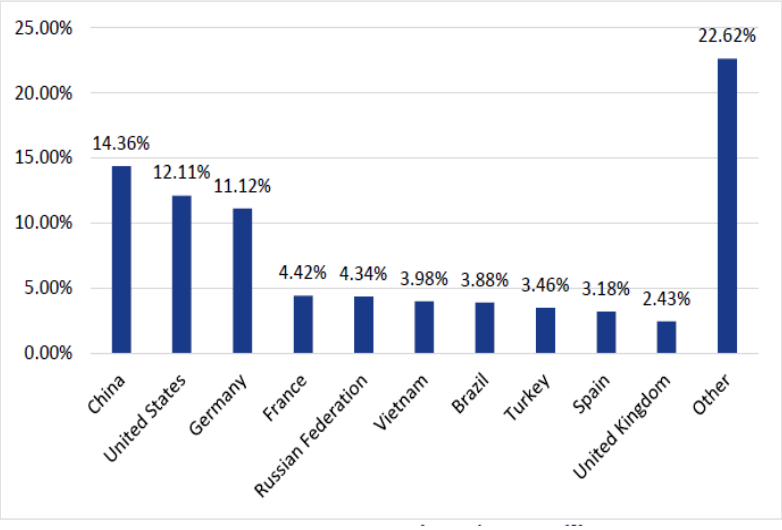
En la mayoría de los casos, el correo no deseado se envía a través de servidores comprometidos, sistemas cliente infectados o a través de cuentas de correo electrónico legítimas, utilizando información de inicio de sesión robada.

La figura siguiente muestra la distribución de spam por áreas[126].



[125] Ver: https://www.talosintelligence.com/reputation_center/email_rep#global-volume
[126] Fuente: BSI, op.cit.

Frecuentemente, los sistemas que distribuyen spam se ensamblan en una botnet, lo que facilita a los atacantes la comercialización de sus actividades como servicio.
La figura de la derecha muestra una distribución del origen de las acciones de spam[127].



Se observa con frecuencia el uso de la información personal sustraída a grandes proveedores de servicios, lo que aumenta significativamente la probabilidad de infección.

Se siguen observando campañas más pequeñas de malspam fuera de la botnet *Necurs*.
De particular interés son las campañas de spam que han perseguido la difusión de *Emotet*. Este código dañino utiliza los datos de Outlook obtenidos durante una infección para enviar un correo electrónico que pretende ser de una persona con la que la víctima potencial ya se ha comunicado.
Si bien una gran cantidad de destinatarios han descrito este ataque como dirigido, en realidad se trata de una operación masiva diseñada para persuadir a los objetivos para que activen la ejecución de una macro en un documento adjunto de MS Office. En la mayoría de los casos, las macros descargaron el propio malware (*Emotet*).

La botnet Necurs
La botnet *Necurs* ha seguido siendo el mayor remitente de mensajes de spam. El tercer trimestre de 2017 fue testigo de un aumento en el número de correos electrónicos de *Necurs* enviados con archivos adjuntos conteniendo código dañino. En su apogeo, sin embargo, esta botnet logró un tercio del volumen que registró a finales de 2016, que sigue siendo el máximo histórico en términos de malspam.
En el cuarto trimestre, su producción se estancó inicialmente y luego aumentó ligeramente en diciembre. Después de las vacaciones de Navidad, solo hubo una ola de spam más grande, a mediados de enero.
Necurs se utilizó principalmente para enviar spam convencional. Promovió, principalmente, los sitios de citas rusos, con algunas campañas más pequeñas que intentaron manipular el precio de las acciones.

El problema dominante en la actualidad es el envío de archivos RTF que aprovechan una vulnerabilidad en el MS Ecuation Editor (CVE-2017-11882, abordada por Microsoft en noviembre de 2017) para ejecutar código dañino que, posteriormente, descarga malware adicional.

[127] Véase: https://securelist.com/spam-and-phishing-in-q2-2018/87368/

Se ha demostrado que el phishing es la forma preferida de comprometer a las organizaciones[128]: el 75% de los Estados miembros de la UE revelaron casos de phishing[129]. Un último dato: más del 90% de las infecciones de código dañino y el 72% de las violaciones de datos en organizaciones se originaron a partir de ataques de phishing[130].

Phishing suplantando a la Federal Office for Informatión Security (BSI) alemana
A principios de 2018, se notificó a la BSI alemana que había en circulación correos electrónicos falsos con remitentes de BSI. Contenían información sobre el tema "Spectre/Meltdown", así como un enlace a una réplica del sitio web de BSI for Citizens [BSI für Bürger]. La URL era similar a las URL oficiales de BSI que incluía un certificado SSL válido emitido para este sitio y contenía un enlace para descargar una supuesta "herramienta de Windows" para eliminar las vulnerabilidades "Spectre" y "Meltdown".
Una vez que se dieron a conocer las vulnerabilidades Spectre y Meltdown, los atacantes aprovecharon el deseo generalizado de los usuarios para actualizar sus sistemas y distribuyeron correos electrónicos con remitentes falsos que pretendían ser de BSI, sugiriendo que la Agencia proporcionaría una actualización para dichas vulnerabilidades.
Está claro que los correos electrónicos y los sitios web falsos se están volviendo cada vez más profesionales. Falsificar sitios web no es un gran desafío; por lo tanto, es importante revisar las URL del sitio web de cerca. Los atacantes a menudo usan URL parecidas a las que pretenden suplantar, usando letras transpuestas o utilizando otros dominios de nivel superior, por ejemplo, ".biz" en lugar de ".es". El acceso a través de HTTPS supone una garantía adicional, aunque no definitiva, como examinamos un poco más adelante.

Estas son las evidencias más significativas de 2018 en torno al phishing:

- Los ataques de phishing se han hecho más específicos. Si bien permanece el modelo tradicional relacionado con el spam, el número de ataques de phishing dirigidos continúa creciendo[131]. El volumen de datos personales sustraídos o filtrados brindan a los phishers la oportunidad de realizar campañas convincentes y específicas a gran escala[132].
- Cambio de objetivo: del consumidor a la organización. Aunque los ataques por phishing se han venido dirigiendo principalmente a consumidores, se ha observado un cambio en sus objetivos, dirigidos ahora también a las propias organizaciones[133]. Este cambio está

[128] Véase: https://www.fireeye.com/company/press-releases/2018/new-fireeye-email-threat-report-underlines-the-rise-in-malware-l.html
[129] Véase: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018
[130] Véase: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf
[131] Véase: https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2018.html
[132] Véanse: https://krebsonsecurity.com/2018/08/the-year-targeted-phishing-went-mainstream/ y https://krebsonsecurity.com/2018/07/sextortion-scam-uses-recipients-hacked-passwords/
[133] Véase: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

impulsado por los beneficios: los datos empresariales se pueden aprovechar de maneras más rentables en comparación con los datos del consumidor (por ejemplo, extorsión, venta de datos en mercados clandestinos, etc.)[134]. Los servicios de correo electrónico (por ejemplo, Microsoft Of365) y los servicios en línea (por ejemplo, DocuSign y Dropbox) han sido también objetivos principales del phishing durante 2018[135].

- Crecimiento de los ataques a dispositivos móviles. Estos ataques han aumentado en torno al 85% anual desde 2011[136]. Se ha observado que el phishing a través de SMS, mensajes móviles (WhatsApp, Facebook Messenger, etc.) y aplicaciones de redes sociales (por ejemplo, Instagram) ha crecido significativamente. Se ha evidenciado un nuevo método de ataque móvil (relleno de URL) que aprovecha el pequeño tamaño de la pantalla de los teléfonos móviles. Finalmente, se han observado actores avanzados que utilizan técnicas de phishing móvil, por ejemplo, *Dark Caracal* y *Pegasus*[137].

- Crecimiento de los sitios de phishing que utilizan HTTPS. Durante 2017, un tercio de los sitios web de phishing han sido accedidos a través de mecanismos HTTPS, utilizándose en muchos casos servicios de certificados gratuitos (por ejemplo, Encrypt o Comodo[138]). Este cambio sigue la tendencia de la creciente adopción de HTTPS en Internet y el hecho de que algunos navegadores comienzan a marcar los sitios HTTP como "No seguro"[139].

- Permanece el problema de Business Email Compromise (BEC). Este es un tipo de ataque de phishing dirigido a ejecutivos y empleados de los departamentos económicos o de recursos humanos, con el objetivo de sustraer dinero de sus organizaciones. Desde octubre de 2013 hasta mayo de 2018, se han notificado 78.000 ataques de BEC en todo el

[134] Véase: https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf

[135] Véanse: https://www.cbronline.com/news/microsoft-office-365-phishing , https://www.docusign.com/trust/alerts y https://www.psafe.com/en/blog/dropbox-phishing-attacks-are-on-the-rise/

[136] Véase: https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-wp-us.pdf

[137] Véanse: https://www.lookout.com/info/ds-dark-caracal-ty y https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/

[138] Véanse: https://letsencrypt.org/ y https://ssl.comodo.com/free-ssl-certificate.php

[139] Véanse: https://letsencrypt.org/stats/ y https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html

mundo, con unas pérdidas estimadas de 12 mil millones de dólares[140]. Debido al hecho de que el 65% de los Estados miembros de la UE han observado este tipo de ataques, las fuerzas policiales europeas han redoblado sus esfuerzos, con la detención de los actores y la eliminación de varias campañas de este tipo[141].

- El Spearphishing es el método de entrega de facto para grupos APT. El 71% de los grupos de APT han usado spearphishing como vector de infección[142]. Durante 2018, los grupos del crimen organizado de más alto perfil fueron *FIN7* y *Cobalt Group*[143]. Además, los actores estatales siguen usándolo como principal vector de infección para sus operaciones de ciberespionaje e interrupción de servicios[144].
- Tendencias en archivos adjuntos maliciosos. Los tipos de archivos maliciosos más comunes en los correos electrónicos de phishing fueron documentos de Microsoft Office, archivos de datos, archivos JavaScript, scripts de Visual Basic y documentos PDF[145].

Según ENISA[146], estos fueron los "temas" más usados en los ataques de phishing:

[140] Véase: https://www.ic3.gov/media/2018/180712.aspx

[141] Véase: https://www.europol.europa.eu/newsroom/news/masterminds-behind-ceo-fraud-ring-arrested-after-causing-more-eur-18-million-of-damage , https://www.europol.europa.eu/newsroom/news/two-arrested-in-france-for-major-ceo-fraud y https://www.fbi.gov/news/stories/international-bec-takedown-061118

[142] Véase: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

[143] Váease: https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html , https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100 y https://www.theregister.co.uk/2018/08/31/cobalt_bank_hackers_phishing_campaign/

[144] Véase: https://www.proofpoint.com/sites/default/files/pfpt-us-wp-human-factor-report-2018-180425.pdf y https://www.bankinfosecurity.com/blogs/nation-state-spear-phishing-attacks-remain-alive-well-p-2643

[145] Véanse: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf , https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf y https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

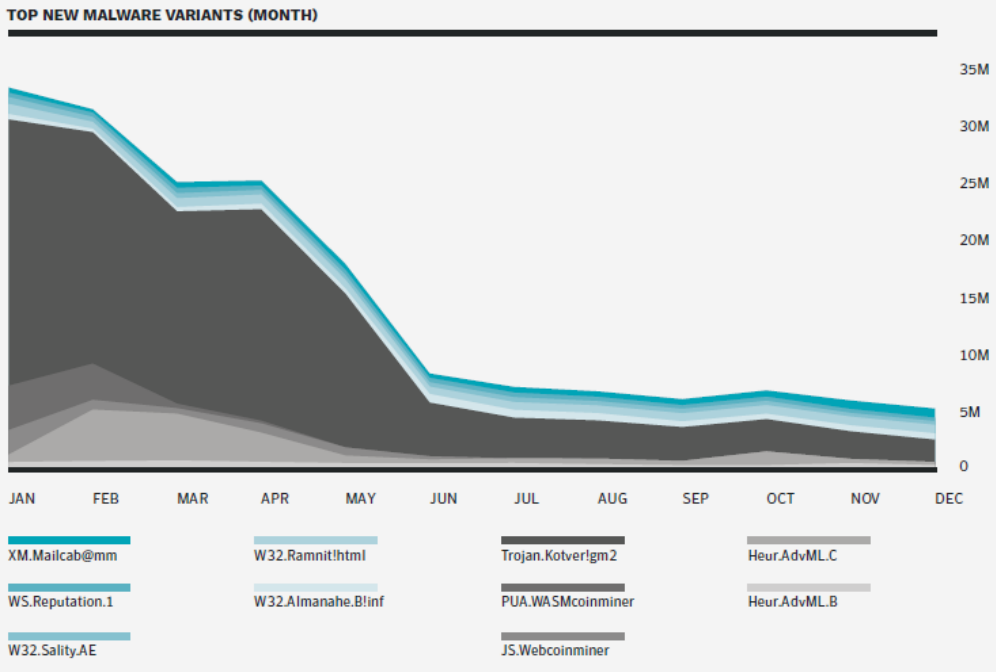
[146] Véase: ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends. FINAL VERSION 1.0. ETL 2018. JANUARY 2019

1. Dropbox account phishing 2. Financial institution phishing 3. Generic email credential phishing 4. Microsoft OWA phishing 5. Office 365 account phishing 6. Adobe account phishing 7. Google Drive phishing 8. Docusign phishing 9. Netflix phishing 10. Paypal phishing	11. Amazon phishing 12. Apple account phishing 13. Microsoft Excel Online phishing 14. LinkedIn account phishing 15. Windows settings phishing 16. Postal/Shipping company phishing 17. MyEtherWallet phishing 18. Alibaba phishing 19. OneDrive phishing 20. Retail phishing

1.23. Código dañino

Se entiende por código dañino todos los tipos de programas que realizan funciones dañinas o malintencionadas, no deseadas en un sistema informático. Los términos troyanos, virus, gusanos, spyware, etc. generalmente se usan como sinónimos para todos los tipos de código dañino. El código dañino o malware es una parte integral de la mayoría de los escenarios de ataque, por ejemplo, cuando un cliente está infectado por ransomware, en botnets o en ataques por APT.

La figura siguiente muestra la evolución de las más significativas variantes de código dañino durante 2018[147].



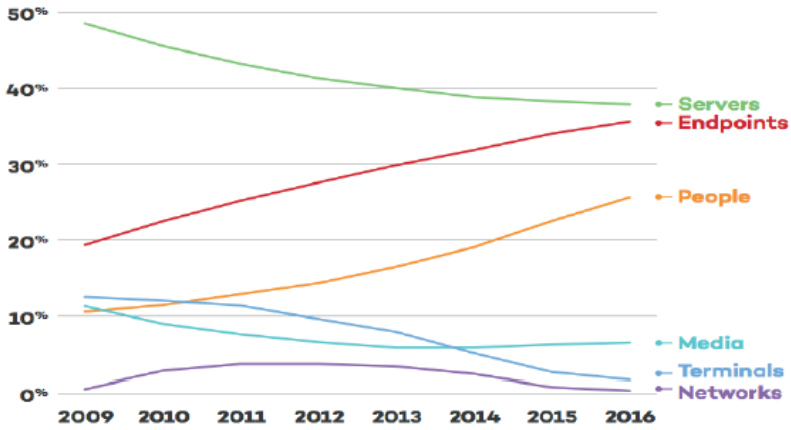
[147] Fuente: Symantec: ISTR, Vol 24 (Feb., 2019)

Los últimos meses de 2017, 2018 y los primeros meses de 2019 han evidenciado lo siguiente:

- Aunque el *adware* es una de las formas más fáciles de distribuir código dañino y el que con más frecuencia se ignora por los usuarios, ha habido pocos desarrollos de esta amenaza durante el pasado año[148].
- Según el Data Breach Investigations (DBIR) de Verizon DBIR[149], la frecuencia de los tipos de código dañino detectados fue la siguiente: .js (37,2%), .vbs (20,8%), ejecutable de Windows (14,8%), MS Office (14,4%), .pdf (3,3%) otro (7,0%).
- El 94% de todos los ejecutables dañinos ha sido malware polimórfico[150].
- El 79% del código dañino detectado en las organizaciones estaba dirigido a Windows, el 18% a Linux y el 3% a los sistemas Mac[151].
- Se ha descubierto el primer malware para la Unified Extensible Firmware Interface (UEFI)[152].
- La mayoría del código dañino móvil se alojó en tiendas de aplicaciones de tercera parte y las categorías de aplicaciones en las que se encontró la mayoría del tal malware móvil fueron: Estilo de Vida *Lifestyle* (27%) y Music&Audio (20%)[153]. Por la parte positiva, se ha observado una disminución en las detecciones de PUA (Potential Unwanted Applications) en relación con el seguimiento del comportamiento de los usuarios[154].
- Durante el período del informe, se ha mantenido la tendencia de malware preinstalado[155], observándose en los casos *RottenSys*[156] y *Triada banking trojan*[157].
- Los troyanos de acceso remoto siguen aumentando. *FlawedAmmyy* es el primer RAT que aparece en la lista de los diez programas maliciosos más importantes[158].

[148] Véase: https://resources.malwarebytes.com/files/2018/07/Malwarebytes_Cybercrime-Tactics-and-Techniques-Q2-2018.pdf
[149] Véase: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf
[150] Véase: https://getmonero.org/
[151] Véase: https://www.crowdstrike.com/resources/reports/2018-crowdstrike-global-threat-report-blurring-the-lines-between-statecraft-and-tradecraft/
[152] https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf
[153] Véase: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf
[154] Véase: https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2017-2018.pdf
[155] Véase: https://research.checkpoint.com/wp-content/uploads/2018/07/Cyber-Attack-Trends-2018-Mid-Year-Report.pdf
[156] Véase: https://research.checkpoint.com/rottensys-not-secure-wi-fi-service/
[157] Véase: https://news.drweb.com/show/?i=11749&lng=en&c=9

- Los endpoints aumentan como objetivos de las amenazas, probablemente debido a lo difuso del perímetro de las organizaciones y el uso de dispositivos móviles[159]. Dirigiéndose al endpoint, los atacantes pueden realizar reconocimientos, moverse lateralmente y desarrollar sus acciones dañinas. La siguiente figura proporciona una perspectiva histórica de los objetivos de los ciberataques de los últimos años[160].



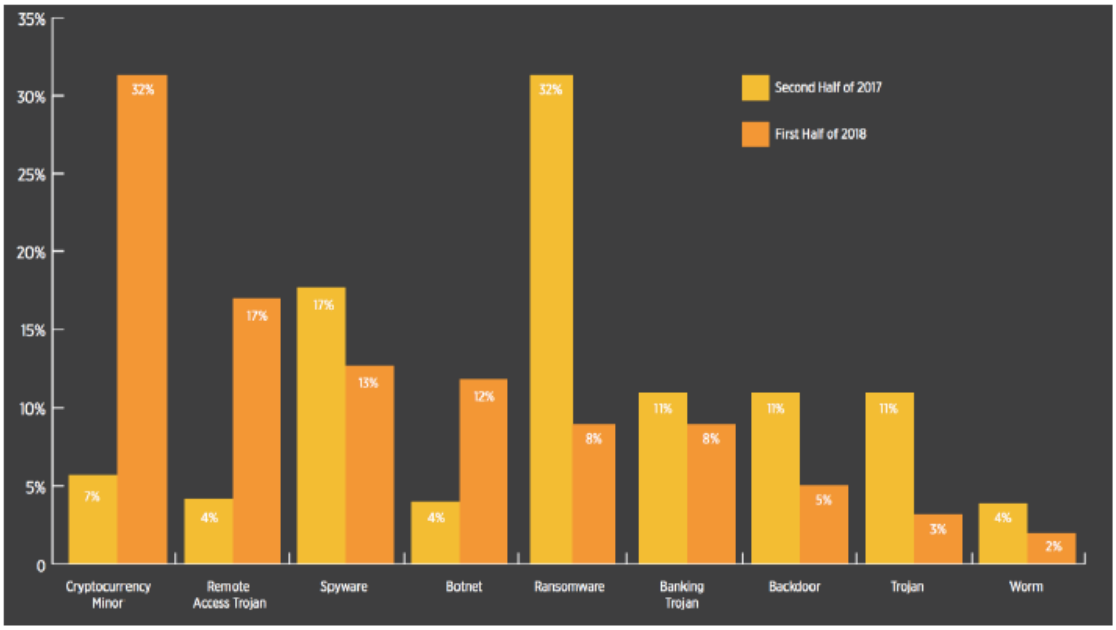
La figura siguiente muestra un análisis comparativo de distintas familias de código dañino, realizado entre el segundo semestre de 2017 y el primer semestre de 2018[161].

[158] Véase: https://www.zdnet.com/article/this-remote-access-trojan-just-popped-up-on-malwares-most-wanted-list/

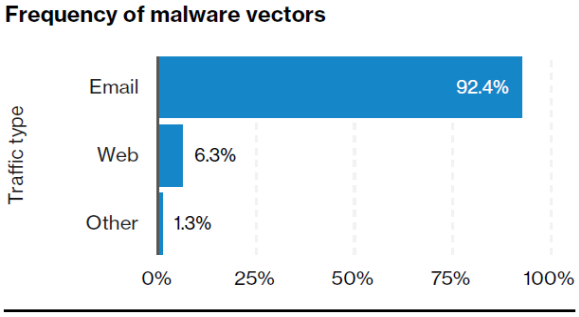
[159] Véase: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

[160] Fuente: https://www.pandasecurity.com/mediacenter/src/uploads/2017/11/PandaLabs_Annual_Report_2017.pdf

[161] Fuente: https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox_Report_Vulnerability_Threat_Trends_2018_Mid-Year_Update.pdf

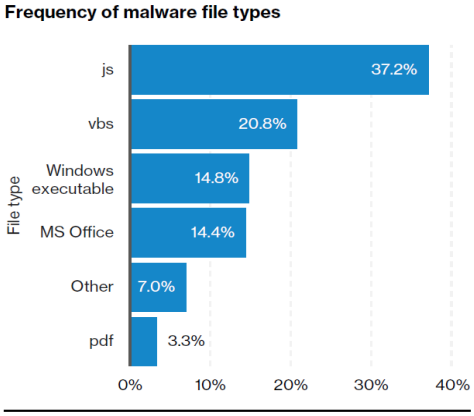


La figura de la derecha muestra la frecuencia del vector de ataque usado para la distribución de código dañino, según un estudio realizado por Verizon, para una muestra de casi 60 millones de instancias. Como puede observarse, la mayor parte del código dañino se introduce vía correo electrónico[162].



En línea con lo anterior, se ha evidenciado una disminución en los exploits para Adobe Flash e Internet Explorer, mientras que aumentaron para Microsoft Office[163]. Según la empresa Kaspersky Lab, más del 90% de los documentos infectados de Office contenían exploits para dos vulnerabilidades específicas.

La figura muestra la distribución de código dañino por tipo de fichero infectado, sobre una muestra de 430 millones de instancias[164].

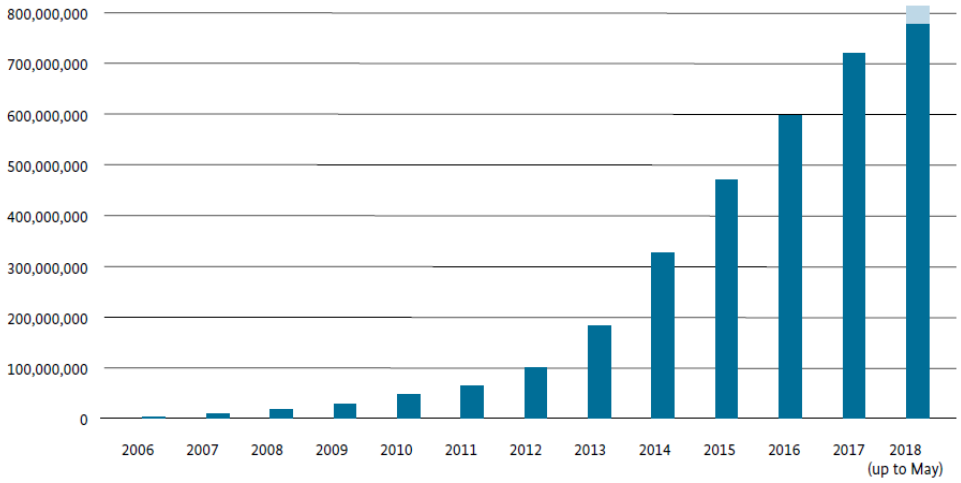


[162] Fuente: Verizon: 2018 Data Breach Investigations Report.

[163] Véase: Kaspersky: OVERALL STATISTICS FOR 2017 (en https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07164706/KSB_statistics_2017_EN_final.pdf)

[164] Fuente: Verizon, op. cit.

Hasta mayo de 2018, la empresa de seguridad cifraba el descubrimiento de nuevos tipos de malware en torno a los 390.000 diarios. La figura siguiente muestra la evolución del código dañino en los últimos años[165].



Durante 2018, además del código dañino para PC, se observó un promedio diario de aproximadamente 690.000 nuevos programas de malware para Android.

Aunque el código dañino sigue siendo la ciberamenaza más común[166], se ha observado que los Estados han incrementado el uso de software legítimo y de proveedores de buena fe, para acceder a víctimas concretas, lo que dificulta la prevención y detección de tales ataques.

A finales de 2017 y principios de 2018, investigadores de la compañía de seguridad Fox-IT evidenciaron la distribución de una gran cantidad de correos electrónicos de phishing con un enlace a un archivo zip descargable. Los destinatarios que abrieron el archivo adjunto se infectaron con el código dañino *Zeus Panda,* que perseguía obtener los datos de inicio de sesión para la información de banca por Internet y de tarjetas de crédito[167]. Aunque el código dañino usado no era nuevo, sí fue exclusivo de esta campaña de phishing, que los atacantes, además de en entidades financieras, también usaron en tiendas de comercio electrónico.

Como se analizará en el epígrafe siguiente, una tendencia es el aumento en el software utilizado para "minar" criptomonedas. Estos "mineros criptográficos" utilizan los recursos computacionales de los sistemas infectados para obtener beneficios económicos directos en forma de criptomonedas. Estos sistemas pueden terminar

[165] Fuente: AV-Test.

[166] Véase: ENISA: Threat Landscape Report 2017 (en https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017)

[167] Aunque los correos electrónicos dañinos no eran muy profesionales (contenían errores ortográficos), unas 48.000 personas hicieron clic en el enlace aunque el número de infecciones fue menor (en torno a las 11.000) porque el código dañino solo funcionada en ordenadores Windows.

convirtiéndose en parte de una botnet que proporciona un servicio de computación y uso intensivo de recursos en el área de los cálculos de blockchain (validación de transacciones), reembolsando este servicio en forma de criptomonedas.

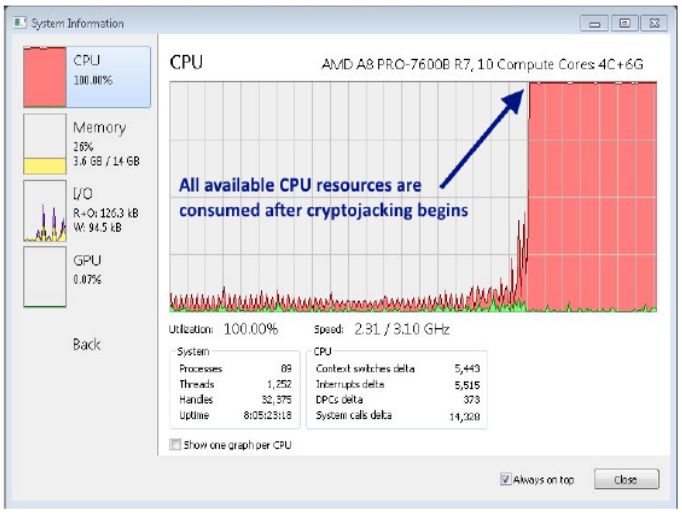
Se debe hacer una distinción entre la minería voluntaria y la minería involuntaria (oculta). En el primer caso, el usuario proporciona voluntariamente la potencia de cálculo de su sistema. Se han descrito diferentes métodos en el uso oculto de estas técnicas: los mineros obligan a los visitantes a un sitio web a participar en la minería con la ayuda de bibliotecas de JavaScript, que son ejecutadas por el navegador; o un malware que permite que los sistemas afectados extraigan criptomonedas como parte de una botnet.

Además, los delincuentes utilizan el código dañino para robar a los usuarios la criptomoneda extraída, penetrando en los repositorios de almacenamiento de criptomonedas (conocidos como carteras criptográficas o *wallets*).

Al igual que en años anteriores, el código dañino sigue siendo una de las mayores amenazas para los consumidores, las empresas y el sector público.

1.24. Criptojacking

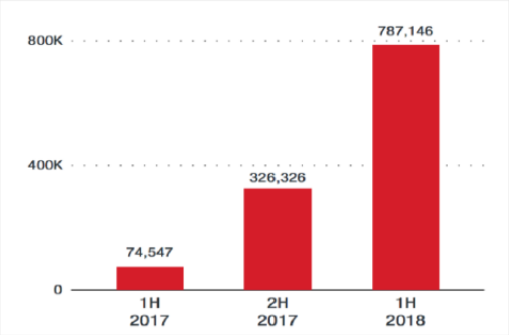
Las monedas criptográficas (*cryptocurrencies*) funcionan sobre la base de principios criptográficos y se obtienen mediante técnicas criptográficas.



En 2018 se ha observado cómo, cada vez más frecuentemente, los ciberdelincuentes intentan obtener beneficios usando lo que se ha denominado *cryptojacking*, es decir: emplear la potencia de cálculo de los sistemas informáticos de terceros para el minado de criptomonedas (cryptomining)[168]. La razón de este comportamiento persigue la monetización directa en base a la generación de criptomonedas.

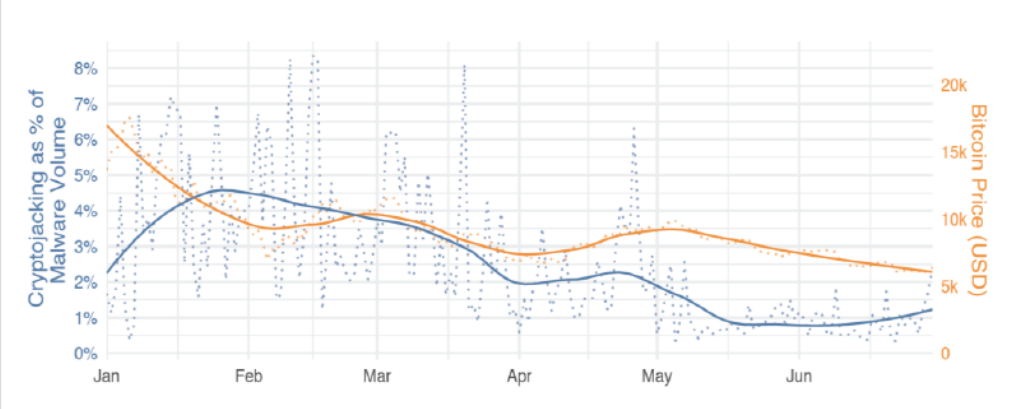
[168] Véase: Check-Point: Global Cyber Attack Trends Report (en file:///C:/Users/CARLOS/Dropbox/CCN%20-%20Documentos%20publicados%20en%202018/CheckPoint%20-%202017%20Global%20CyberAttacks%20Trends%20Report.pdf)

La figura de la derecha muestra el crecimiento de este tipo de acciones, durante 2017 y el primer semestre de 2018, según datos de la empresa TrendMicro[169].



Asimismo, se ha observado que la tendencia de los cryptominers sigue de cerca el flujo de dinero y la valoración de los precios del mercado de criptomonedas[170].

La figura siguiente muestra la correlación entre el precio de mercado de Bitcoin y las detecciones de malware de cryptojacking durante la primera mitad de 2018.



[169] Véase: https://documents.trendmicro.com/assets/rpt/rpt-2018-Midyear-Security-Roundup-unseen-threats-imminent-losses.pdf .

[170] Ver: https://resources.malwarebytes.com/files/2018/07/Malwarebytes_Cybercrime-Tactics-and-Techniques-Q2-2018.pdf

TOP CRYPTO MINING MALWARE

In this section of the report the graphs illustrate the percentage of organizations that were affected by each crypto mining malware. The graphs provide global views and also regional insight into the top crypto mining malware.

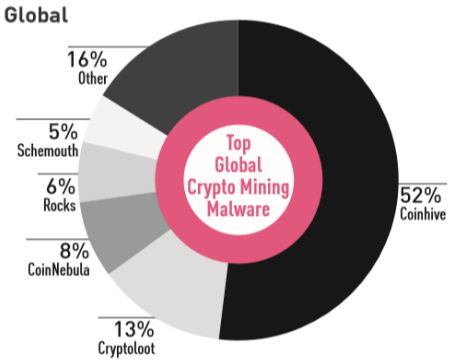


Figure 20: Top Crypto Mining Malware Globally

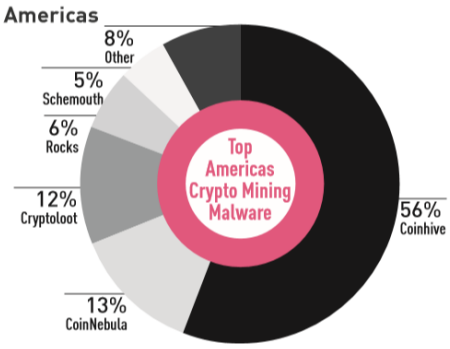


Figure 21: Top Crypto Mining Malware in the Americas

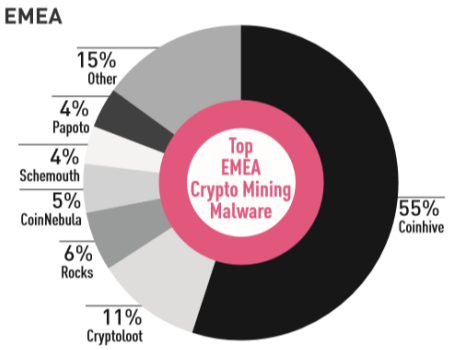


Figure 22: Top Crypto Mining Malware in EMEA

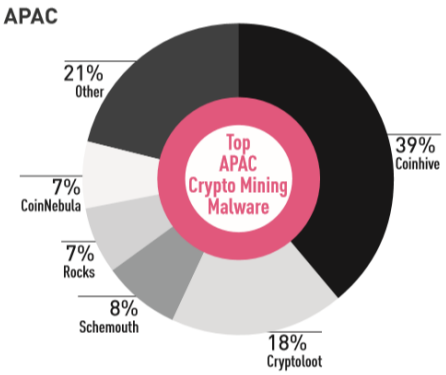
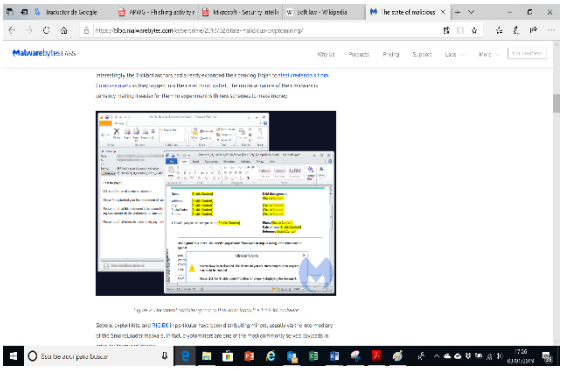


Figure 23: Top Crypto Mining Malware in APAC

Por otro lado, además de los delincuentes, hay casos en que los actores internos pueden representar una amenaza cuando utilizan los sistemas de sus empleadores para criptominar en su propio beneficio personal[171]. En estos casos, es habitual que los agentes de las amenazas intenten obtener el acceso a tantos sistemas como sea posible, infectándolos con malware criptográfico y haciéndolos parte de una botnet.

[171] Véanse:
BBC News: Russian nuclear scientists arrested for 'Bitcoin mining plot' (en https://www.bbc.com/news/world-europe-43003740) y
BitsOnline: Australian Government Staffers Questioned in 'Sneaky' Mining Operation (en https://bitsonline.com/australian-meteorology-staffers-questioned-sneaky-mining-operation/)

Los investigadores de la compañía Proofpoint han seguido la botnet *Smominru*, responsable de la infección de más de 526.000 máquinas Windows con malware criptográfico[172]. Para tales ataques se utilizaron -igual que en *WannaCry*- las vulnerabilidades *EternalBlue* y *DoublePulsar* filtradas con anterioridad. Se afirma que los delincuentes lograron con la botnet más de dos millones de dólares.



Además de los sistemas informáticos tradicionales, los dispositivos de IoT también se utilizan para extraer criptomonedas[173].

Aunque, con frecuencia, los dispositivos móviles suelen tener una capacidad de computación limitada, la gran cantidad de estos equipos que todavía son explotables a través de vulnerabilidades públicas, los convierte en un objetivo muy atractivo para el cryptojacking[174].

Worker ID	Average Hash Rate	Potential Profit
4BrL51JCc9NGQ71kWhnYoDRffsDZy7m1HUU7MRU4nUMXAHNFBEJhkTZV9HdaL4gfuNBxLPc3BeMkLGaPbF5vWtANQpR48NWyTtgLF8daDK	450 KH/s	$330,000.00
4AQe5sAFWZKECiaeNTt59LG7kVtqRoSRJMjrmQ6GiMFAeUvoL3MFeTE6zwwHkFPrAyNw2JHDxUSWL82RiZThPpk4SEg7Vqe	350 KH/s	$257,000.00
4875jA3AmHFaaiYMxSCqnw39viv7NcqJUcbW3kR1kwpQ1stxLKhHM75DDqFBqpMsfzPkqKxJEHokjXP8m3uwzXZx38rEX4C	325 KH/s	$238,000.00
43rfEtGjJdFaXDjRYvo7wJ9Cmq1vWjMdkZzaKEkgp4aQBHKhKZ7Rp6oB1QMBPFJUKGGWc9AeAbr9V6gYVSM8XwbXBYZXBss	245 KH/s	$180,000.00
46xzbEFicggME8PBfwPnwuHbtk2UQY6xmMjAs3MHvLEmSyTnBv3BQTdYZ5Nfw5qLGbZmvTH4rZMXZF6rYNjgfAABSm9FaYT	240 KH/s	$176,000.00
Total	**1.6 MH/s**	**$1,181,000.00**

Como quiera que el criptominado se realice en segundo plano, puede pasar mucho tiempo antes de ser descubierto. Es plausible que el uso creciente del cryptojacking obedezca al notable incremento del valor de muchas criptomonedas. Según la compañía Cisco Talos, un atacante que usara 2.000 sistemas (lo que no es difícil, según los expertos) podría ganar alrededor de 500 dólares diarios (o 182.500 dólares al año).

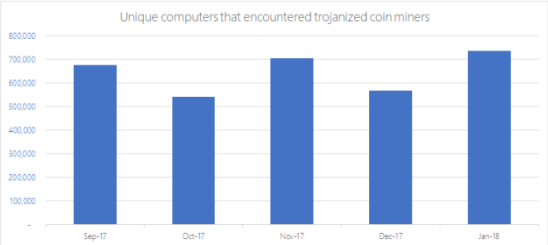
[172] Véanse:
Malwarebytes: The state of malicious cryptomining (en https://blog.malwarebytes.com/cybercrime/2018/02/state-malicious-cryptomining/) y
ProofPoint: Smominru Monero mining botnet making millions for operators (en https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators)

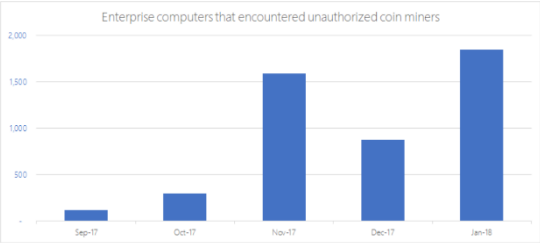
[173] Véase: Avast: Cybercriminals could build cryptomining armies using vulnerable IoT devices at Mobile World Congress 2018 (en https://press.avast.com/cybercriminals-could-build-cryptomining-armies-using-vulnerable-iot-devices-at-mobile-world-congress-2018)

[174] Véase: Cisco-Talos: Ransom Where? Malicious Cryptocurrency Miners Takeover, Generating Millions (en https://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html)

Durante 2018, los investigadores han observado botnets con millones de sistemas infectados, con los que, en teoría, podrían obtenerse beneficios de más de 100 millones de dólares anuales[175].

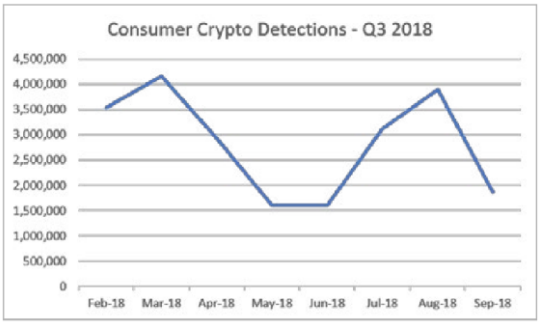
Durante los últimos meses de 2017 los ataques de cryptojacking parecen haber aumentado al tiempo que disminuían los ataques por ransomware. Varias fuentes han establecido una relación entre ambas realidades[176].

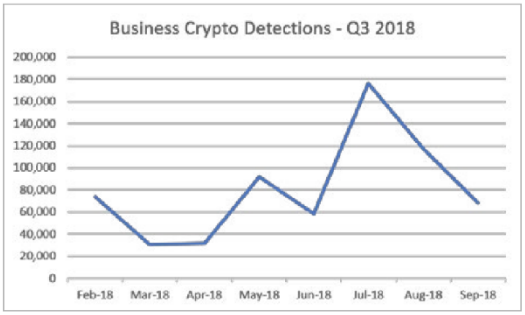




Además de la relativa invisibilidad del ataque, una ventaja del cryptojacking en relación con el ransomware, es que se consiguen beneficios sin que las víctimas tengan que hacer absolutamente nada (como, por ejemplo, pagar bitcoins a cambio de recuperar el acceso al sistema). Aunque todavía es demasiado pronto para decirlo, es posible que se esté asistiendo a una transición del ransomware tradicional al software dañino criptográfico.

La figura siguiente muestra la evolución del cryptojacking y del ransomware hasta el tercer trimestre de 2018[177].

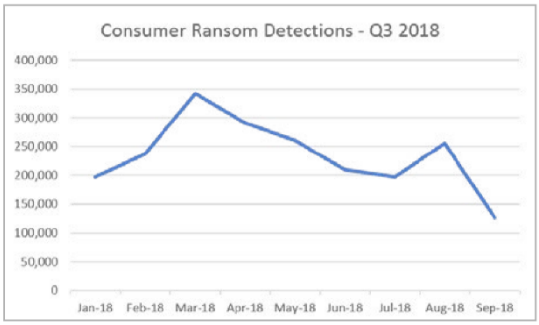


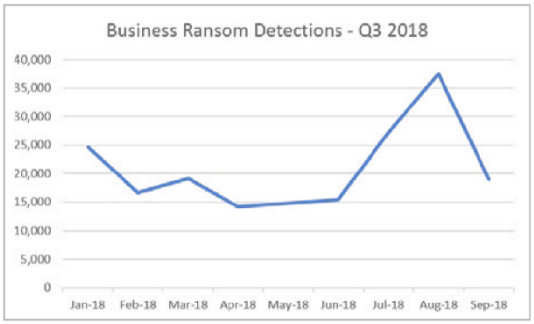


[175] Véase: Op. cit. Cisco-Talos.

[176] Véanse: Microsoft: Invisible resource thieves: The increasing threat of cryptocurrency miners (en https://cloudblogs.microsoft.com/microsoftsecure/2018/03/13/invisible-resource-thieves-the-increasing-threat-of-cryptocurrency-miners/) y Forbes: Top Cyberthreat Of 2018: Illicit Cryptomining (en https://www.forbes.com/sites/jasonbloomberg/2018/03/04/top-cyberthreat-of-2018-illicit-cryptomining/#2b751e975ae8)

[177] Véase: MalwareBytes Lab: Cybercrime tactics and techniques Q3 2018 (en https://resources.malwarebytes.com/files/2018/10/Malwarebytes_Cybercrime-Tactics-and-Techniques-Q3-2018.pdf)

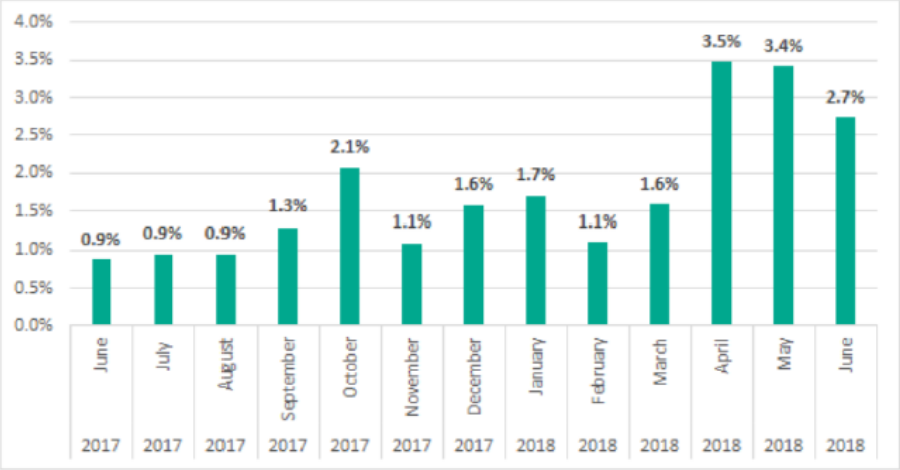




Hay que señalar que los servidores de las organizaciones suelen ser objetivos muy atractivos para los delincuentes debido a sus recursos, generalmente más grandes, y la permanente disponibilidad de los mismos. Se puede suponer que, en el futuro, se usarán otros objetivos y plataformas (por ejemplo, cámaras web, dispositivos domésticos inteligentes, etc.) lo que también obliga a su supervisión constante. Este es especialmente el caso, ya que los mineros criptográficos a menudo permanecen sin ser detectados en los sistemas afectados durante mucho tiempo y, dejando a un lado la disminución en el rendimiento y, posiblemente, el aumento del consumo de energía, el comportamiento de los equipos infectados puede seguir percibiéndose como normal. En todo caso, estas "anomalías" suelen ser tan marginales que no representan indicadores adecuados que le permitan pensar al usuario que está siendo atacado.

Finalmente, en febrero de 2018, se informó sobre el primer incidente de este tipo localizado en los sistemas SCADA de una empresa de servicios de agua[178], conectados a internet. Se trata de una preocupante tendencia general para la infraestructura crítica, porque podría tener un impacto en la estabilidad y la capacidad de respuesta de las operaciones de tales sistemas, como muestra la figura, que representa el porcentaje de sistemas ICS atacados por cryptomining[179] en el periodo mostrado.

[178] Ver: https://radiflow.com/case-studies/detection-of-a-crypto-mining-malware-attack-at-a-water-utility/
[179] Ver: https://securelist.com/threat-landscape-for-industrial-automation-systems-in-h1-2018/87913/

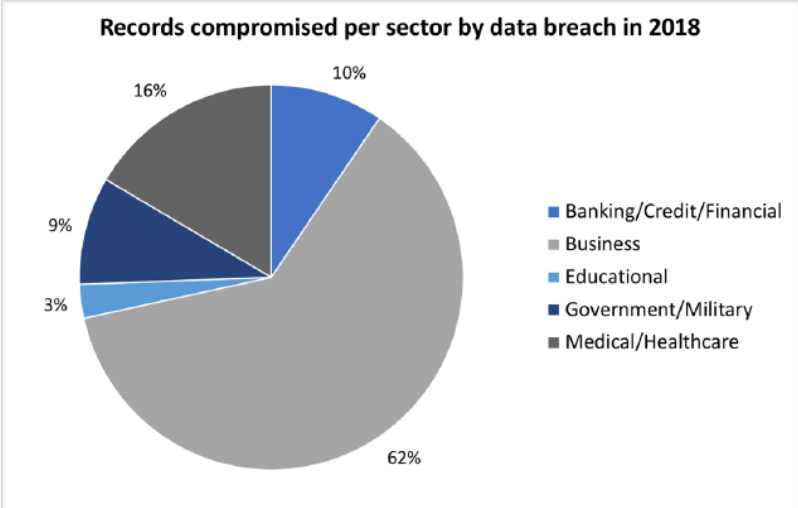


1.25. Robo de identidad

Esta actividad consiste en sustraer información de identificación personal, de manera masiva (que muchas veces incluye información relacionada con aspectos legales o civiles[180]: credenciales de cuentas bancarias, domicilios, registros contables, registros de salud, etc.) que son vulnerables a la actividad de los ciberatacantes.

Como se ha afirmado, el robo de identidad es un procedimiento más que un incidente aislado; los atacantes necesitan varios "elementos" o "piezas" de información personal para "construir" con precisión el perfil completo de una persona concreta. Si lo obtenido en un instante no es suficiente, los datos se intercambian entre los actores dañinos a través de la Dark Web[181].

La amenaza del robo de identidades está fuertemente asociada con las violaciones de datos en compañías u organizaciones en todas las parcelas de la industria.
La figura muestra el número de registros comprometidos durante 2018, en diferentes sectores[182].



[180] Véase: https://www.splunk.com/pdfs/ebooks/a-guide-to-fraud-in-the-real-world.pdf
[181] Véase: http://www.thecommentator.com/article/6849/nhs_trusts_misplace_10_000_patient_records_in_major_security_breach
[182] Fuente: https://www.idtheftcenter.org/images/breach/2018/ITRCBreachStatsReportSummary2018.pdf

Los aspectos más significativos relacionados con este tipo de acciones han sido en 2018 los siguientes:

- La plena aplicación del RGPD. En mayo de 2018 fue de plena aplicación el Reglamento General de Protección de Datos para todas las organizaciones de la Unión Europea. El RGPD define las normas y los requisitos para que los responsables de tratamiento establezcan políticas de protección de datos personales a nivel de los Estados miembros, cuyo incumplimiento puede acarrear significativas sanciones. Algunos de los elementos de tales políticas incluyen el cifrado de datos y la autenticación de doble factor.

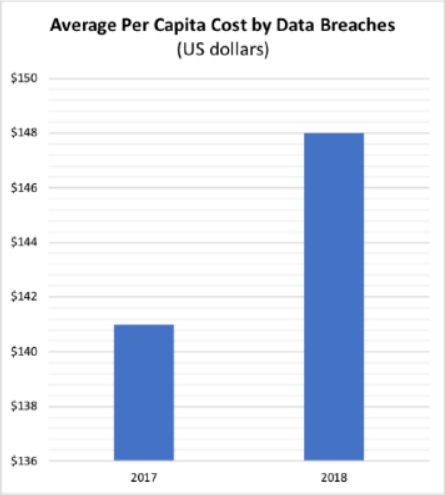
- Extensiones de software legítimas utilizadas en cibercampañas. En mayo de 2018 se hizo pública la campaña *Unimania*[183]. Se observó que a través de extensiones de Chrome (tales como Video Downloader para Facebook, con 170.000 usuarios, aproximadamente; el PDF Merge, con 25.000 usuarios, y otras instaladas en este navegador), se ha recopilado información personal basada en el comportamiento del usuario: mensajes, tweets, videos de YouTube, ID de usuario y datos de ubicación. Aunque el desarrollador es desconocido, el EULA mencionaba el nombre de la compañía Unimania, Inc., ubicada en Tel-Aviv, Israel. Más de 420.000 usuarios podrían estar afectados por este incidente.

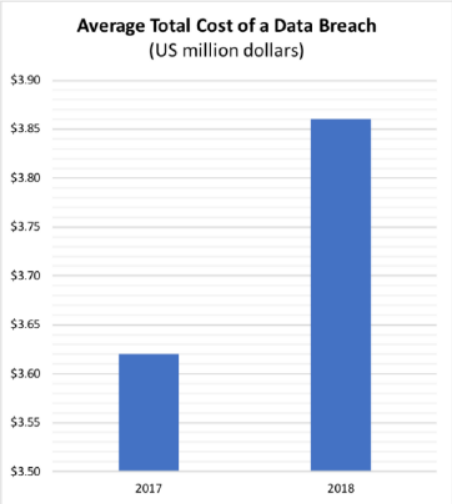
- En julio de 2018 se hizo pública la campaña *Big Star Labs*[184] que se distribuyó a través de Chrome y de otras extensiones de software legítimo, como *Block Site*, *AdBlockPrime* y varias aplicaciones más de Android e iOS, así como extensiones de Chrome y Firefox. La campaña *Big Star Labs* podría haber infectado a más de 11 millones de usuarios. Ciertas partes del código analizado señalaron la participación de una empresa de análisis web con sede en Israel.

- Filtraciones gubernamentales de datos. En septiembre de 2018, el canal de noticias norteamericano CNN informó sobre la exposición de datos personales (números de seguridad social, antecedentes penales, etc.) en el portal público FOIA.gov. El portal de la FOIA opera como intermediario entre los ciudadanos y agencias gubernamentales y procesa la información personal de los solicitantes. Un fallo en los servidores de FOIA.gov permitió búsquedas no autorizadas en sus registros sin el permiso de la agencia ni del solicitante.

[183] Ver: https://adguard.com/en/blog/unimania-spyware-campaign/
[184] Ver: https://adguard.com/en/blog/big-star-labs-spyware/

Las figuras siguientes muestran la evolución del coste medio de la pérdida de datos.





1.26. Ataques Web

7.11.1 Ataques basados en web

Este tipo de ataques se centra en los sistemas y servicios web para comprometer a la víctima, lo que comprende la explotación de los navegadores (incluidas sus extensiones), los sitios web, la explotación del sistema de gestión de contenido (CMS) y los propios servicios web. Los ataques *drive-by, waterhole, redirection y man-in-the-browser* son algunas de las categorías más conocidas de tales acciones.

Durante 2018, los ataques basados en la web siguieron siendo una de las amenazas más importantes, por su amplia difusión, que va desde campañas de spam relacionadas con anuncios, a troyanos bancarios[185], pasando por grupos de amenazas persistentes avanzadas (APT)[186].

Estas son algunas de las evidencias más significativas de este tipo de ataques durante 2018:

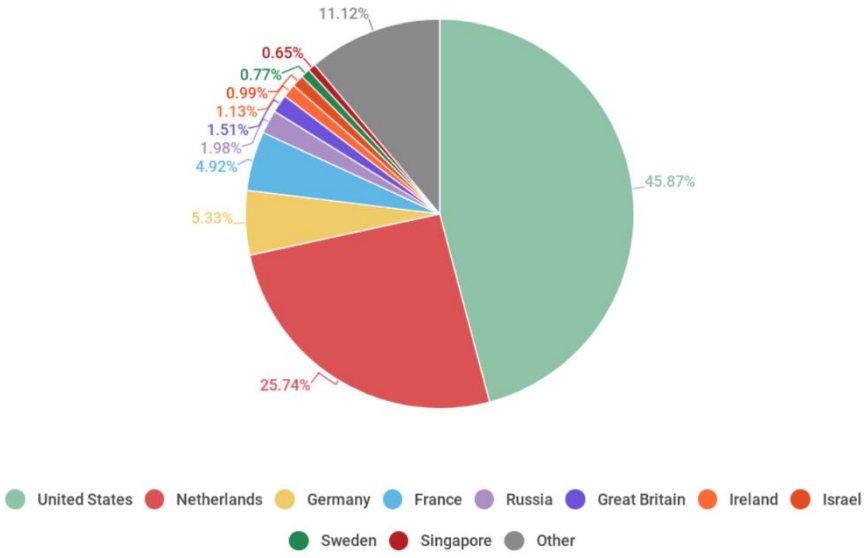
- APT, campañas de código dañino y ataques basados en *watering hole*. En marzo de 2018, una compañía de seguridad investigó a una importante empresa de telecomunicaciones en Hong Kong e identificó un flash exploit (CVE-2018-4878) en su sitio web corporativo; un buen ejemplo de ataques por watering hole[187].

[185] Véase: https://securelist.com/it-threat-evolution-q2-2018-statistics/87170/
[186] Véase: https://attack.mitre.org/techniques/T1189/
[187] Véase: https://blog.morphisec.com/watering-hole-attack-hong-kong-telecom-site-flash-exploit-cve-2018-4878

- Extensiones para navegadores. En junio de 2018, se identificó la extensión del navegador Chrome "Desbloquear Conteúdo", dirigida a los ciudadanos brasileños usuarios de banca online. Este ataque perseguía recopilar credenciales bancarias[188]. Además, se detectaron extensiones falsas que se hacían pasar por extensiones legítimas[189].
- Incremento de los compromisos relacionados con los sistemas de gestión de contenido (CMS). A principios de 2018 se observaron varios ataques contra Drupal que entregaban mineros de criptomonedas y herramientas de ingeniería social[190]. Más tarde, en septiembre de 2018, se evidenció una ola de ataques dirigidos a sitios de Wordpress vulnerables[191].
- Exploits kits basados en el navegador web (drive-by). Según el informe de primavera y verano de Malwarebytes, la mayoría de los exploits kits fueron detectados en Asia (especialmente, en Japón y Corea del Sur), lo que podría estar relacionado con el uso masivo de Internet Explorer en esta zona geográfica. Además, los investigadores observaron un aumento en las descargas ocultas etiquetadas como "pseudo exploit-kits". Este tipo de exploits kits no suele tener una infraestructura sólida y, frecuentemente, son el resultado de un único desarrollador que copia y pega desde exploits ya filtrados o de tipo POC[192].

La figura siguiente muestra la distribución por países de ataques basados en web en el segundo trimestre de 2018[193].

[188] Véase: https://securelist.com/a-mitm-extension-for-chrome/86057/
[189] Véase: https://thenextweb.com/hardfork/2018/09/05/mega-browser-extension-hacked-google/
[190] Véase: https://blog.malwarebytes.com/threat-analysis/2018/09/mass-wordpress-compromises-tech-support-scams/
[191] Véase: https://labs.sucuri.net/?note=2018-09-18
[192] Véase: https://blog.malwarebytes.com/threat-analysis/2018/08/exploit-kits-summer-2018-review/
[193] Fuente: https://securelist.com/it-threat-evolution-q2-2018-statistics/87170/



7.11.2 Ataques a aplicaciones web

Son intentos directos o indirectos de explotar vulnerabilidades en servicios y aplicaciones web, abusando de sus API, entornos de ejecución o servicios.

Aunque constituyen objetivos muy interesantes para los agentes de las amenazas, a medida que las organizaciones dependen cada vez más de los servicios web, tanto en lo relativo a los ingresos como en imagen, la frecuencia de este tipo de ataques ha disminuido ligeramente[194]. No obstante, permanecen como vectores muy peligrosos los denominados "ataques automatizados", que muestran capacidades de explotación más eficientes[195]. Dada la peligrosidad de este tipo de ataques, en 2018 las organizaciones han incrementado la inversión en sistemas de detección, protección y defensa de aplicaciones web[196].

Se señalan seguidamente las cuestiones más significativas de este tipo de ataques:

- *SQL injection* sigue liderando este tipo de ataques. Los ataques de SQLi en las organizaciones siguen siendo los mayoritarios en este tipo de acciones (51%) pese a ser la variante más conocida, tanto para los atacantes como para las víctimas.

[194] Véase: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q3-2018.pdf

[195] Véase: https://info.tcell.io/hubfs/DemandGen_Content/Research%20Papers/tCell_wp-stateofsecurity-2018-web.pdf

[196] Véanse: https://blogs.akamai.com/2018/06/summer-soti---web-attacks.html y https://cyber-edge.com/wp-content/uploads/2018/03/CyberEdge-2018-CDR.pdf

- La inclusión de archivos locales y el *cross-site-scripting* ocupan el segundo y tercer lugar entre los tipos de ataque más frecuentes, con un 34% y un 8%, respectivamente, de las acciones.
- Los denominados "códigos muertos" también conocidos como rutas/API huérfanas, son porciones obsoletas o abandonadas de aplicaciones web, que aumentan injustificadamente la superficie de ataque en sistemas interconectados[197].
- Si bien el volumen de vulnerabilidades críticas en las aplicaciones web aumenta cada año, no se ha apreciado un significativo incremento de las vulnerabilidades en el sector financiero, comercio minorista y atención sanitaria[198].
- Los ataques a aplicaciones legacy siguen estando en los puestos más altos. Según datos de Fortinet, las 20 primeras explotaciones de aplicaciones web con mayor prevalencia se remontan a 2005. La inyección de PHP es la segunda en la lista con un 33,6% (CVE-2012-2311, CVE-2012-1823)[199].

1.27. Botnets, IoT, IoT botnets y Android

El uso de botnets permite a los atacantes la penetración a gran escala en los sistemas de múltiples víctimas, buscando sustraer datos personales o acceder a recursos tales como la potencia de cálculo o el ancho de banda.

Dada la creciente profesionalización de las herramientas y los servicios de ataque, ya no es necesario que los atacantes construyan sus propias botnets, sino que pueden recurrir a soluciones ya desarrolladas que posibilitan el alquiler de capacidades de ataque de forma relativamente sencilla y económica.

El código dañino utilizado se diseña generalmente de forma modular y tiene la opción de descargar de manera flexible funcionalidades individuales desde el servidor de Mando y Control (C&C). Esto permite que una botnet cambie de forma dinámica o amplíe su propósito muy rápidamente.

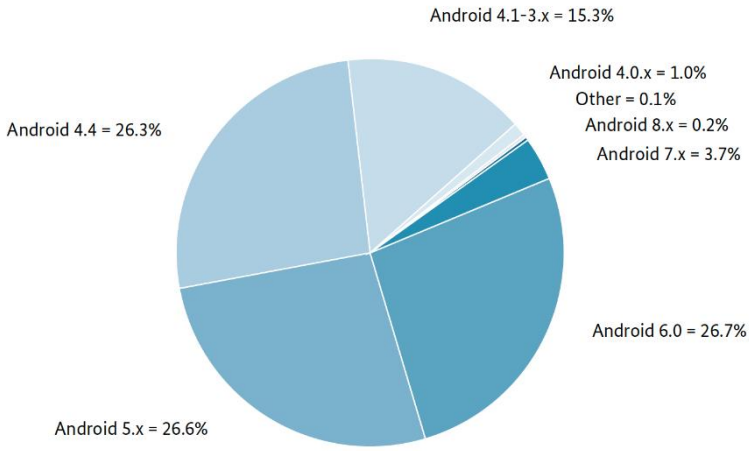
Como decimos, durante 2018, las botnets se utilizaron principalmente para el robo de información, ataques de denegación de servicio (DDoS) y para el envío de correo no deseado con código dañino. Lo más significativo ha sido el aumento en la aparición de botnets que comprometen dispositivos electrónicos del hogar conectados

[197] Véase: https://info.tcell.io/hubfs/DemandGen_Content/Research%20Papers/tCell_wp-stateofsecurity-2018-web.pdf,
[198] Véase: https://info.whitehatsec.com/rs/675-YBI-674/images/WhiteHatStatsReport2018.pdf
[199] Véase: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q3-2018.pdf

a internet, utilizándolos como bots. Se ha de recordar que, en agosto de 2016, la botnet *Mirai* fue la causante de la ejecución de ataques DDoS masivos, de un ancho de banda sin precedentes. A partir de ahí, han salido a la luz nuevas botnets de IoT, como *HNS (Hide 'N Seek*), que evidencian características nuevas: por ejemplo, el bot *HNS* podría anclarse permanentemente en una parte de los sistemas infectados y sobrevivir a los reinicios del dispositivo.

Todos estos ejemplos muestran que hay un desarrollo continuo en el área de programas de código dañino IoT, incrementando y refinando constantemente sus funcionalidades para comprometer y explotar sistemas vulnerables. A medida que crece la cantidad de dispositivos IoT conectados, se incrementa correlativamente la superficie de ataque.

Durante 2017 y 2018, las infecciones notificadas mundialmente se distribuyeron entre más de 130 familias diferentes de botnets. Es significativo que cada vez más botnets apuntan a sistemas Android (aproximadamente, un 25%), mientras que las infecciones restantes son, predominantemente, en sistemas Windows. El siguiente gráfico muestra una distribución de las versiones de dispositivos Android infectados utilizando una muestra tomada a finales de mayo de 2018 y procesada por la BSI alemana.



Un examen más detallado muestra que todas ellas tienen la funcionalidad de extraer información del dispositivo (tal como la *International Mobile Subscriber Identity (IMEI)*, su ubicación) o permiten la descarga posterior de código dañino adicional. Algunas de las instancias analizadas pueden acceder a los datos de banca online o pueden enviar SMS premium.

La mayoría de las infecciones para Android se deben a aplicaciones dañinas obtenidas de terceros. No obstante, también es posible la infección sin la intervención del usuario. Muchos fabricantes de sistemas Android entregan los dispositivos con una

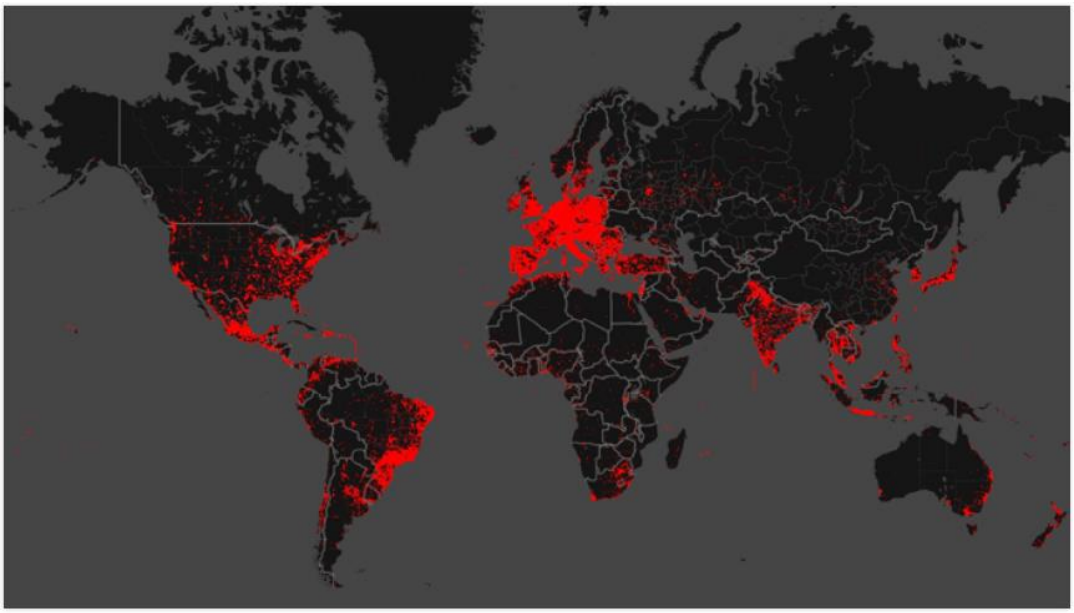
instalación de software desactualizada. A medida que envejecen, estos dispositivos ofrecen una mayor superficie de ataque al incrementarse las vulnerabilidades. Un ejemplo: la mayoría de los sistemas infectados analizados (>40%) todavía ejecutan una versión de Android 4, que no es soportada por Google desde hace tiempo. Las variantes más recientes (como Android 7, por ejemplo) solo representan el 3,7% de los casos. Los sistemas Android 8 infectados constituyen la parte más pequeña, con una penetración aproximada del 0.2%.

Como en años anteriores, los sistemas operativos infectados también incluyen servidores web basados en Linux y, en ocasiones, sistemas basados en Mac OS X.

La amenaza derivada de las botnets sigue siendo alta y se puede observar una reorientación hacia dispositivos móviles y dispositivos IoT, ampliando de este modo la superficie de ataque a millones de víctimas potenciales.

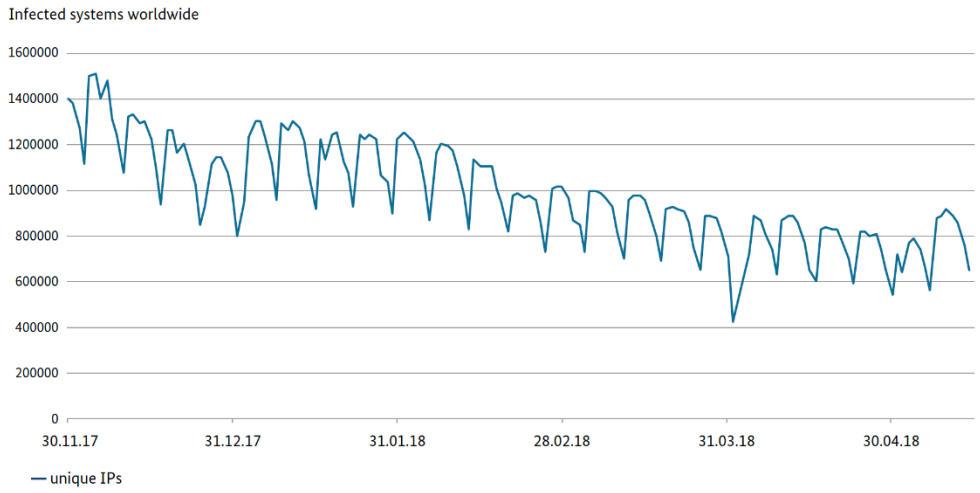
Los análisis de finales de 2017 evidenciaron que un gran número de sistemas en todo el mundo estaban infectados con el código dañino *Andrómeda* (también conocido como *Gamarue*). Los principales objetivos identificados de este malware se localizaron en Asia, América del Norte y Europa, particularmente, en Rumanía, Italia, Alemania y Polonia. Esta botnet global fue desactivada el 30 de noviembre de 2017 gracias la colaboración internacional. La autoridad judicial europea Eurojust coordinó las actividades de los fiscales involucrados en todo el mundo.

La figura siguiente muestra el despliegue de infecciones de *Gamarue* desde diciembre de 2017 a enero de 2018[200].



[200] Fuente: Microsoft Security Intelligence Report - VOLUME 23 – 2018.

El 5 de diciembre de 2017, se detectaron e informaron casi 1,5 millones de infecciones en todo el mundo, en un solo día. Hasta mediados de 2018 se ha evidenciado una caída del 42%.



Se debe resaltar que los routers y las cámaras conectadas son la principal fuente de los ataques, con un 90% de la actividad dañina.
La figura de la derecha muestra los diez dispositivos más atacados.

TOP DEVICE TYPES PERFORMING IOT ATTACKS (YEAR)

DEVICE TYPE	PERCENT
Router	75.2
Connected Camera	15.2
Multi Media Device	5.4
Firewall	2.1
PBX Phone System	0.6
NAS (Network Attached Storage)	0.6
VoIP phone	0.2
Printer	0.2
Alarm System	0.2
VoIP Adapter	0.1

1.28. Ataques DDoS

Como quiera que los ataques DDoS sigan siendo una de las amenazas más significativas, se ha evidenciado en las organizaciones un notable incremento de las acciones de prevención. Así lo demuestra el aumento de la demanda de proveedores de servicios gestionados de mitigación, especialmente en los sectores financieros, el comercio electrónico, los proveedores de servicios en la nube y los gobiernos[201]. Por otro lado, es de destacar la actividad de los cuerpos policiales en la lucha contra tales

[201] Véase: https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf

acciones, desmantelando servicios como "webstresser.org"[202], en el primer semestre de 2018.

Sea como fuere, pese a las actividades de mitigación desplegadas, las investigaciones señalan que el número de acciones DDoS sigue aumentando, en torno al 16%[203].

Algunas de las cuestiones más significativas en este tipo de ataques son:

- Herramientas para contrarrestar los ataques DDoS (BCP38). Las investigaciones sobre la implementación del filtrado del tráfico de entrada, al objeto de evitar la falsificación de direcciones IP en los ISP, es un enfoque adecuado que evita que la infraestructura de los ISP genere ataques DDoS desarrollando técnicas de spoofed-IP[204].
- Internet de servicios conectados. Varias investigaciones señalan que las API se están convirtiendo en una superficie de ataque muy popular entre los agentes de las amenazas. Una acción hostil contra tales tecnologías posibilitaría la interrupción de los servicios en diferentes organizaciones, incluso en sectores específicos, como el sanitario ("hospitales conectados" con 80.000 dispositivos médicos públicamente expuestos)[205].
- Ataques DDoS y geopolítica. Se han advertido ataques DDoS dirigidos contra autoridades o candidatos políticos en México (página web del candidato Ricardo Anaya) y Ucrania (presidente Poroshenko) y en Dinamarca (contra un proveedor de billetes de ferrocarril).
- Los ataques DDoS como servicio. El precio de estos proveedores para ejecutar ataques DDoS sencillos ronda los 5 dólares, variando su coste en función de las diferentes capacidades ofrecidas: ataques paralelos, límites por día y múltiples vectores de ataque. En abril de 2018, la National Crime Agency de UK, junto con la unidad de delitos holandesa (Dutch National High Tech Crime Unit) desmanteló una importante plataforma DDoS conocida como "webstresser.org" que albergaba a más de 136.000

[202] Véase: https://krebsonsecurity.com/2018/04/ddos-for-hire-service-webstresser-dismantled/

[203] Veáse: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-summer-2018-web-attack-report.pdf

[204] Véanse: https://www.caida.org/projects/spoofer/ y https://www.ncsc.gov.uk/content/files/protected_files/article_files/ACD%20-%20one%20year%20on_0.pdf

[205] Véase: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf

usuarios y que se había utilizado para iniciar entre 4 y 6 millones de ataques en todo el mundo[206].

- Ataques DDoS multivectoriales. Akamai informó sobre una serie de ataques específicos dirigidos a los servidores DNS durante casi dos días, de manera intermitente, que también incluía otro vector (basado en PSH / ACK - TCP) con un pico de 120 Gbps (18.6Mpps). Además, un actor malicioso introdujo un conjunto de generadores de tráfico en un tutorial de YouTube que podía alcanzar un máximo de 170 Gbps (65Mpps). Otros ataques multivectoriales utilizan incorrectamente los protocolos IKE e IPMI sustentan las teorías de que el código *Mira*" sigue usándose[207].
- IOT y ataques DDoS. Durante el primer trimestre de 2018 se observó un aumento en el número y la duración de los ataques DDoS detectados. Los investigadores de los laboratorios Kaspersky creen que estaban vinculados directamente con las botnets IoT de Darkai y AESDDoS. Además, en el tercer trimestre, Fortinet informó sobre la actividad de *Mirai* y *Gafgyt* después de recibir nuevas actualizaciones, además de la acción de la botnet *Bushido*, que se inspiró principalmente en la fuerza bruta de Mirai a través de dispositivos habilitados para telnet e IRC[208].

Los informes sobre ataques DDoS con anchos de banda record también se han producido el pasado año. Como hemos visto, en febrero de 2018, los atacantes descubrieron que se pueden lograr factores de amplificación muy altos utilizando *Memcached*. Arbor Networks reportó un ataque con un ancho de banda de 1.7 Tbps (1700 Gbps). Los ataques de esta magnitud son una seria amenaza. Hasta ahora, sin embargo, estas acciones son excepcionales. En los primeros cuatro meses de 2018, solo un pequeño porcentaje de los ataques superaron los 100 Gbps, estando la mayoría de ellos en torno a 1 Gbps. Si bien los datos relativos al ancho de banda, velocidad de los paquetes y duración varían mucho, los valores promedio son en gran medida constantes.

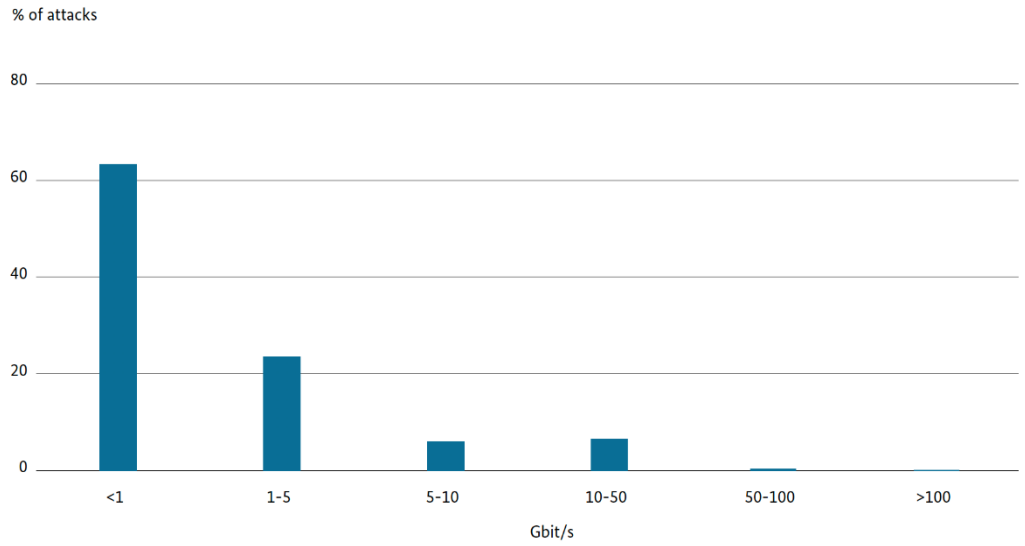
La figura siguiente muestra la distribución de ataques por ancho de banda, desde el 1 de enero al 30 de abril de 2018[209].

[206] Véanse: https://securitybrief.com.au/story/it-s-an-active-buyer-s-market-for-ddos-as-a-service-netscout y https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-summer-2018-web-attack-report.pdf

[207] Véase: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-summer-2018-web-attack-report.pdf

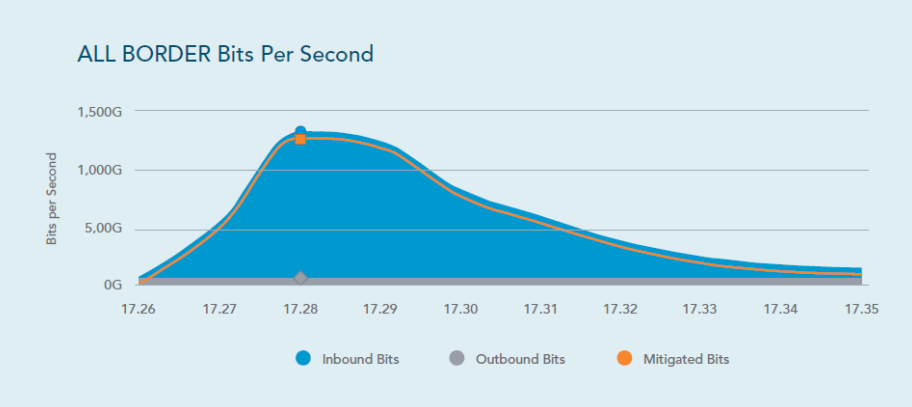
[208] Ver: https://securelist.com/ddos-report-in-q1-2018/85373/ y https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q3-2018.pdf

[209] Fuente: BSI, op. cit.



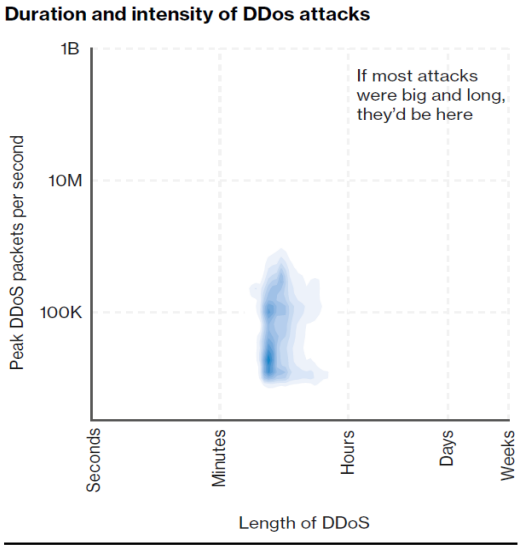
El ancho de banda por sí solo no es un indicador adecuado de la gravedad de un ataque DDoS. Con componentes tales como los balanceadores de carga o los cortafuegos, el factor limitante es, a menudo, la cantidad de paquetes que se pueden procesar. Los ataques en el nivel de aplicación, como las conexiones TCP o las solicitudes HTTPS, pueden causar daños significativos incluso con bajos anchos de banda y bajo ratio de paquetes.

La figura de la derecha muestra una gráfica del ataque DDoS sufrido por un cliente de Akamai el último día de febrero de 2018[210].

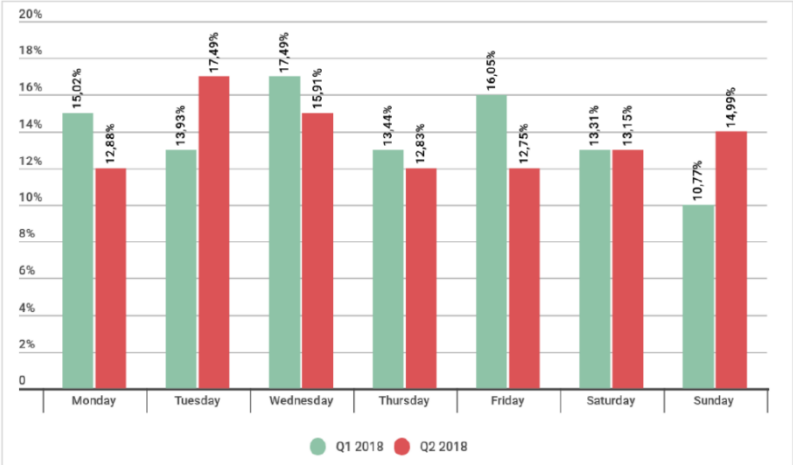


[210] Fuente: Akamai: SOTI 2018. State of the Internet / Security: A year in review.

Respecto de la duración (medida en segundos, minutos, horas, días o semanas) y la intensidad (medida en paquetes por segundo) de los ataques DDoS, la figura de la derecha muestra una estimación realizada por la empresa Verizon.

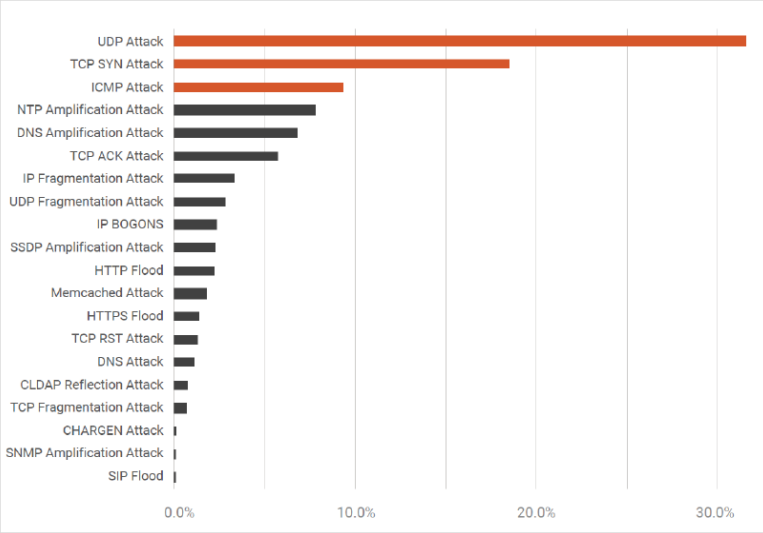


En este caso, la figura muestra una comparación de la distribución semanal de los ataques DDoS, entre el primer y el segundo trimestre de 2018[211].



[211] Ver: https://securelist.com/ddos-report-in-q2-2018/86537/

De acuerdo con el informe del segundo trimestre de 2018 de Nexusgaurd, la mayoría de los ataques usaron tácticas de ejecución rápida, siendo UDP, TCP (SYN) e inundaciones de ICMP los 3 principales vectores. La duración de estos ataques fue, en su mayoría, menor de 90 minutos, y el más largo, más de 6 días[212].



1.29. Criptografía

La tecnología criptográfica es esencial para la efectividad de muchos productos de seguridad IT. El estado del arte en materia criptográfica evidencia que métodos, como el cifrado simétrico AES o el intercambio de claves asimétrico Diffie-Hellman, ofrecen excelentes garantías de seguridad[213].

No obstante, son varios los aspectos que pueden hacer que un sistema criptográfico falle, entre ellos:

- Agujeros de seguridad en el hardware (por ejemplo, *Spectre* y *Meltdown*).
- Errores en las implementaciones.
- Errores a nivel de protocolo.
- Uso de estándares obsoletos (por ejemplo, *ROBOT*)
- Debilidades en la generación de claves (por ejemplo, *ROCA*)
- Inadecuados generadores de números aleatorios.

En la actualidad, existe una serie de procedimientos habituales de cifrado que permiten asumir que un atacante que pudiera tener acceso a los datos cifrados (criptograma) no podría calcular la clave secreta de cifrado o el texto en claro. Sin

ROCA
En noviembre de 2017, investigadores checos publicaron una vulnerabilidad en la generación de claves RSA utilizada en una librería criptográfica del fabricante de tarjetas inteligentes Infineon, con el título "Return of Coppersmith Attack" (ROCA). Para el cifrado o la firma RSA se requieren dos números

[212] Véase: https://www.nexusguard.com/hubfs/Threat%20Report%20Q2%202018/Nexusguard_DDoS_Threat_Report_Q2_2018_EN.pdf

embargo, si dicho atacante tiene acceso de red al dispositivo o está cerca de él, puede intentar recopilar información sobre determinados datos secretos, observando el comportamiento del dispositivo en términos de tiempos de cálculo, consumo de energía o emisiones electromagnéticas. Estos ataques, denominados de ***canal lateral,*** han venido siendo analizados durante mucho tiempo en relación con la construcción de sistemas de seguridad IT. La investigación intensiva sobre este tema ha producido una serie de contramedidas y nuevos vectores de ataque. El último desarrollo es el uso de técnicas de Aprendizaje Automático o *Machine Learning* (ML) para reconocer patrones en la medición de los datos.

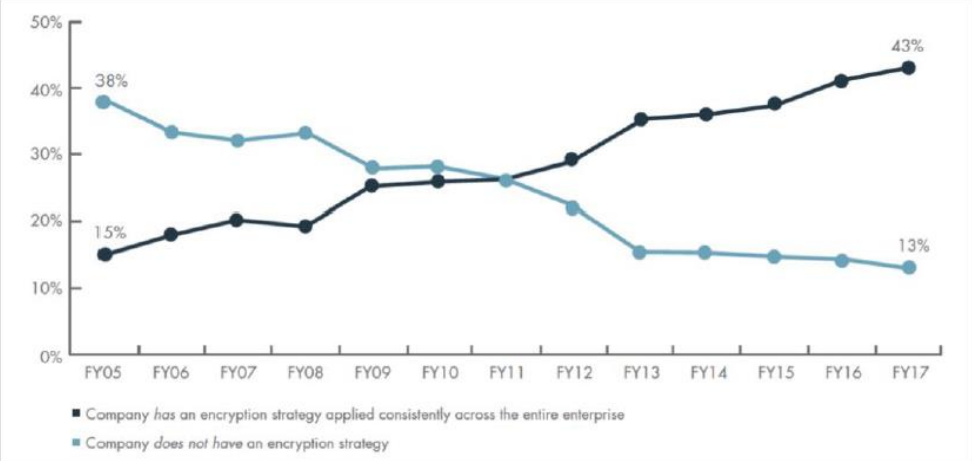
También llamado a estos efectos "reconocimiento de patrones", "minería de datos" o "inteligencia artificial", el ML, una herramienta muy utilizada en otras áreas TIC, aún no se ha popularizado como mecanismo para la perpetración de ataques, aunque -y así se contempla en todos los estudios de tendencias-, lo será claramente en un próximo futuro.

Otro requisito indispensable para el uso de los mecanismos criptográficos como elementos de seguridad, muy importante en la práctica, es la generación de números aleatorios que cumplan con ciertos criterios de calidad.

primos grandes y secretos (por ejemplo, 1024 bits) cuyo producto forma el módulo RSA. La librería de Infineon afectada compone números primos con una estructura muy especial, lo que significa que los números primos generados de esta manera pueden reconstruirse a partir del módulo público, utilizando un método desarrollado por Don Coppersmith en la década de 1990. La forma especial de los números primos también se transfiere al módulo, lo que permitiría determinar rápidamente si una clave RSA pública se habría generado de esta manera y, por lo tanto, si era o no vulnerable.
ROBOT El acrónimo ROBOT proviene de "Return of Bleichenbacher Oracle Threat". El ataque publicado por Hanno Böck, Juraj Somorovsky y Craig Young en diciembre de 2017 describe una vulnerabilidad en las actuales implementaciones TLS que utilizan cifrado RSA junto con un procedimiento obsoleto (PKCS#1 v1.5). El ataque, originariamente descrito por Daniel Bleichenbacher, tiene ya 20 años. Bleichenbacher había usado mensajes de error TLS como predicciones para determinar si el relleno (padding) de un mensaje era correcto o no. Usando un ataque adaptativo de texto cifrado, fue capaz de descifrar sucesivamente mensajes cifrados. Como resultado, el estándar TLS contiene recomendaciones sobre cómo pueden protegerse las implementaciones contra el ataque de Bleichenbacher. Los autores de ROBOT han demostrado que una gran cantidad de implementaciones de TLS son todavía vulnerables.

Según la encuesta de referencia[214], para muchos directivos de las empresas encuestadas, establecer una solución de cifrado para el almacenamiento es uno de los controles más efectivos en la protección de datos. La citada encuesta identificó que solo el 43% de las compañías tienen actualmente una estrategia de cifrado coherente para toda la empresa. El cumplimiento de las regulaciones (el RGPD, por ejemplo) es un importante motor para implementar tecnologías de cifrado. La figura siguiente muestra la tendencia en la adopción de las estrategias de cifra en las organizaciones[215].

[214] Véase: https://www.kroll.com/en-us/global-fraud-and-risk-report-2018
[215] Véase: https://www.thalesesecurity.com/2018/global-encryption-trends-study



Por otro lado, las garantías de seguridad de los mecanismos criptográficos utilizados en la actualidad podrán seguir aplicándose hasta que se disponga de una computadora cuántica "lo suficientemente grande" (medida en número de qubits lógicos entrelazados). Desde la década de 1990, se conocen algoritmos cuánticos que reducen a la mitad el nivel de seguridad de los métodos clásicos (algoritmo Grover para sistemas criptográficos simétricos) o que los rompen completamente (algoritmo Shor para sistemas criptográficos asimétricos). El algoritmo cuántico de Brassard, Hoyer y Tapp encuentra colisiones de una función hash de *n* bits después de aproximadamente 2^(*n*/3) pasos.

La criptografía post-cuántica ofrece una alternativa. Se trata de mecanismos criptográficos basados en problemas matemáticos que probablemente no pueden resolverse con una computadora cuántica. Sin embargo, no hay pruebas de la resistencia cuántica de estos métodos. A raíz de la perspectiva de desarrollo de un ordenador cuántico de potencia suficiente, las actividades de investigación y estandarización en el campo de la criptografía post-cuántica han aumentado enormemente en los últimos años[216].

1.30. El impacto económico de los ciberataques

Según estimaciones de McAfee[217], el ciberdelito, en la actualidad, puede estar representando un coste mundial cercano a los 600.000 millones de dólares (o el 0,8% del PIB mundial). Se apuntan las siguientes razones para su crecimiento:

[216] Para conocer el estado de las investigaciones sobre criptografía cuántica puede consultarse el estudio "Development of Quantum Computer", encargado por la BSI alemana a investigadores de las Universidades Saarland y Florida Atlantic. El informe examina en detalle los enfoques tecnológicos actuales y las innovaciones algorítmicas cuánticas y analiza sus implicaciones en el contexto de los mecanismos de clave pública actualmente en uso. (El estudio y un resumen se pueden descargar del sitio web de BSI en http://www.bsi.bund.de/qcstudie).

[217] Ver: Economic Impact of Cybercrime—No Slowing Down. CSIS. February 2018

- Rápida adopción de nuevas tecnologías por parte de los ciberdelincuentes.
- Mayor número de usuarios nuevos en línea (que tienden a ser de países de bajos ingresos, con escasa o nula ciberseguridad)
- Mayor facilidad para cometer delitos informáticos, aprovechando el crecimiento de los delitos *as-a-service*.
- Número creciente de "polos" de ciberdelincuencia, que ahora también incluyen a Brasil, India, Corea del Norte y Vietnam.
- Creciente sofisticación financiera entre los cibercriminales de primer nivel, lo que, entre otras cosas, facilita la monetización.

La figura siguiente muestra la actividad económica diaria estimada del cibercrimen.

Cybercrime	Estimated Daily Activity
Malicious scans	80 billion
New malware	300,000
Phishing	33,000
Ransomware	4,000
Records lost to hacking	780,000

La actividad delictiva en Internet es mucho más amplia que el mero ciberdelito económico, ya que, esencialmente, todos los elementos de la actividad delictiva humana se han trasladado al ciberespacio. Un alto funcionario británico informó, por ejemplo, de que la mitad de todos los delitos denunciados en el Reino Unido están relacionados, directa o indirectamente, con el ciberespacio. Algunos ejemplos son:

- Pérdida de propiedad intelectual e información comercial confidencial.
- Fraude en línea y delitos financieros, a menudo como resultado de información de identificación personal (PII) sustraída.
- Manipulación financiera, mediante el uso de información empresarial confidencial robada en fusiones potenciales o conocimiento avanzado de informes de rendimiento para empresas que cotizan en bolsa.
- Costos de oportunidad, incluida la interrupción en la producción o los servicios, y una menor confianza para las actividades en línea.
- El coste de proteger redes, adquirir pólizas de ciberseguros y pagar por la recuperación de los ciberataques.

- Daños en la reputación y riesgo de responsabilidad para la empresa atacada y su marca, incluido el daño temporal al valor de las acciones.

El cuadro siguiente muestra la distribución regional de los ciberataques, en términos económicos, durante 2017.

Region (World Bank)	Region GDP (USD, trillions)	Cybercrime Cost (USD, billions)	Cybercrime Loss (% GDP)
North America	20.2	140 to 175	0.69 to 0.87%
Europe and Central Asia	20.3	160 to 180	0.79 to 0.89%
East Asia & the Pacific	22.5	120 to 200	0.53 to 0.89%
South Asia	2.9	7 to 15	0.24 to 0.52%
Latin America and the Caribbean	5.3	15 to 30	0.28 to 0.57%
Sub-Saharan Africa	1.5	1 to 3	0.07 to 0.20%
MENA	3.1	2 to 5	0.06 to 0.16%
World	**$75.8**	**$445 to $608**	**0.59 to 0.80%**

8. Medidas

Este epígrafe describe las principales medidas adoptadas, en el periodo considerado, para prevenir los ataques o mitigar sus efectos.

1.31. La necesidad de implantar las adecuadas medidas de seguridad

Aun cuando la adopción de adecuadas medidas de seguridad hacen más resilientes a las organizaciones frente a los ciberataques, la descripción de los incidentes ocurridos en el periodo considerado, revelan que las organizaciones no siempre implementan, tan siquiera, las medidas más básicas que podrían haber prevenido o mitigado el daño causado. Un par de ejemplos: ataques como *WannaCry* o *BadRabbit*, explotaron vulnerabilidades conocidas. Las actualizaciones para estas vulnerabilidades habían estado disponibles durante meses pero no se habían instalado

en las organizaciones afectadas[218]. En otros casos, aunque las vulnerabilidades eran desconocidas, la adopción de las medidas de seguridad más elementales habrían supuesto un impedimento para el ataque o habrían mitigado sus efectos.

La ausencia de medidas de seguridad se extiende también a los teléfonos móviles. Por ejemplo, los proveedores de teléfonos Android suelen ser muy lentos en lo relativo a la implementación de las actualizaciones de seguridad, lo que obliga a las organizaciones a adoptar acuerdos corporativos con tales fabricantes, so pena de correr el riesgo de que el producto quede obsoleto tan pronto como se ponga en uso.

Por otro lado, el hecho de que los ciberataques permanezcan sin ser detectados durante mucho tiempo puede ser evidencia de que las medidas básicas no están correctamente implementadas. Recientes investigaciones han revelado que las empresas, los gobiernos y las organizaciones en Europa, frecuentemente, solo descubren que han sido víctimas de un ciberataque meses después[219].

Como ha señalado el CSAN[220], hay varias razones, internas o externas, por las que las organizaciones no siempre implementan las medidas adecuadas. Un ejemplo es la creciente escasez de especialistas en ciberseguridad en el mercado laboral. En otros casos, algunas organizaciones sienten que los ciberataques “no les puede pasar a ellos” y solo adoptan las medidas cuando han sido víctimas.

1.32. El mantenimiento de la resiliencia y la revelación de vulnerabilidades

La imparable interconexión de los sistemas y su creciente complejidad hacen más difícil alcanzar una infraestructura digital resiliente. Por otro lado, el incesante uso de sistemas y servicios en la nube y la utilización de servicios compartidos dificultan poseer una visión general de la infraestructura utilizada.

Todo ello hace que, mientras que la responsabilidad última de la seguridad permanece en la organización, la implementación práctica de los servicios se encuentra fragmentada en distintos sistemas de información interdependientes, de dispar robustez, suministrados por distintos responsables y sometidos a criterios de seguridad diferentes, incrementando la complejidad para mantener la seguridad global.

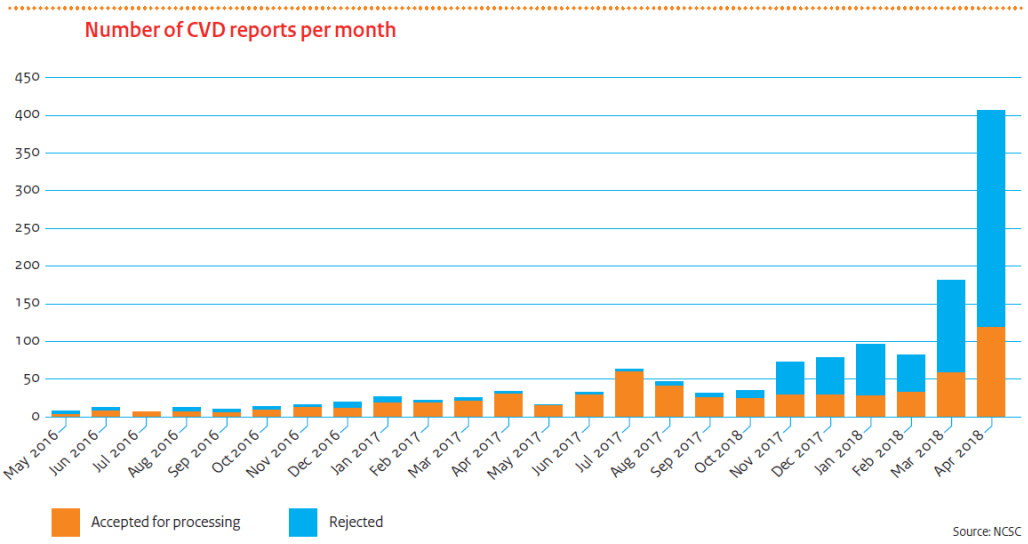
A todo ello hay que añadir la escasa importancia que, frecuentemente, se concede al desarrollo de software seguro o a la utilización de versiones actualizadas de

[218] Véase: The Register: 74 countries hit by NSA-powered WannaCrypt ransomware backdoor: Emergency fixes emitted by Microsoft for WinXP+ (en https://www.theregister.co.uk/2017/05/13/wannacrypt_ransomware_worm)
[219] Véase: De Telegraaf: ’Cyberaanval pas na half jaar ontdekt’ (‘Ciberataque descubierto después de seis meses'), (en https://www.telegraaf.nl/nieuws/1905093/cyberaanval-pas-na-half-jaar-ontdekt)
[220] Fuente NCSC: CSAN 2918.

de software. Por ejemplo, ciertos protocolos tienen décadas de antigüedad, habiéndose demostrado que no son capaces de resistir ciberataques realizados con técnicas actuales. Las versiones, mejoradas, de anteriores estándares de Internet (como IPv6 o HTTPS) se están adoptando muy lentamente, lo que conlleva que el uso de sus versiones anteriores (IPv4 y HTTP) permanezca como un problema latente.

Se han de resaltar también las vulnerabilidades de la cadena de suministro, como elemento de riesgo: los incidentes originados en algún lugar de la cadena pueden transmitirse a otros eslabones, situación que obedece a la relativa independencia con la que cada proveedor determina el nivel de seguridad de la parte que le corresponde y, en su consecuencia, las medidas de seguridad que adopta. Lo que es óptimo para un proveedor concreto puede no serlo para los clientes a los que atiende o al contrario.

Desde hace algunos años, ciertos Estados y organizaciones privadas han desarrollado mecanismos de **Revelación Responsable de Vulnerabilidades**, también llamada Divulgación Coordinada de Vulnerabilidades, como un procedimiento idóneo para aunar los intereses de los investigadores de seguridad y las organizaciones. El National Ciber Security Centre holandés ha hecho públicas las estadísticas sobre Divulgación Coordinada de Vulnerabilidades desde mayo de 2017 a abril de 2018[221].

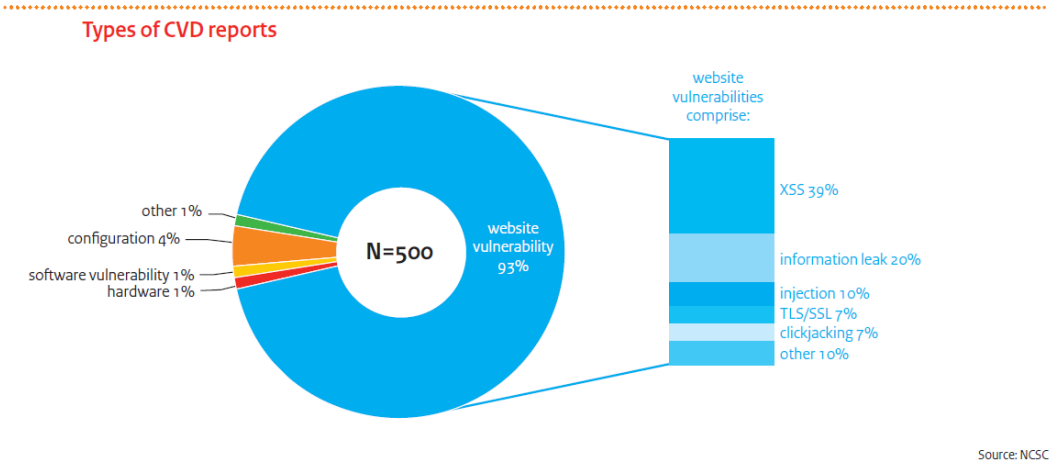


Como se desprende de la figura, se rechaza un importante número de informes sobre vulnerabilidades, y existen varias razones para ello, como puede ser la recepción de vulnerabilidades relacionadas con organizaciones que no se encuentran en el ámbito acordado. También se rechaza un informe si, tras una investigación previa, se detecta que realmente no existe tal vulnerabilidad o que el riesgo de seguridad es

[221] Véase: NCSC – CSAN 2018.

insignificante. Además, un informe puede ser rechazado si la misma vulnerabilidad ha sido notificada anteriormente, para el mismo sistema.

La figura siguiente muestra la distribución de vulnerabilidades, por tipo.



La inmensa mayoría (93%) de los informes recibidos por el NCSC holandés se refieren a vulnerabilidades en sitios web, aplicaciones web o infraestructuras en las que se ejecutan aplicaciones web (habitualmente, parámetros TLS débiles, cross site scripting (XSS), inyección de SQL, XML y HTML y fugas de información). Solo el 4% de todos los informes se refieren a errores de configuración en el hardware o software. Finalmente, pocos informes versan sobre vulnerabilidades en software o hardware (excluyendo servidores web y aplicaciones web).

1.33. El marco estratégico y legal

El año 2018 ha sido testigo del desarrollo y/o entrada en vigor de varias iniciativas legales, europeas y nacionales, en aspectos relacionados con la ciberseguridad. Repasamos las más significativas.

1) Estrategia de Ciberseguridad Nacional

En 2018 comenzaron los trabajos para la actualización de la Estrategia de Ciberseguridad Nacional de 2013, cuya elaboración se sustenta en lo dispuesto en la **Orden PCI/870/2018, de 3 de agosto, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba el procedimiento para la elaboración de una nueva Estrategia de Ciberseguridad Nacional.**

Dicho procedimiento confiere al **Consejo de Seguridad Nacional** (cuyas competencias están reguladas en la Orden PRA73372012, de 22 de enero) la responsabilidad de su redacción. De él depende el Consejo Nacional de Ciberseguridad

que, a su vez, contará con un **Comité técnico,** integrado por representantes de la Administración, y un **Comité de expertos** independientes.

Así pues, el Consejo Nacional de Ciberseguridad, bajo la presidencia del secretario de Estado-Director del Centro Nacional de Inteligencia (CNI) es el órgano encargado del proceso de formulación de la Estrategia de Ciberseguridad Nacional.

El **Comité técnico** está integrado por representantes del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación; Ministerio de Industria, Comercio y Turismo; Ministerio de Ciencia, Innovación y Universidades; por el Centro Nacional de Inteligencia (CNI); Mando Conjunto de Ciberdefensa (MCCD); Centro Nacional de Protección de Infraestructuras Críticas y Ciberseguridad (CNPIC); Instituto Nacional de Ciberseguridad (INCIBE); Secretaría de Estado para la Sociedad de la Información y la Agenda Digital (SESIAD); Secretaría General de Administración Digital y Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno. Igualmente podrán ser parte del Comité representantes de algún otro organismo de la Administración que el Consejo Nacional de Ciberseguridad considere necesario.

El **Comité de expertos** independientes está compuesto por representantes de los sectores público y privado, de la sociedad civil y de la Academia, caracterizados por su experiencia y formación jurídica, técnica y científica en el ámbito de la ciberseguridad, al objeto de oír su parecer acerca del borrador de estrategia y recibir sus aportaciones para su análisis y, en su caso, incorporación al documento.

Finalmente, el **Departamento de Seguridad Nacional,** del Gabinete de la Presidencia del Gobierno, dirige y coordina el trabajo del Comité técnico y del Comité de expertos independientes.

2) El 25 de mayo de 2018 se produjo la plena aplicación del **Reglamento (UE) 2016/679 del Parlamento Europeo y del consejo, de 27 de abril de 2016,** relativo a la protección de las personas físicas en lo que respecta al **tratamiento de datos personales** y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

3) Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

El Boletín Oficial del Estado publicaba esta norma, cumpliendo el mandato de latransposición de la **Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016,** relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

Aunque la Directiva Europea limitaba su ámbito de aplicación a los denominados “operadores de servicios esenciales” y los “proveedores de servicios digitales”, la

norma española ha ampliado su alcance a sectores no expresamente incluidos en la Directiva, como los prestadores de servicios de confianza o de comunicaciones electrónicas, que entran a formar parte de los destinatarios de la norma, en cuanto puedan ser designados operadores críticos.

Conviene señalar el esfuerzo desarrollado por el grupo de trabajo de redacción del RD-ley para cohonestar tres normas estatales en materia de ciberseguridad: el **Real Decreto 3/2010**, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS), la **Ley 8/2011, de 28 de abril**, por la que se establecen medidas para la protección de las Infraestructuras Críticas y la **Ley 36/2015**, de 28 de septiembre, de Seguridad Nacional. Estas tres regulaciones constituyen los pilares funcionales del nuevo Real Decreto-ley, cuyo desarrollo reglamentario deberá tener en cuenta para la determinación de los servicios esenciales (y sus operadores) concernidos.

El **modelo de gobernanza** recogido en el nuevo RD-ley se sustenta en el esquema de competencias que las vigentes Estrategias de Seguridad y Ciberseguridad Nacional han dibujado:

- Consejo de Seguridad Nacional, punto de contacto español para el resto de la UE.
- Consejo Nacional de Ciberseguridad, órgano colegiado de apoyo al Consejo de Seguridad Nacional en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, creado por Acuerdo del Consejo de Seguridad Nacional del 5 de diciembre de 2013, cuya presidencia ostenta el Secretario de Estado – Director del Centro Nacional de Inteligencia.
- Autoridades Competentes, por razón de los sectores implicados destinatarios de la norma.
- CSIRT de referencia, por razón de sus funciones legales para cada una de sus comunidades competenciales.

Estos CSIRT de referencia constituyen la piedra angular sobre la que descansa el tratamiento de la ciberseguridad, pues materializan los mecanismos de prevención, detección y respuesta a los incidentes, funciones que, a partir de la entrada en vigor del RD-ley, exigen de todos ellos la máxima coordinación. La norma confiere al CCN-CERT (del Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia) la función de coordinador nacional en los supuestos de especial gravedad.

			CSIRT DE REFERENCIA		AUTORIDAD COMPETENTE
OPERADORES DE SERVICIOS ESENCIALES	ES OPERADOR CRÍTICO	Pertenece al Sector Público	CCN-CERT	ESPDEF-CERT Cooperación o incidencia en la Defensa Nacional. (Requiere desarrollo reglamentario)	CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD (CNPIC) (Secretaría de Estado de Seguridad – M. Interior)
		No pertenece al Sector Público	INCIBE-CERT		
	NO ES OPERADOR CRÍTICO	Pertenece al Sector Público	CCN-CERT		CENTRO CRIPTOLÓGICO NACIONAL (CCN) (Ministerio de Defensa)
		No pertenece al Sector Público	INCIBE-CERT		AUTORIDAD SECTORIAL CORRESPONDIENTE (Requiere desarrollo reglamentario)
PROVEEDORES DE SERVICIOS DIGITALES	ES OPERADOR CRÍTICO	Pertenece al Sector Público	CCN-CERT		CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD (CNPIC) (Secretaría de Estado de Seguridad – M. Interior)
		No pertenece al Sector Público	INCIBE-CERT		
	NO ES OPERADOR CRÍTICO	Pertenece al Sector Público	CCN-CERT		CENTRO CRIPTOLÓGICO NACIONAL (CCN) (Ministerio de Defensa)
		No pertenece al Sector Público	INCIBE-CERT		SECRETARIA DE ESTADO PARA EL AVANCE DIGITAL (Ministerio de Economía y Empresa)

Al tiempo de redactar estas páginas, se está trabajando en la elaboración del Reglamento de Desarrollo de este Real Decreto-ley.

4) Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad

La Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad establece los criterios y procedimientos para la notificación por parte de las entidades que forman parte de los ámbitos subjetivos de aplicación de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, al Centro Criptológico Nacional (CCN) de aquellos incidentes que tengan un impacto significativo en la seguridad de la información que manejan y los servicios que prestan en relación con la categoría del sistema, al objeto de poder dar adecuada respuesta al mandato del Capítulo VII, Respuesta a incidentes de seguridad, del Real Decreto 3/2010, de 8 de enero.

5) Cybersecurity Act

Propuesta en 2017 como parte de un amplio conjunto de medidas para hacer frente a los ciberataques y construir una robusta ciberseguridad en la UE, la denominada *Cibersecurity Act* incluye:

- Un mandato permanente para la Agencia de Ciberseguridad de la UE, ENISA, para reemplazar su mandato limitado que habría expirado en 2020, así como más recursos asignados a la agencia para permitirle cumplir sus objetivos.
- Una base más sólida para ENISA en el nuevo marco de certificación de seguridad cibernética para ayudar a los Estados miembros a responder eficazmente a los ataques cibernéticos con un mayor papel en la cooperación y coordinación a nivel de la Unión.

Además, ENISA ayudará a aumentar las capacidades de seguridad cibernética a nivel de la UE y apoyará la creación y preparación de capacidades. Asimismo, será un centro de experiencia independiente que ayudará a promover un alto nivel de concienciación de los ciudadanos y las empresas, pero también ayudará a las instituciones de la UE y los Estados miembros en el desarrollo y la implementación de políticas.

La Cibersecurity Act crea también un marco para los certificados europeos de ciberseguridad para productos, procesos y servicios que serán válidos en toda la UE. Es la primera ley del mercado interno que asume el reto de mejorar la seguridad de los productos conectados, los dispositivos de Internet de las cosas y la infraestructura crítica a través de dichos certificados. Dicho marco de certificación incorpora características de seguridad en las primeras etapas de su diseño y desarrollo técnico (seguridad por diseño). También permite a sus usuarios determinar el nivel de garantía de seguridad y garantiza que estas características de seguridad se verifiquen de forma independiente.

Esta norma se encuentra actualmente en discusión por el Parlamento y el Consejo.

6) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

El Reglamento General de Protección de Datos ha supuesto la revisión de las bases legales del modelo europeo de protección de datos. Refuerza la seguridad jurídica y la transparencia a la vez que permite que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros. Contiene un amplio número de habilitaciones a los Estados miembros, a fin de regular determinadas materias, permitiendo incluso en su considerando 8 que, cuando sus normas deban ser especificadas, interpretadas o, excepcionalmente, restringidas por el Derecho de los Estados miembros, estos tengan la posibilidad de incorporar al derecho nacional previsiones contenidas específicamente en el Reglamento, en la medida en que sea necesario por razones de coherencia y comprensión.

La adaptación al Reglamento general de protección de datos, aplicable desde el 25 de mayo de 2018, según establece su artículo 99, requirió la elaboración de una nueva ley orgánica que sustituya a la anterior. En esta labor se han preservado los principios de buena regulación, al tratarse de una norma necesaria para la adaptación del ordenamiento español a la citada disposición europea y proporcional a este objetivo, siendo su razón última procurar seguridad jurídica.

Merece destacarse la importancia que le confiere esta nueva Ley Orgánica al **Esquema Nacional de Seguridad** (ENS) en su Disposición adicional primera, señalando que el ENS incluirá las medidas que deban implantarse en caso de tratamiento de

datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679; y extendiendo su aplicación a: a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos; b) Los órganos jurisdiccionales; c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local, d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas; e) Las autoridades administrativas independientes; f) El Banco de España, g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público; h) Las fundaciones del sector público; i) Las Universidades Públicas; j) Los consorcios y k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

Todas estas entidades deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

Finalmente, en los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al ENS.

7) Propuesta de Reglamento para poner en común recursos y conocimientos técnicos en tecnologías de ciberseguridad[222].

La Comisión plantea crear una Red de Centros de Competencia en Ciberseguridad con el fin de canalizar y coordinar mejor la financiación disponible para la cooperación, investigación e innovación en materia de ciberseguridad. Un nuevo Centro Europeo de Competencia en Ciberseguridad gestionará la ayuda económica con cargo al presupuesto de la UE destinado a ciberseguridad, lo que fomentará la inversión conjunta de la Unión, los Estados miembros y empresas del sector para fortalecer la industria de ciberseguridad de la UE y asegurar que los sistemas de defensa incorporen las técnicas más avanzadas[223].

8) El acceso a pruebas electrónicas

En abril de 2018, la CE propuso dos normas para facilitar a las autoridades policiales y judiciales la obtención de pruebas electrónicas necesarias para investigar y

[222] Propuesta para una "Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres", COM (2018) 630, de 12 de septiembre.

[223] Fuente: Evolución de la agenda de ciberseguridad de la Unión Europea. Javier Alonso Lecuit. ARI 121/2018 - 13/11/2018.

enjuiciar a delincuentes individualizados y a organizaciones terroristas. Tales normas son un reglamento para el acceso transfronterizo a pruebas electrónicas (e-evidence) y una directiva que lo complementa con el propósito de armonizar la designación de los representantes legales de las compañías en línea[224].

9) Consejo de Certificación del Esquema Nacional de seguridad (CoCENS)

El desarrollo y la expedición de las Certificaciones de Conformidad con el ENS, tal y como se encuentran regulados en la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, exige el concurso coordinado de diferentes actores y elementos. Por este motivo, en 2018, se ha constituido el Consejo de Certificación del Esquema Nacional de Seguridad (CoCENS), compuesto por representantes de todas las partes involucradas: Entidad Nacional de Acreditación (ENAC), Ministerio de Hacienda y Función Pública, Agencia Española de Protección de Datos, Centro Criptológico Nacional y todas las Entidades de Certificación del ENS, públicas y privadas.

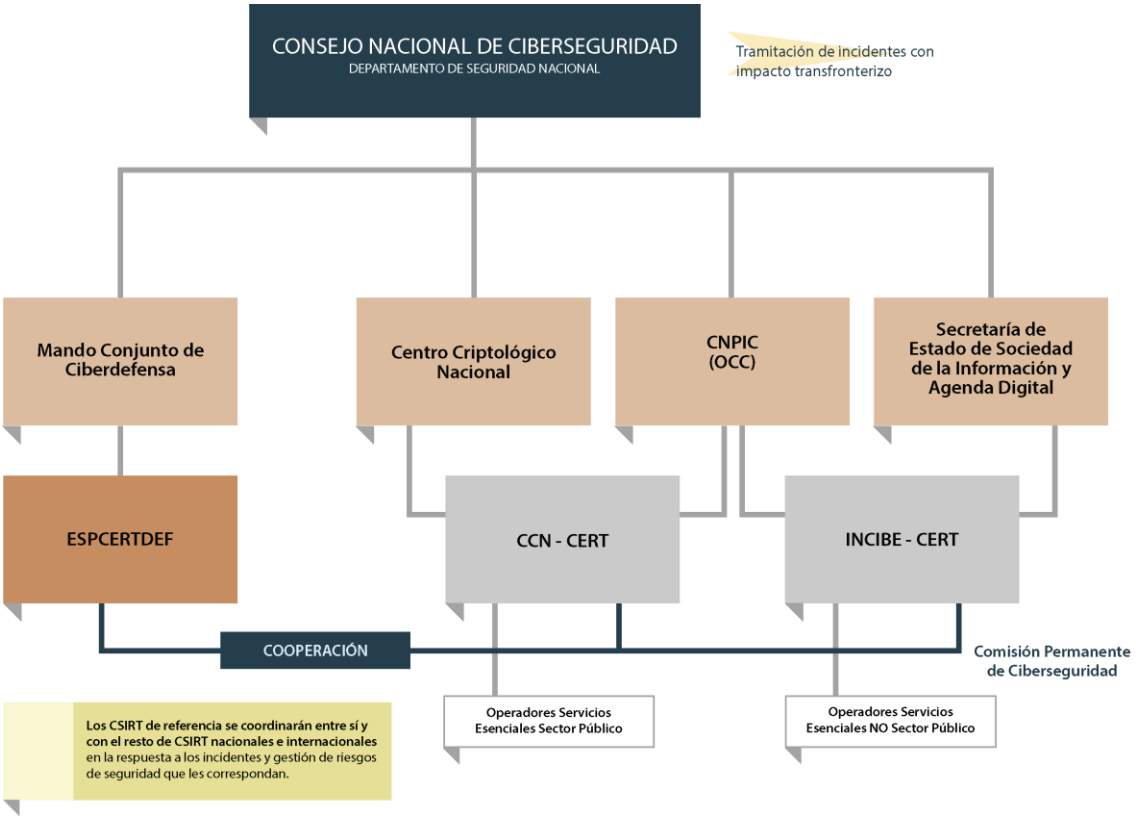
1.34. La actividad del Centro Criptológico Nacional (CCN)

Las competencias del Centro Criptológico Nacional, CCN, se encuentran recogidas en varias normas legales: la Ley 11/2002, reguladora del Centro Nacional de Inteligencia; el Real Decreto 421/2004, regulador del CCN; el Real Decreto 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por RD 951/2015, de 23 de octubre y, más recientemente, por lo dispuesto en el RD-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, como consecuencia de la transposición de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

El papel del CCN en el despliegue de la ciberseguridad española

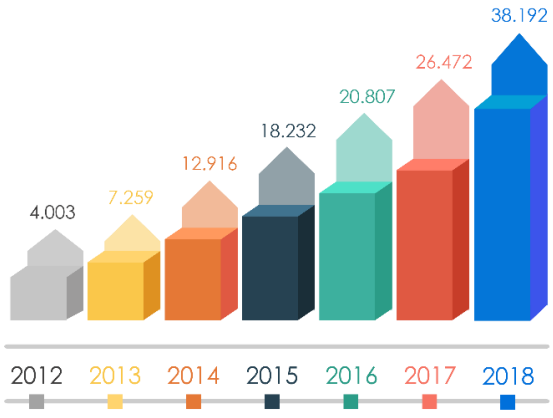
Tomando como referencia lo dispuesto en esta última norma (RD-ley 12/2018), puede desarrollarse el marco simplificado nacional de competencias en materia de ciberseguridad que recoge la figura siguiente, en el que el CCN-CERT, del Centro Criptológico Nacional, se configura como coordinador nacional en la gestión de incidentes

[224] Propuesta para la "Regulation on European Production and Preservation Orders for electronic evidence in criminal matters", COM (2018) 225, de 17 de abril, y propuesta para una "Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM (2018) 226, de 17 de abril.

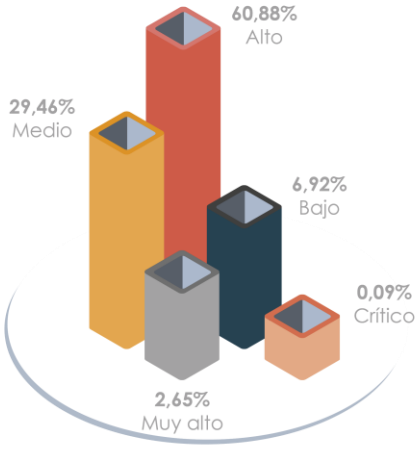


1.1.1. Gestión de incidentes

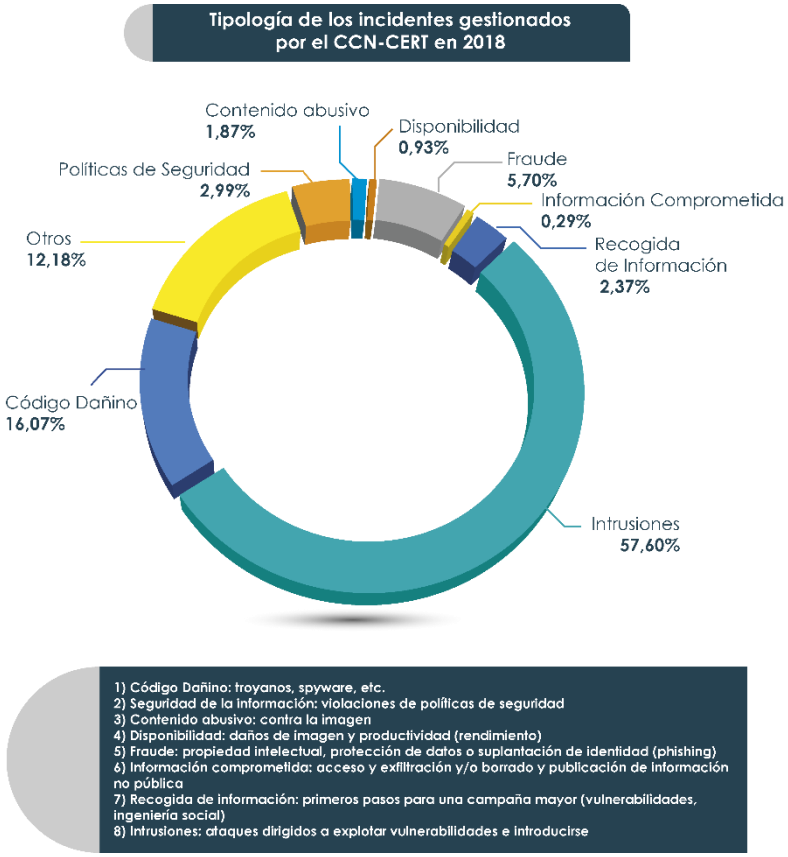
En 2018, el CCN-CERT ha gestionado un total de 38.029 incidentes de seguridad, lo que ha supuesto un incremento del 43,65% con respecto a 2017. De ellos, el 2,7% de tenían una peligrosidad "Muy Alta" o "Crítica"; es decir, ha tenido que hacer frente a una media de 2,8 incidentes diarios de este tipo.



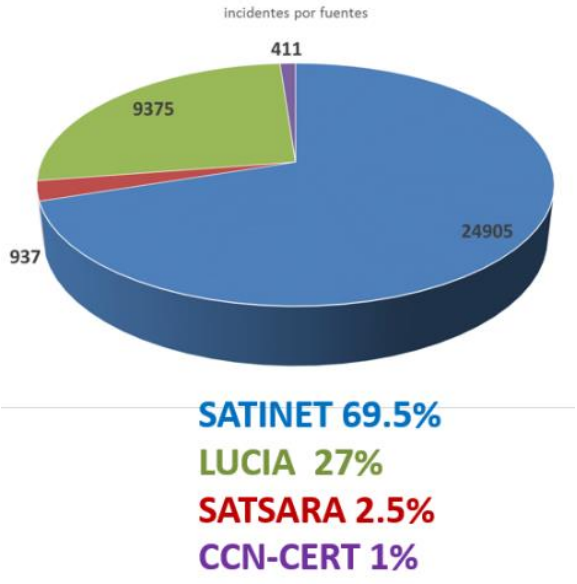
Incidentes gestionados por el CCN-CERT



Peligrosidad de los incidentes gestionados por el CCN-CERT en 2018



La efectividad de los mecanismos de detección es fundamental para asegurar una respuesta temprana y eficaz. En este sentido, como puede observarse en la figura de la derecha, ha sido significativo el número de incidentes detectados gracias al Sistema de Alerta Temprana en Internet, "SAT-INET" desplegadas por el CCN-CERT, que han supuesto casi el 70% de los hallazgos (con casi 25.000 incidentes), seguido por las notificaciones a través de la solución LUCIA (9.375 incidentes, 27%) y SAT-SARA (937 incidentes, 2,5%).

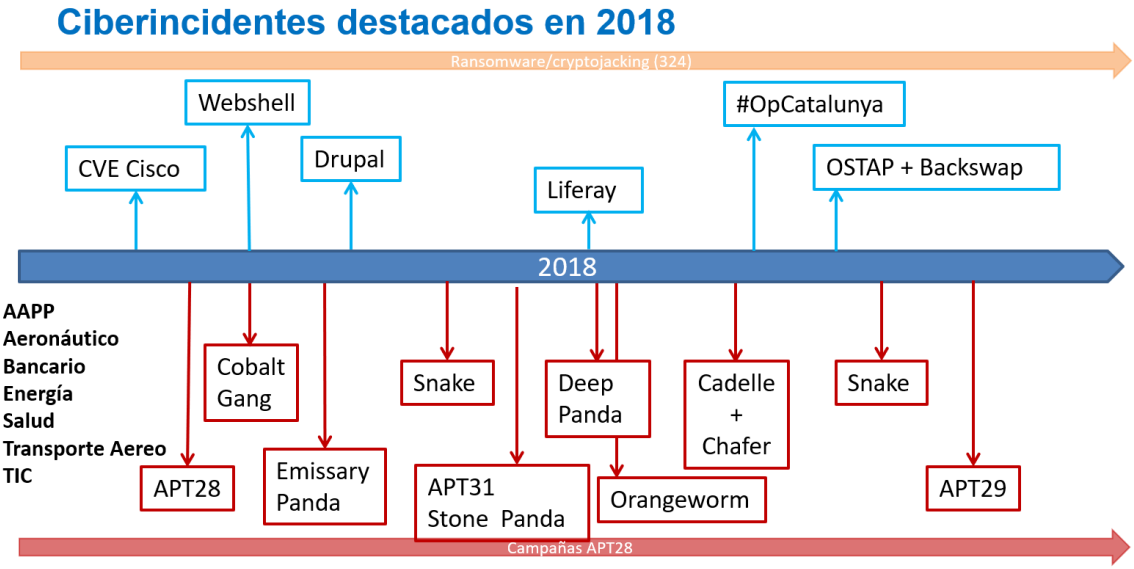


Los Sistemas de Alerta Temprana del CCN-CERT se han incrementado en 2018 con un nuevo servicio SAT-ICS, dirigido a Sistemas de Control Industrial.

La figura siguiente resume el número de entidades adscritas a cada servicio, y su evolución en el tiempo.

Como hemos visto a lo largo del presente informe, 2018 ha sido testigo de la aparición de una gran cantidad de ciberincidentes que han afectado a múltiples sectores: público, aeronáutico, entidades financieras, energético, sanitario, transporte aéreo y servicios e infraestructuras TIC.

La figura siguiente muestra la aparición cronológica en 2018 de las amenazas más significativas detectadas por el CCN-CERT, entre las que destaca, un año más, las campañas de APT.



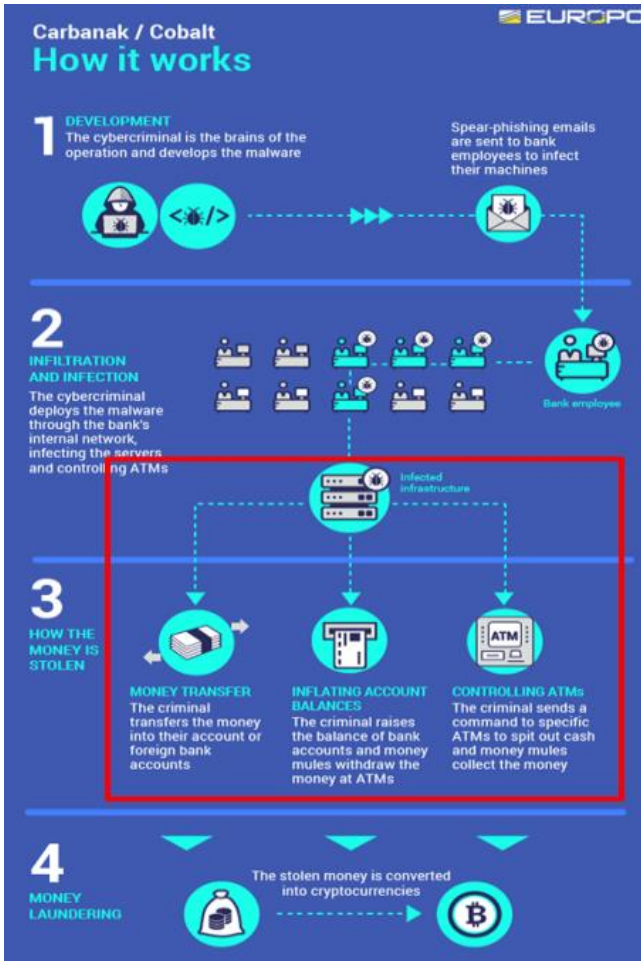
En todo caso, merecen destacarse los ataques al sector financiero, con el objetivo de la sustracción económica de fondos, cuya actividad ha reportado a los atacantes un beneficio estimado de más de 1.000 millones de dólares, desde 2014.

En el **sector bancario**, en marzo de 2018, los ciberataques *Carbanak-Cobalt* fueron detectados gracias a la actividad conjunta de una empresa de seguridad y un CERT extranjero.

El CCN-CERT, por su parte, desplegó su actuación en los momentos previos al *cash-out*, lo que evitó en gran medida, consecuencias aun más graves.

El vector de agresión (como en otros casos que se han visto en el presente informe) fue spear-phishing, atacando vulnerabilidades no parcheadas. El progreso de los ataques en las redes de las víctimas fue muy rápido: menor de 2 semanas hasta alcanzar el control total.

Y lo más significativo: se utilizaron herramientas disponibles al público (*Powershell* y *Cobalt Strike Beacon*), no herramientas construidas a propósito.



En el **sector aeroespacial**, en abril de 2018, los ataques del grupo conocido como *Emissary Panda* -cuya presencia se mantiene desde hace más de dos años-, exfiltraron más de 200 Gb de datos, de entidades de dicho sector.

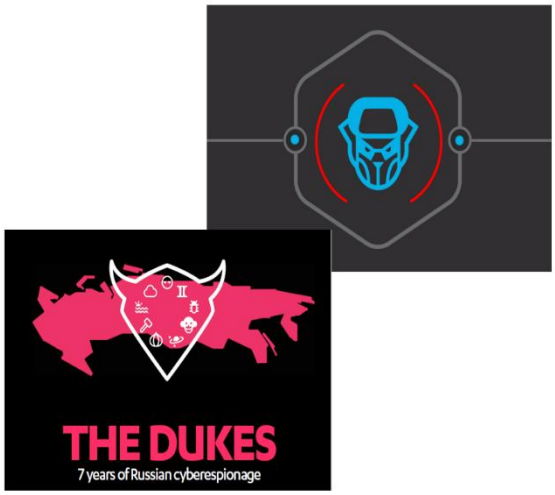
En este caso, el vector de ataque fueron servidores web "abandonados", es decir, sin parchear, y situados en la DMZ.

Lo más significativo de los ciberataques de *Emissary Panda* fue la inexistencia de código dañino: los accesos se lograron mediante webshells (*China Chopper*) y robo de información vía peticiones HTTP.

En el **sector público** el actor principal ha seguido siendo APT29 que, en noviembre de 2018, lanzó una campaña global que apuntaba a un total aproximado de 3.000 víctimas.

El vector de ataque fue el uso de una funcionalidad del Sistema Operativo, que permitía la instalación y ejecución de código dañino.

De nuevo, los atacantes prescindieron de materiales específicos, usando *Cobalt Strike Beacon*, una herramienta disponible al público.

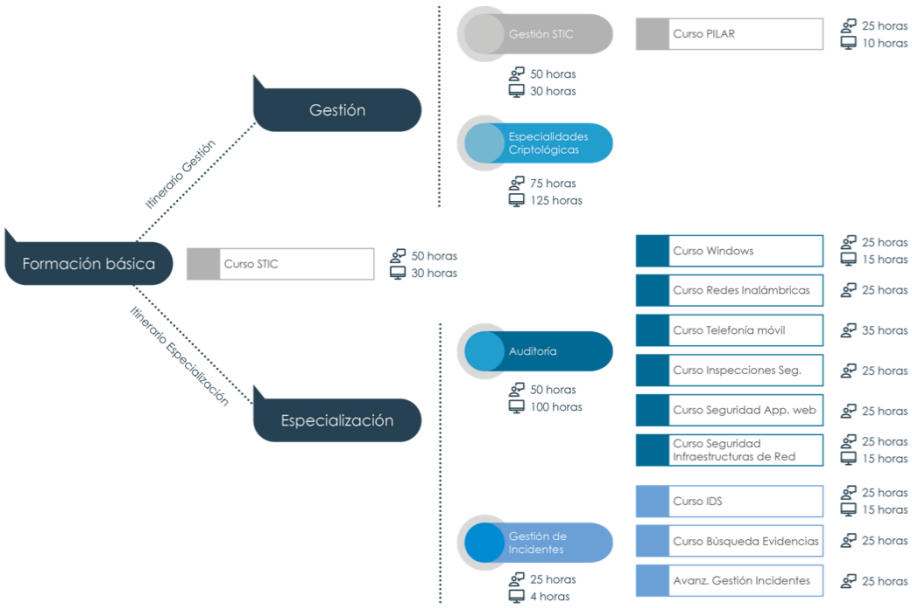


1.1.2. Otros servicios del CCN

Durante 2018, el CCN ha proseguido su actividad en múltiples campos:

- **53 nuevas Guías CCN-STIC**, que vienen a engrosar un catálogo de 335 publicaciones, hasta diciembre de 2018.
- **132 informes de ciberseguridad:** 72 informes técnicos, 30 informes de amenazas, 26 informes de código dañino y 4 informes de buenas prácticas, que entre otros teman abordan la seguridad Wifi, el ransomware o la seguridad en redes sociales.
- **Formación**: se han desarrollado 22 cursos presenciales, 8 cursos on-line y 13 cursos a distancia (usando la Plataforma de Formación *Vanesa*). Como novedades, se ha presentado una primera edición del Curso STIC de Seguridad en Infraestructuras de Red y el curso piloto STIC sobre Auditorías de Seguridad.

  La figura siguiente muestra los **itinerarios de formación** del Centro Criptológico Nacional



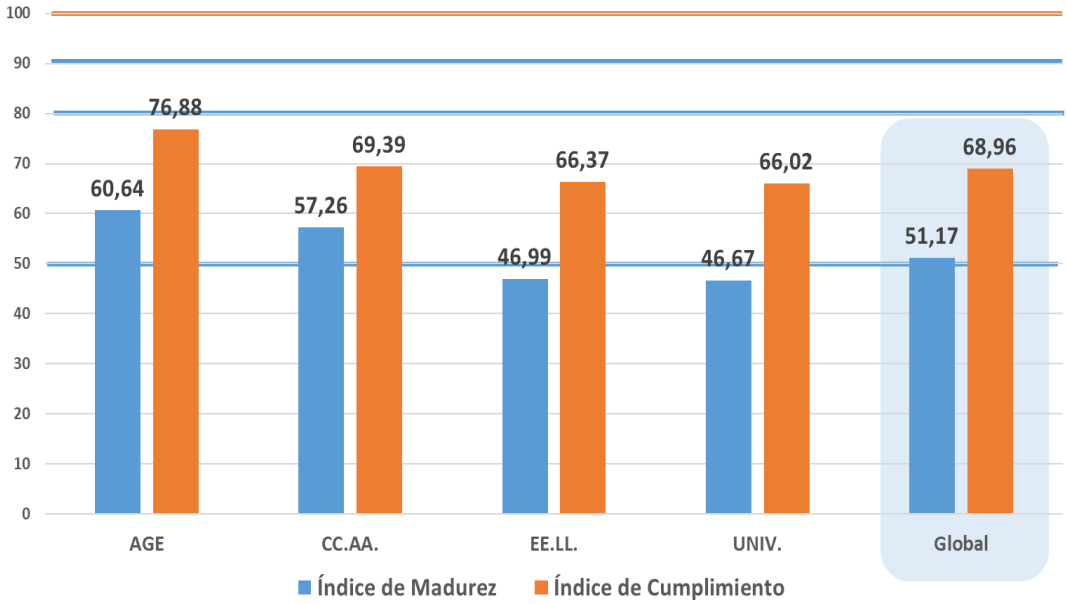
- En materia de detección del talento, el CCN-CERT ha proseguido en 2018 con su Plataforma ATENEA de desafíos de seguridad, que ha albergado la actividad de más de 5.000 usuarios y más de 70 retos de seguridad; a la que se ha unido ATENEA ESCUELA, que ha incorporado más de 60 retos de seguridad básicos[225].

1.1.3. Implantación y Certificación del Esquema Nacional de Seguridad

Durante 2018, se avanzó en la implantación del Esquema Nacional de Seguridad, ENS, en las Administraciones Públicas, aunque el nivel de madurez sigue siendo bajo. Según los datos recogidos en la campaña de 2017 de implantación del ENS (usando la herramienta INES (Informe del Estado de la Seguridad) las cifras fueron las siguientes:

- Número de organismos: 873
- Número de sistemas: 19.135
- Número de usuarios: 4.261.078
- Indicador global de Madurez: 52%
- Indicador global de Cumplimiento: 64%

[225] Puede encontrarse más información de estos recursos en https://atenea.ccn-cert.cni.es (ATENEA) y https://atenea.ccn-cert.cni.es/escuela (ATENEA ESCUELA).



En cuanto a las entidades que han obtenido la certificación, destaca el notable incremento en el sector privado, circunstancia que obedece a la exigencia de las entidades públicas de contar con productos y servicios conformes al ENS, antes de su puesta en explotación.

1.1.4. Catálogo de Productos STIC

El artículo 18 del ENS señala que "En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados por las administraciones públicas se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad".

Por este motivo, el CCN está elaborando el , la Guía CCN-STIC 105 **Catálogo de Productos de STIC,** que ofrece unas garantías de seguridad contrastadas, a organismos del Sector Público o entidades privadas que den servicio a éstos y que se encuentren afectados por el Esquema Nacional de Seguridad (ENS) o manejen información clasificada..

En este sentido, se ha creado la Certificación Nacional Esencial de Seguridad, LINCE, que incluye una metodología orientada a la evaluación y certificación de productos de seguridad TIC para su inclusión en el CPSTIC (CCN-STIC-105) como productos cualificados para ENS Medio y Bajo.

Nuevas versiones y soluciones del CCN-CERT

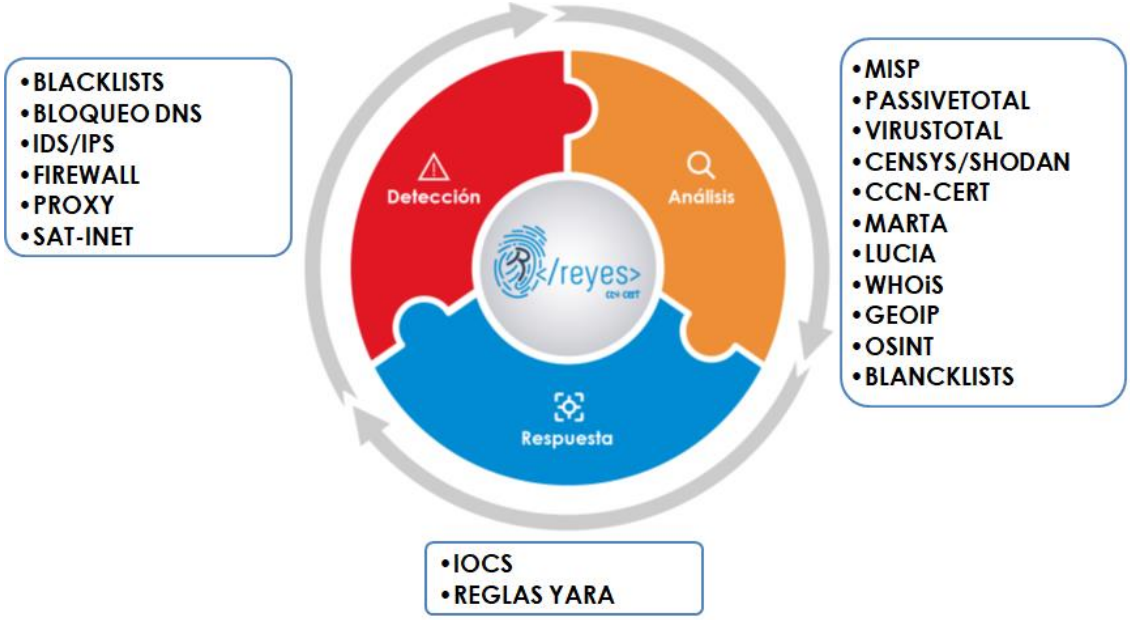
Con el fin de adecuarse a las nuevas necesidades, el CCN-CERT ha ido actualizando todas sus soluciones y desarrollando nuevas herramientas, como ANA, solución para la gestión y evolución de los niveles de exposición a los que se encuentra sometida una entidad. De este modo, ANA proporciona la capacidad de evaluación continua de los activos de una empresa u organismo oficial, ayudando a reducir las probabilidades de aprovechamiento de vulnerabilidades desde el exterior.

Asimismo, se está realizando el despliegue de la versión 2.0 de CLARA, facilitando su integración con ANA; y PILAR, en su versión 7.2, ha incorporado un nuevo conjunto de amenazas, capaces de generar un Análisis de Riesgos aplicable no solo al ENS (metodología Magerit), sino también a la normativa europea. En 2019 dará comienzo el proyecto PILAR-Cloud, cuyo objetivo es disponer de la última versión de esta herramienta en la nube, con un nuevo interfaz de usuario.

En cuanto a las soluciones de **análisis y detección,** el sector público dispone de un SIEM (GLORIA), fundamental para contar con unas mínimas capacidades de vigilancia y se han mejorado tanto MARTA como MARÍA y CARMEN.

</marta> CCN-CERT	</maría> CCN-CERT	carmen Ciberinteligencia Avanzada
Total de binarios subidos: 314 Total de análisis realizados: 1796	Total de usuarios: 267 Total de análisis: 343 (positivos: 161 / negativos: 182) Mejor ratio de detección: 70,81% Peor ratio de detección: 1,86%	Implantaciones operativas en todo el mundo: 54 Implantaciones en organismos y empresas: 28 Integraciones con CARMEN Central: 16 Integración con: REYES, MARTA, CLAUDIA y PANDA. Cabeceras completas HTTP y subida de ficheros PCAP

Por último, REYES ha evolucionado para mejorar el conocimiento de la ciberamenaza de todos los organismos públicos.



1.1.5. SOC de la AGE y del Ministerio de Justicia

Con el fin de optimizar los recursos, durante el 2018, se ha puesto en marcha el Centro de Operaciones de Seguridad del Ministerio de Justicia (a través de un Convenio de colaboración del CNI-CCN y la Subdirección General de Nuevas Tecnologías de la Justicia) y el de la Administración General del Estado (SOC AGE). La **finalidad** del SOC es la prestación de servicios horizontales de ciberseguridad que aumenten la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas de información y comunicaciones de la Administración, así como la mejora de su capacidad de respuesta ante cualquier ataque.

1.1.6. Objetivos para 2019 del CCN

Durante 2019, el Centro Criptológico Nacional desarrollará sus actividades con la mirada puesta en el cumplimiento de los siguientes objetivos prioritarios:

- Reforzar la capacidad de vigilancia y respuesta del CCN-CERT, aumentando los elementos de disuasión y el impulso al despliegue de los SOC virtuales (vSOC) en las Entidades Locales.
- Extender la implantación del ENS al Sector Público y potenciar la Certificación de Conformidad, estableciendo de forma clara las necesidades adicionales para Infraestructuras Críticas, Protección de Datos, Directiva NIS, y resto de normativa de aplicación.

- Potenciar la formación, facilitando la integración de la formación presencial y a distancia y definiendo el perfil de seguridad en los puestos de trabajo de las AA.PP.
- Impulsar la comunidad de CERT y ciberinteligencia, de cara a generar confianza mutua y fortalecer el intercambio de información.
- Mejorar el intercambio de información, en relación con los patrones de detección en cualquier formato (Listas negras, IOC, reglas Yara, Reglas SIGMA etc.), mediante la utilización de las herramientas REYES 3.0 / LUCIA y propiciando la aplicación de las experiencias del CCN en el apoyo a la resolución de incidentes.

Las recomendaciones para Europa.

Por su importancia, sintetizamos las recomendaciones de ENISA en relación con la *CyberThreat Intelligence* (CTI) para los próximos años[226]:

Conclusiones políticas

- Los gobiernos, los Estados miembros y las instituciones de la UE deben facilitar la capacitación del personal de CTI y desarrollar condiciones de empleo que permitan atraer y retener el talento.
- Una política adecuada debe permitir una mejor ingesta de información para producir CTI mediante la eliminación de barreras legales y reglamentarias.
- La CTI debe ser considerada un bien público. Las administraciones deberán subsidiar la creación de centros de conocimiento de CTI y apoyar el desarrollo de buenas prácticas y herramientas para distintas organizaciones.
- Las administraciones deberán contribuir al intercambio de información de CTI y evitar la duplicación de trabajo entre los estados.

Las administraciones deberán hacer esfuerzos para cerrar la brecha entre los usuarios finales y los operadores CTI de alto nivel. Conclusiones de negocio

- Las empresas necesitarán desarrollar servicios viables de CTI para cubrir una amplia gama de organizaciones con escasas o nulas habilidades en estas materias.
- Las empresas deberán definir procesos para la gestión del conocimiento de CTI. Dichos procesos deben estar sincronizados con

[226] Fuente: ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends. FINAL VERSION. 1.0. ETL 2018. JANUARY 2019

otros procesos de ciberseguridad y, en particular, con la gestión de riesgos.

- Las empresas deben procurar herramientas que automaticen la adaptación de los controles basados en feeds-CTI.
- Las empresas deben estimar los riesgos que surgen de los posibles ciberataques a su base de clientes, extrapolando su impacto. Al tomar en cuenta las pérdidas potenciales que pueden experimentar los usuarios, reducirán las superficies de ataque y ayudarán a los usuarios finales a proteger sus activos. Este enfoque mejorará la confianza del usuario y eliminará las barreras para el despliegue de tecnología. Esto es particularmente importante en áreas como IoT, eHealth y computación móvil.
- Las empresas deben ser conscientes de las amenazas a la cadena de suministro, especialmente importantes en procesos de desarrollo de productos que involucran a múltiples proveedores. Los procesos de certificación de los componentes utilizados pueden ser una opción adicional para reducir la exposición a dichas amenazas.

Conclusiones técnicas, de investigación y educativas

- Será necesario desarrollar evaluaciones de amenazas sobre una base sectorial. Dichas evaluaciones estarán orientadas a áreas tecnológicas específicas y ayudarán a los usuarios de estos sectores a administrar las amenazas en esos entornos.
- El cibercrimen evoluciona hacia la profesionalización en varios sectores. Además, los ciberdelincuentes combinan sus habilidades para aumentar la automatización y la eficiencia de los vectores de ataque. Los defensores deberán comprender mejor estos desarrollos y proporcionar nuevos métodos de detección.
- Hay una necesidad apremiante de vocabulario común en el área de CTI. Las actuales taxonomías de amenazas[227] y los esquemas comunes[228], son, frecuentemente, productos secundarios de los proyectos de evaluación de amenazas y no se mantienen, actualizan o consolidan sistemáticamente.
- La eficiencia de los ciberataques depende de la existencia de vulnerabilidades en los sistemas atacados. Las prácticas de gestión de

[227] Ver: https://www.sans.org/reading-room/whitepapers/threatintelligence/evaluation-comprehensive-taxonomies-information-technology-threats-38360
[228] Ver: https://www.slideshare.net/attackcon2018/mitre-infosec-john-lambert-microsoft

vulnerabilidades deben formar parte de las estrategias de defensa. La comunidad de ciberseguridad deberá desarrollar mejores medios para la detección y eliminación de vulnerabilidades al cubrir también puntos de vista geográficos (por ejemplo, el espacio europeo).

- Hay muchas mejoras necesarias en el nivel de ingesta del conocimiento de CTI. Mejores esquemas de intercambio y mejor análisis de incidentes conocidos son vías importantes para lograr este objetivo.
- La CTI debe combinarse con disciplinas relacionadas para ampliar el alcance e incluir fuentes adicionales. En 2018, la combinación de CTI e inteligencia tradicional ha mostrado un gran potencial para la mitigación de amenazas.

2. TENDENCIAS

En 2019 (y años siguientes), los agentes estatales continuarán realizando campañas de intrusión como parte de sus estrategias nacionales. Las entidades de los sectores del gobierno, la defensa, los think tanks y las ONG continuarán siendo los objetivos prioritarios de sus operaciones. Estas intrusiones, probablemente, serán respaldadas (deliberada o accidentalmente) por proveedores de los sectores de telecomunicaciones y tecnología (particularmente, proveedores de servicios administrados) y pueden incluir compromisos en la cadena de suministro, como se ha observado en los años precedentes.

Teniendo en cuenta la evolución de los ciberincidentes en el periodo considerado, es de esperar que los futuros ciberataques incrementen su volumen y su sofisticación. Los siguientes párrafos esbozan lo que cabe esperar del inmediato futuro[229].

2.1. Aumentarán los ciberataques patrocinados por Estados

Los sistemas de información conectados a internet son vitales para la mayoría de las economías nacionales, por lo que constituyen un objetivo obvio en caso de conflicto o controversia. Hay muchos ejemplos de ello en el pasado: desde ciberataques convencionales hasta acciones comprendidas en lo que hemos denominado amenazas híbridas. Los próximos años serán testigos de nuevas acciones de este tipo.

Con la tecnología digital omnipresente y la explosión de IoT, las posibilidades de ataque son ilimitadas. Piénsese, por ejemplo, en los reactores nucleares, las plantas

[229] Tomados de diversas fuentes, entre ellas: Panda (PandaLabs Annual Report), Forbes (Cubersecurity Predictions for 2109), etc.

químicas y los satélites espaciales; todos ellos son objetivos potencialmente vulnerables. Los ataques patrocinados por Estados pueden presentarse en todas las intensidades, y muchos de ellos, probablemente, se activarán como advertencia.

2.2. Ataques a la cadena de suministro

Los ciberdelincuentes son cada vez más expertos y son conscientes de que la ruta más fácil hacia objetivos de alto perfil es a través de la red de proveedores y contratistas de las organizaciones. En 2019, los ataques a la cadena de suministro aumentarán a medida que las grandes corporaciones, que ya tienen suficientes problemas para salvaguardar sus activos, se abran a un mayor riesgo a medida que aumenten la confianza en sus partners.

Debido a estos peligros, muchas empresas que dependen de socios y terceros han creado procesos de gestión de riesgos de proveedores dentro de sus organizaciones. Estos pueden incluir políticas sobre una supervisión constante y el acceso y la retención de registros, medidas que pueden parecer difíciles de cumplir pero que ya forman parte de muchos marcos normativos de cumplimiento. Los equipos de gestión de riesgos de proveedores dentro de las organizaciones serán más habituales a medida que aumenten los ataques a la cadena de suministro.

2.3. La ciberseguridad alcanza a la dirección de las organizaciones

En 2019, las preocupaciones por la ciberseguridad serán un tema importante en los Consejos de Administración o en los órganos directivos de las organizaciones, públicas o privadas, Las violaciones de datos sufridas por las firmas líderes en todas las industrias han provocado temor en los CEOs y en los altos funcionarios, que son conscientes de que su organización podría ser la próxima. Además, los socios, accionistas y clientes responsabilizarán en última instancia a los líderes corporativos, sentimiento que también ha calado internamente en las organizaciones.

A medida que los daños causados por las brechas de seguridad continúen haciéndose cada vez más evidentes (menor rentabilidad, menor precio de las acciones o merma en la reputación), la responsabilidad por las fallas de ciberseguridad irá más allá de la supervisión del departamento TIC, del CIO y del CISO y recaerá en el CEO. Es previsible que muchos debates de los Consejos de Gobierno giren en torno a cómo mitigar los ciberriesgos y mejorar la posición de la organización en materia de seguridad.

2.4. Enfoque empresarial de los atacantes

Los ciberdelincuentes son atacantes sin discriminaciones por razón de la víctima. Mientras que casos como Target o Equifax acaparan los titulares de los medios de comunicación, las empresas y organizaciones de todos los tamaños, públicas y privadas, están sometidas a los ciberataques, especialmente en industrias como la salud, las administraciones públicas y las finanzas, que almacenan y administran grandes cantidades de datos personales, sensibles o confidenciales. En 2019, las empresas más pequeñas utilizarán los mismos enfoques de ciberseguridad que utilizan las grandes empresas.

El impulso para hacerlo será liderado por organizaciones más grandes (las del sector gobierno, por ejemplo), que exigirán que las empresas con las que trabajan cumplan con ciertos estándares de ciberseguridad: “Si tus sistemas no son seguros, no puedo contratarte”.

2.5. La nube como objetivo

Durante 2018 se han producido muchos incidentes relacionados con la computación en la nube y se espera que continúen y evolucionen en los próximos años. En primer lugar, porque una gran cantidad de datos se está moviendo a la nube y los atacantes siguen los mismos pasos. Durante 2018 se han reportado muchas acciones hostiles avanzadas y no avanzadas relacionadas con la nube. De cualquier manera, los ataques están ocurriendo y eso significa que las organizaciones deben estar atentas. En realidad, la pregunta que debe hacerse es: ¿Tiene visibilidad de las cosas que están sucediendo en la nube y puede configurar su Centro de Operaciones de Seguridad (SOC) para poder responder a lo que sucede?

2.6. Sofisticación del código dañino

Los agentes de las amenazas están refinando permanentemente sus herramientas de código dañino para hacerlas más eficientes. El uso de amenazas persistentes avanzadas (APT) aumentará a medida que los atacantes necesiten invertir tiempo y esfuerzos para llevar a cabo acciones significativas (tales como el ciberespionaje, por ejemplo).

2.7. Ciberataques dirigidos a personas

Los seres humanos siguen siendo el eslabón débil en todos los sistemas de seguridad, por lo que, a medida que aumente la eficacia de las protecciones contra código dañino, los agentes de las amenazas modificarán su objetivo, atacando a las personas. Es de esperar que los próximos años sean testigo de muchos más correos

electrónicos de suplantación de identidad (phishing) y sitios web falsos diseñados para engañar al usuario y facilitar el acceso a datos confidenciales, tales como contraseñas o números de tarjetas de crédito.

2.8. Utilización de dispositivos inteligentes en ciberataques

Los dispositivos conectados a internet vía WiFi (profesionales, comerciales o domésticos) ofrecen nuevas formas para que los agentes de las amenazas penetren en las redes internas, atacando a los dispositivos conectados, incluyendo los ordenadores, y, generalmente, al objeto de sustraer datos o información personal.

2.9. Permanencia de los ataques DDoS y su relación con la IoT

Los ataques DDoS siguen siendo una de las armas preferidas de determinado tipo de atacantes. Sobrecargar con exceso de tráfico un sitio web desprotegido, usando redes de bots, seguirá constituyendo un escenario habitual.

Por otro lado, en los últimos años, los ataques masivos DDoS distribuidos por botnets han explotado decenas de miles de dispositivos IoT infectados, para enviar volúmenes paralizantes de tráfico a los sitios web de las víctimas. Estos ataques continúan ocurriendo y seguirán siendo una amenaza en los próximos años. Al mismo tiempo, es de esperar más dispositivos IoT mal protegidos destinados a otros fines perjudiciales. Entre los más problemáticos se encuentran los ataques contra dispositivos de IoT que conectan los mundos digital y físico.

Algunos de estos objetos son cinéticos, como automóviles y otros vehículos, mientras que otros controlan sistemas críticos. Es de esperar un número creciente de ataques contra dispositivos IoT que controlan la infraestructura crítica, como la distribución de energía y las redes de comunicaciones, y a medida que los dispositivos IoT del hogar se hagan más omnipresentes, es probable que haya futuros intentos de utilizarlos como arma por los Estados.

2.10. Incremento del criptojacking

Las criptomonedas, como Bitcoin y otras, continúan ganando atención de los usuarios. Usando el código dañino adecuado, los agentes de las amenazas pueden tomar el control de los ordenadores de los usuarios para "minar" monedas, impidiendo con ello que pueda usarse toda la potencia de la máquina. Este tipo de ataque se incrementará y se hará más sofisticado en el futuro.

2.11. Código dañino más engañoso

Debido a que los atacantes pueden usar los ordenadores comprometidos para una multiplicidad de actividades (minería de criptomonedas, bots DDoS, robo de información, etc.), necesitan acceder a las máquinas varias veces. Para permanecer sin ser detectado, el malware tendrá que ocultarse mejor. Durante los próximos años veremos nuevas variantes de malware más difíciles de detectar, y que podrían residir en los sistemas infectados durante un período de tiempo muy largo.

2.12. El aprendizaje automático para bloquear nuevas amenazas

El desarrollo de nuevos tipos de código dañino sigue a un ritmo incesante, frecuentemente demasiado rápido para que las investigaciones de seguridad puedan atajarlos en tiempo. Las herramientas de Machine Learning, que monitorizan la actividad del ordenador para detectar y bloquear automáticamente los procesos sospechosos, incluso antes de que un malware haya sido identificado oficialmente, constituirán herramientas primordiales. Esta protección proactiva será vital para vencer a los ciberdelincuentes, especialmente a aquellos que usan malware que utilice técnica de ocultación.

2.13. Los viejos ordenadores con Windows serán más peligrosos

El soporte oficial para Microsoft Windows XP y Vista concluyó hace varios años, aunque muchos usuarios (y organizaciones) siguen usándolo. Como es sabido, Microsoft ya no publica actualizaciones ni parches de seguridad para ninguno de estos sistemas, por lo que cualquier PC que los ejecute corre un mayor riesgo de ser víctima de ciberataques. Puesto que la base de usuarios en todo el mundo es todavía bastante grande, los agentes de las amenazas seguirán teniéndolos entre sus objetivos.

2.14. Inteligencia artificial como herramienta en los ciberataques

La esperada promesa comercial de la inteligencia artificial ha comenzado a materializarse en los últimos años. Incluso cuando estos sistemas automatizan de forma útil las tareas manuales y mejoran la toma de decisiones y otras actividades humanas, también emergen como objetivos de ataque prometedores.

Además, los investigadores están cada vez más preocupados por la susceptibilidad de estos sistemas a la entrada maliciosa que puede corromper su lógica y afectar sus operaciones. La fragilidad de algunas tecnologías de IA se convertirá en una preocupación creciente en 2019. De alguna manera, el surgimiento de sistemas críticos de IA como objetivos de ataque comenzará a reflejar la secuencia que se vio

hace 20 años en internet, lo que atrajo rápidamente la atención de los delincuentes cibernéticos.

2.15. IA para identificar las vulnerabilidades

La historia de la seguridad IA también tiene un lado positivo: los sistemas de identificación de amenazas ya utilizan técnicas de aprendizaje automático para identificar amenazas completamente nuevas. Ya no solo los atacantes podrán usar sistemas de inteligencia artificial para detectar vulnerabilidades abiertas: los defensores también podrán usar la IA para fortalecer sus sistemas de los ataques. Por ejemplo, los sistemas dirigidos por IA estarán en condiciones de lanzar una serie de ataques simulados en una red empresarial con el propósito de que un ataque encuentre una vulnerabilidad que pueda solucionarse antes de que los verdaderos agentes de las amenazas la descubran.

Más cerca de casa, es probable que la IA y otras tecnologías empiecen a ayudar a las personas a proteger mejor su propia seguridad y privacidad digital. La IA podría estar integrada en los teléfonos móviles para advertir a los usuarios si ciertas acciones comportan un riesgo adicional. Por ejemplo, cuando configura una nueva cuenta de correo electrónico, el teléfono puede advertir automáticamente al usuario para que configure la autenticación de doble factor. Con el tiempo, esta inteligencia artificial dirigida a la seguridad también podría ayudar a las personas a comprender mejor las concesiones dadas cuando entregan información personal a cambio del uso de una aplicación u otro beneficio adicional.

2.16. La adopción de 5G ampliará la superficie de ataque

En 2018 se iniciaron varias implementaciones de infraestructura de red 5G, y 2019 se perfila como un año de actividad acelerada 5G. Si bien tomará tiempo que las redes 5G, los teléfonos y otros dispositivos con capacidad 5G se implementen de manera generalizada, el crecimiento se producirá rápidamente.

Aunque los teléfonos inteligentes son el foco de interés para la tecnología 5G, es probable que la cantidad de teléfonos con esta capacidad sea limitada durante 2019 y 2020. Sin embargo, con el tiempo, más dispositivos 5G IoT se conectarán directamente a la red 5G en lugar de a través de un enrutador Wi-Fi. Esta tendencia hará que esos dispositivos sean más vulnerables al ataque directo. Para los usuarios domésticos, también hará que sea más difícil monitorear todos los dispositivos IoT. En términos generales, la capacidad de realizar copias de seguridad o transmitir fácilmente volúmenes masivos de datos a almacenamientos basados en la nube dará a los atacantes nuevos objetivos.

2.17. Incremento de la actividad legislativa y regulatoria

La plena aplicación del RGPD en la Unión Europea es solo un precursor de varias iniciativas de seguridad y privacidad en países fuera de Europa. Canadá ya ha implantado una legislación similar al RGPD, y Brasil ha aprobado una nueva legislación de privacidad similar, que entrará en vigor en 2020.

Singapur e India están estudiando adoptar regímenes de notificación de incumplimiento, mientras que Australia ya ha adoptado diferentes plazos para la notificación de brechas de seguridad, comparables a las del RGPD. Otros países en todo el mundo también han puesto atención en el RGPD europeo. En EE. UU., por ejemplo, poco después de la publicación del RGPD, se aprobó una ley de privacidad en California, considerada como la más rigurosa en los Estados Unidos hasta la fecha.

Es de prever que el impacto del RGPD será más evidente en todo el mundo en los próximos años.

Para cerrar estas tendencias, un último elemento: la atribución y la responsabilidad.

La atribución y la responsabilidad son dos de los aspectos más importantes cuando se trata de derrotar a los ciberatacantes. Sin riesgos y sin repercusiones por la actividad dañina llevada a cabo en el ciberespacio, los agentes de las amenazas seguirán atacando y las organizaciones seguirán siendo violadas. Las recientes acusaciones formales, que se han descrito en el presente Informe, ofrecen un poco de esperanza para lo que podría hacerse en el futuro; pero aún queda un largo camino por recorrer.