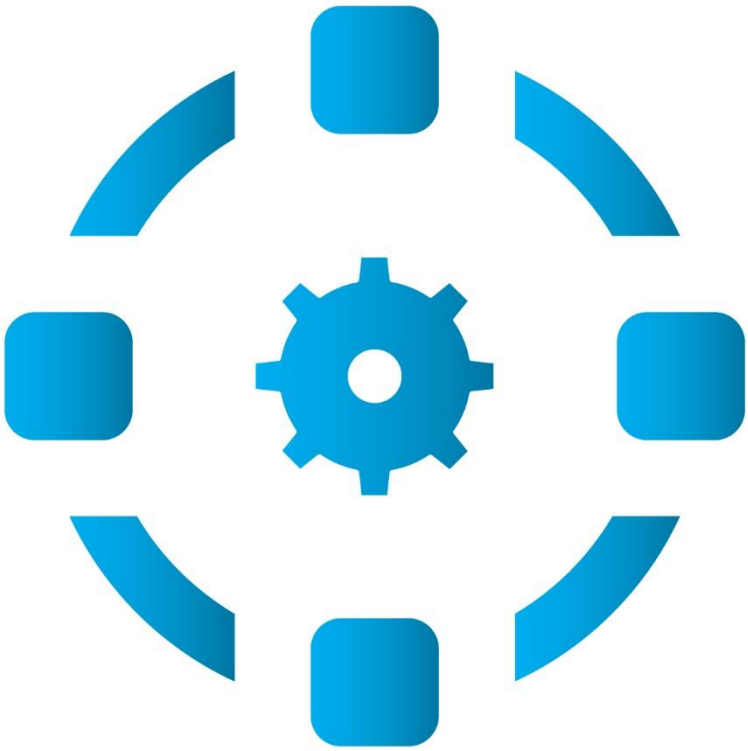
GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN-CERT centro criptológico nacional

CCN-CERT IA-09/18

Ciberamenazas y Tendencias
Edición 2018



Mayo 2018

Edita:

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.05.10 11:10:44 +02'00'

Fecha de Edición: mayo de 2018

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

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 con 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.

2.1 Contenido/Ámbito

Este documento contiene un análisis de las ciberamenazas, nacionales e internacionales, de su evolución y tendencias futuras. Ha sido realizado con el propósito de resultar de utilidad para los responsables de seguridad TIC de las entidades públicas españolas, las organizaciones de interés estratégico y, en general, a los profesionales y ciudadanos de nuestro país.

Aunque el ámbito del presente Informe es mundial, se ha hecho más énfasis en los países del entorno europeo y occidental. No obstante, en determinados epígrafes se han realizado acotaciones específicas para España y sus intereses en el extranjero, con especial incidencia en las redes y sistemas de información de las entidades del Sector Público español y sus Infraestructuras Estratégicas.

2.2 Base documental

La información que ha servido de base para la confección del presente Informe proviene de diferentes fuentes: documentos internos del CCN y de sus organismos homólogos internacionales (especialmente de la Unión Europea, de EE.UU. y de los socios y aliados de España), documentos públicos 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.

2.3 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 al cuarto apartado, titulado “Los Ciberincidentes de 2017”, comprenden el año natural 2017 e incluye, en algún caso y para mejor comprensión de la evolución de los hechos citados, varios datos relativos al último semestre de 2016 y los primeros meses de 2018. Sin embargo, será oportuno esperar al desarrollo y evolución en los próximos meses de las cuestiones citadas en el apartado “Tendencias.

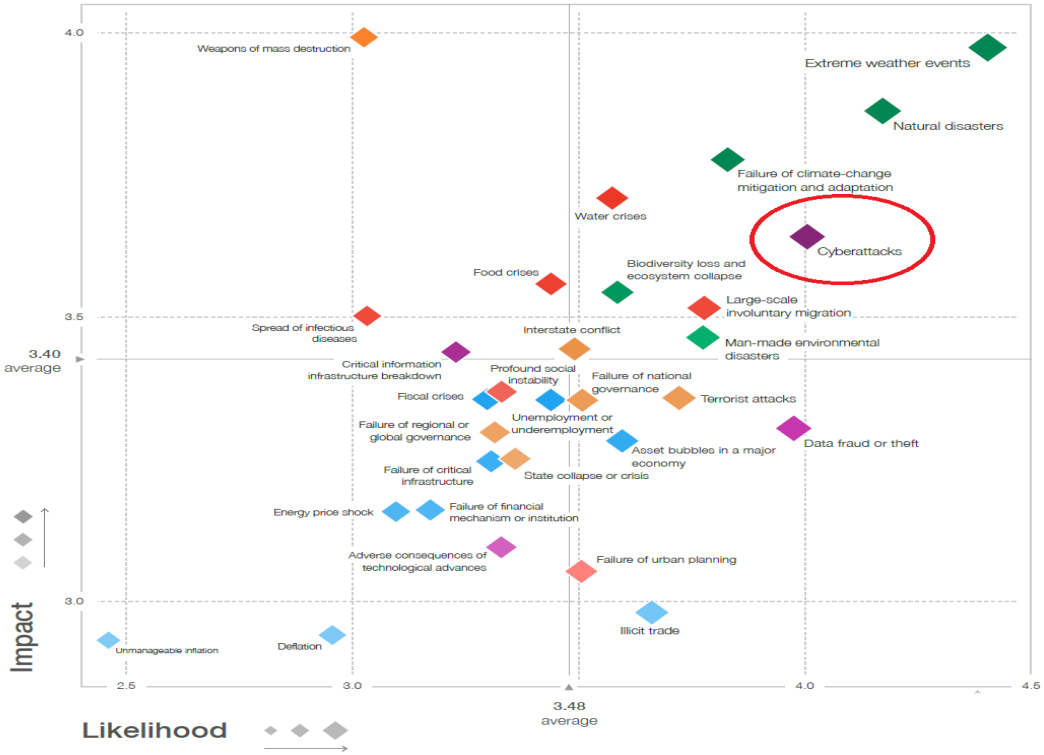
3. RESUMEN EJECUTIVO

A finales de 2017, el número de usuarios de Internet en todo el mundo se acercaba a los cuatro mil millones de personas, sobre un total estimado de más de siete mil millones y medio de habitantes. Por tanto, más de la mitad de los habitantes de nuestro planeta ya son usuarios de Internet. Unas cifras que se pueden ver desglosadas por ubicación geográfica en la siguiente figura[1]:

[1] Fuente: Internet World Stats. (Véase: http://www.internetworldstats.com/stats.htm)

WORLD INTERNET USAGE AND POPULATION STATISTICS DEC 31, 2017 - Update						
World Regions	Population (2018 Est.)	Population % of World	Internet Users 31 Dec 2017	Penetration Rate (% Pop.)	Growth 2000-2018	Internet Users %
Africa	1,287,914,329	16.9 %	453,329,534	35.2 %	9,941 %	10.9 %
Asia	4,207,588,157	55.1 %	2,023,630,194	48.1 %	1,670 %	48.7 %
Europe	827,650,849	10.8 %	704,833,752	85.2 %	570 %	17.0 %
Latin America / Caribbean	652,047,996	8.5 %	437,001,277	67.0 %	2,318 %	10.5 %
Middle East	254,438,981	3.3 %	164,037,259	64.5 %	4,893 %	3.9 %
North America	363,844,662	4.8 %	345,660,847	95.0 %	219 %	8.3 %
Oceania / Australia	41,273,454	0.6 %	28,439,277	68.9 %	273 %	0.7 %
WORLD TOTAL	7,634,758,428	100.0 %	4,156,932,140	54.4 %	1,052 %	100.0 %

La figura siguiente muestra la relación impacto/probabilidad de los ciberataques, dentro de los riesgos globales considerados por el World Economic Forum. Como puede observarse, el WEF sitúa a este riesgo entre los más significativos.



La evolución en el tiempo de los riesgos señalados por el WEF se muestra en el cuadro siguiente. Obsérvese cómo los Ciberataques vuelven a situarse entre los primeros motivos de preocupación para este organismo internacional en términos de probabilidad.


Top 5 Global Risks in Terms of Likelihood
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
1st
Asset price collapse
Asset price collapse
Asset price collapse
Storms and cyclones
Severe income disparity
Severe income disparity
Income disparity
Interstate conflict with regional consequences
Large-scale involuntary migration
Extreme weather events
Extreme weather events
2nd
Middle East instability
Slowing Chinese economy (<6%)
Slowing Chinese economy (<6%)
Flooding
Chronic fiscal imbalances
Chronic fiscal imbalances
Extreme weather events
Extreme weather events
Extreme weather events
Large-scale involuntary migration
Natural disasters
3rd
Failed and failing states
Chronic disease
Chronic disease
Corruption
Rising greenhouse gas emissions
Rising greenhouse gas emissions
Unemployment and underemployment
Failure of national governance
Failure of climate-change mitigation and adaptation
Major natural disasters
Cyberattacks
4th
Oil and gas price spike
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
5th
Chronic disease, developed world
Retrenchment from globalization (emerging)
Global governance gaps
Climate change
Water supply crises
Mismanagement of population ageing
Cyber attacks
High structural unemployment or underemployment
Major natural catastrophes
Massive incident of data fraud/theft
Failure of climate-change mitigation and adaptation
Top 5 Global Risks in Terms of Impact
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
1st
Asset price collapse
Asset price collapse
Asset price collapse
Fiscal crises
Major systemic financial failure
Major systemic financial failure
Fiscal crises
Water crises
Failure of climate-change mitigation and adaptation
Weapons of mass destruction
Weapons of mass destruction
2nd
Retrenchment from globalization (developed)
Retrenchment from globalization (developed)
Retrenchment from globalization (developed)
Climate change
Water supply crises
Water supply crises
Climate change
Rapid and massive spread of infectious diseases
Weapons of mass destruction
Extreme weather events
Extreme weather events
3rd
Slowing Chinese economy (<6%)
Oil and gas price spike
Oil price spikes
Geopolitical conflict
Food shortage crises
Chronic fiscal imbalances
Water crises
Weapons of mass destruction
Water crises
Natural disasters
Natural disasters
4th
Oil and gas price spike
Chronic disease
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
5th
Pandemics
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
Water crises
Economic
Environmental
Geopolitical
Societal
Technological

Por su parte, los hallazgos más significativos en materia de ciberseguridad en 2017 son:

Hallazgos más significativos de 2017

- Los actores estatales y los criminales profesionales continúan siendo la amenaza más importante, causando el mayor daño[2].
- Los ciberataques se han utilizado para influir en los procesos democráticos[3].
- La ciberguerra, los ciberconflictos y la guerra híbrida se hacen cada día más presentes en el mundo, siempre apoyados por acciones en el ciberespacio[4].
- Las vulnerabilidades de Internet of Things han propiciado la existencia de ataques disruptivos que justifican la necesidad de mejorar la resiliencia digital[5].
- Muchas organizaciones dependen de un número limitado de proveedores extranjeros de servicios de infraestructuras digitales, lo que significa que el impacto social de eventuales interrupciones podría ser notable[6].
- La capacidad de recuperación de las personas y las organizaciones sigue a la zaga de las crecientes amenazas[7].

Como en anteriores ediciones, el cuadro de la figura siguiente esquematiza y actualiza los agentes de las amenazas más significativos durante 2017, la tipología de sus acciones y sus víctimas[8].

[2] Los actores estatales han intensificado sus esfuerzos en acciones de sabotaje digital y espionaje económico y político. Además, durante 2017 se han centrado en influir digitalmente en los procesos democráticos al objeto de obtener beneficios geopolíticos. A nivel mundial, más de 100 países se dedican al espionaje utilizando tecnología y herramientas digitales. Por otro lado, la escalabilidad casi ilimitada de los ataques propicia que invertir en cibercrimen sea una propuesta muy atractiva para los delincuentes, en permanente crecimiento y focalizándose en las grandes empresas, con el propósito de obtener beneficios económicos.

[3] Por ejemplo, los ciberataques dieron lugar a filtraciones de información sobre las elecciones presidenciales de EE. UU. Además de ello, varios países han observado cómo tales ataques han podido influir en los procesos democráticos o cómo lo han intentado.

[4] El concepto de "guerra híbrida" busca debilitar a las democracias interfiriendo en sus procesos electorales y alimentando sus conflictos internos, sean ideológicos o territoriales, valiéndose para ello de instrumentos como las noticias falsas o la manipulación de las redes sociales.

[5] Los costes y beneficios de la ciberseguridad no siempre recaen en los mismos actores: la explotación de las vulnerabilidades de dispositivos puede ocasionar daños a terceros que no sean sus usuarios. Internet of Things es una muestra de lo que decimos. Muchos de estos dispositivos contienen vulnerabilidades para las que no se publican actualizaciones de seguridad. En varias ocasiones, durante el periodo considerado, se explotaron dispositivos vulnerables para realizar ataques DDoS a gran escala utilizando botnets y provocando significativas interrupciones. Por regla general, los usuarios de los dispositivos no son los que sufren las consecuencias sino los objetivos atacados. El hecho de que estos ataques podrían haber sido perpetrados por cibervándalos muestra que no solo sofisticados delincuentes profesionales o actores estatales pueden llevar a cabo ataques disruptivos.

[6] Muchos países -España, entre ellos- dependen en gran medida de los servicios de un número limitado de proveedores extranjeros de infraestructura de Internet, tales como Amazon Web Services, Microsoft o Google. Aunque los principales proveedores de tales servicios tienen significativos recursos para hacer frente a los ataques, el impacto social de las interrupciones es muy significativo porque son muchos los servicios que dependen de un pequeño número de proveedores.

[7] Las medidas adoptadas por organizaciones y ciudadanos para mejorar su resiliencia digital son, todavía, limitadas. El crecimiento en el número de ciberincidentes señala que la resiliencia de los países occidentales sigue por detrás del crecimiento de las amenazas.

[8] Fuente: Cyber Security Assessment Netherlands. CSAN 2017 y elaboración propia.

	Víctimas		
Agentes de las amenazas	**Sector Público**	**Organizaciones privadas**	**Ciudadanos**
Estados	Ciberespionaje político	Ciberespionaje económico	Ciberespionaje
	Ciberconflictos / Ciberguerra / Guerra híbrida		Guerra híbrida
	Capacidades ofensivas. Sustracción y publicación de información	Capacidades ofensivas Sustracción y publicación de información	
	Perturbación del funcionamiento de instituciones o procesos democráticos		Fake News
Organizaciones criminales	Disrupción de sistemas	Disrupción de sistemas	Disrupción de sistemas
	Robo y publicación o venta de información	Robo y publicación o venta de información	Robo y publicación o venta de información
	Manipulación de la información	Manipulación de la información	Manipulación de la información
	Toma de control de sistemas	Toma de control de sistemas	Toma de control de sistemas
Organizaciones privadas		Sustracción de información (Ciberespionaje industrial)	Abuso comercial o reventa de información corporativa
Ciberterroristas (incluyendo a los ciberyihadistas o grupos terroristas de motivación ideológica o religiosa)	Disrupción / toma de control de sistemas Ataque a Infraes. Críticas	Disrupción / toma de control de sistemas Ataque a Infraes. Críticas	
	Propaganda / Obtención de info. / Reclutamiento / Radicalización / Financiación	Propaganda / Obtención de info. / Reclutamiento / Radicalización / Financiación	Propaganda / Obtención de info. / Reclutamiento / Radicalización / Financiación
Ciberactivismo	Robo y publicación de información	Robo y publicación de información	
	Desfiguraciones	Desfiguraciones	
	Disrupción de sistemas	Disrupción de sistemas	
	Toma de control de sistemas	Toma de control de sistemas	Toma de control de sistemas
Civervándalos y script kiddies	Robo de información	Robo de información	Robo y publicación de información
	Disrupción de sistemas	Disrupción de sistemas	
Actores internos	Robo y publicación o venta de información	Robo y publicación o venta de información	
	Disrupción de sistemas	Disrupción de sistemas	
Ciber-investigadores	Publicación de información	Publicación de información	Publicación de información

Código de colores:	No han aparecido nuevas amenazas. o Existen suficientes medidas para eliminar la amenaza o No han existido incidentes apreciables derivados de la amenaza.	Se han observado nuevas tendencias o fenómenos asociados con la amenaza. o Existe un conjunto de medidas limitadas para eliminar la amenaza o El número de incidentes derivados de la amenaza no ha sido especialmente significativo	Existen claros desarrollos relacionados con la amenaza o Las medidas desplegadas tienen un efecto limitado en la amenaza o El número de incidentes derivados de la amenaza ha sido significativo

4. LOS CIBERINCIDENTES DE 2017

En los siguientes epígrafes se desarrollan los ciberincidentes más significativos de 2017, agrupados por las motivaciones de los agentes de las amenazas.

4.1 Actividades de Ciberconflictos/Ciberguerra/Guerra híbrida

El año 2017 ha sido testigo de la explotación que se ha hecho de información obtenida a través de ataques de este tipo con el objeto de influir en la opinión pública o de las perturbaciones que los agentes de las amenazas -en muchas ocasiones, patrocinados por estados- han realizado sobre procesos electorales o al socaire de situaciones de conflicto. En la mayoría de las ocasiones las víctimas han sido instituciones democráticas o partidos políticos de muchos países del mundo, España entre ellos[9].

Ha quedado claro que la sustracción digital, la publicación de información o la intoxicación de los medios de comunicación o las redes sociales se ha utilizado profusa y estratégicamente por actores estatales con el objetivo de desestabilizar a otros Estados y polarizar a la población civil.

Este tipo de actividades contempla una gran variedad de herramientas, entre ellas:

- Diplomacia y acciones de inteligencia tradicional
- Actos subversivos y de sabotaje
- Influencia política y económica
- Instrumentalización del crimen organizado
- Operaciones psicológicas
- Propaganda y desinformación

Los dos últimos tipos de acciones han sido los más frecuentemente utilizados en el periodo considerado.

4.2 Actividades dirigidas a influenciar a la opinión pública

En esta línea, y buscando perturbar e influir en procesos democráticos, el partido político alemán CDU; el movimiento En Marche!, del presidente francés Emmanuel Macron; y el Partido Demócrata Americano fueron víctimas en 2017 de ataques digitales de este tipo. Se trataba de ataques dirigidos a las vulnerabilidades personales de los votantes y no a ninguna (posible) vulnerabilidad del proceso de votación.

[9] Parece demostrada la presencia de activistas patrocinados por instituciones rusas en la expresión mediática del conflicto derivado de la situación creada en Cataluña durante 2017, como consecuencia del alejamiento de la legalidad constitucional vigente de ciertas instituciones autonómicas catalanas.

En Francia, un importante volumen de correos electrónicos y documentos del citado movimiento del entonces candidato presidencial Emmanuel Macron se publicó online poco antes de las elecciones presidenciales de mayo de 2017. Ya en diciembre de 2016, el movimiento había detectado que sus miembros estaban siendo atacados por una campaña de *phishing-email*[10].

La compañía de seguridad TrendMicro anunció en mayo de 2016 que el partido de la canciller alemana Angela Merkel (CDU) había sido víctima de ciberataques. Igual que en el caso anterior, los empleados de la CDU recibieron correos electrónicos de *spear phishing* que, en este caso, apuntaban a una falsa pantalla de inicio de sesión utilizada en el servicio de correo web, con el objeto de adquirir las credenciales de inicio de sesión. No está claro si el ataque tuvo o no éxito[11].

Por su parte, tal y como se señaló en el informe del pasado año, en el verano de 2016 se anunció que el Partido Demócrata de Estados Unidos había sufrido una serie de ataques que había permitido la sustracción de material políticamente sensible. Según los servicios de inteligencia norteamericanos, los ataques fueron parte de una campaña originada por actores rusos destinada a influir en las elecciones presidenciales[12], en la toma de decisiones y en la opinión pública.

En enero de 2017, el FBI anunció que el Partido Republicano también había sido blanco de ciberataques, aunque la información sustraída no se había filtrado al exterior. Según el FBI, se utilizó un sistema de correo electrónico perteneciente al Comité Nacional Republicano (RNC) que ya no estaba en uso[13]. No había constancia de que hubiera habido con anterioridad un intento a esta escala de influir en las elecciones estadounidenses con ataques digitales contra sus instituciones democráticas.

[10] Véase: https://www.nytimes.com/2017/05/09/world/europe/hackers-came-but-the-french-were-prepared.html

[11] Véase: http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-german-christian-democratic-union/ y https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/espionage-cyber-propaganda-two-years-of-pawn-storm

[12] Véase: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ , https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democraticnational-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html , https://www.fireeye.com/blog/threat-research/2017/01/apt28_at_the_center.html y https://www.dni.gov/files/documents/ICA_2017_01.pdf

[13] Véase: http://edition.cnn.com/2017/01/10/politics/comey-republicans-hacked-russia/

Así, en diciembre de 2017, el gobierno norteamericano anunció medidas diplomáticas contra Rusia[14], aunque han negado repetidamente la participación en los ataques[15]; del mismo modo que lo hizo el presunto atacante, autodenominado *Guccifer* 2.0[16].

4.3 Actividades dirigidas a la disrupción de sistemas

En el verano de 2016, la botnet *Mirai* infectó decenas de miles de dispositivos de consumidores en Internet of Things (IoT)[17]. El proveedor francés OVH de servicios de hosting fue también fue víctima de Mirai. Los sitios web de los clientes de OVH se ralentizaron o estuvieron temporalmente indisponibles[18].

Por otro lado, la botnet *LizardStresser* fue responsable, a principios de 2016, de varios ataques, sirviéndose también de IoT infectados. Aunque la utilización de grandes botnets no es algo novedoso, sí lo es el hecho de que ambas utilizaran dispositivos IoT de consumidores finales para perpetrar significativos ataques DDoS[19].

El 21 de octubre el proveedor Dyn (que da servicio de DNS al 14% de los dominios mundiales más importantes -entre ellos Twitter, Spotify o Netflix-) fue víctima de una campaña de ataques DDoS usando botnets que compartían el código fuente de *Mirai*[20].

En la noche del 17 al 18 de diciembre de 2016 se produjo un corte de energía de una hora de duración, aproximadamente, en varios distritos de Kiev. La compañía energética ucraniana Ukrenergo informó de que el corte de energía había sido causado por un ciberataque[21]. En enero de 2017 los investigadores de seguridad de ISSP y Honeywell confirmaron que, efectivamente, había sido un ciberataque, al igual que el ataque del año anterior[22]. El objetivo habría sido probar técnicas de ataque usando la estación de distribución eléctrica ucraniana como campo de pruebas[23]. En el mismo

[14] Véase: https://www.whitehouse.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity

[15] Véase: http://www.reuters.com/article/us-usa-election-hack-russia-idUSKCN0Z02EK y https://www.usnews.com/news/world/articles/2016-12-15/russian-officials-deny-vladimir-putins-involvement-in-election-hacking

[16] Véase: https://guccifer2.wordpress.com/2017/01/12/fake-evidence

[17] Véase: https://en.blog.nic.cz/2016/09/01/telnet-is-not-dead-at-least-not-on-smart-devices/

[18] Véase: https://www.ovh.com/us/news/articles/a2367.the-ddos-that-didnt-break-the-camels-vac

[19] Aunque la autoría no está clara, el colectivo hacktivista "New World Collective" se responsabilizó de los ataques.

[20] Véase: https://www.nytimes.com/2016/12/13/us/politics/house-democrats-hacking-dccc.html

[21] Véase: http://ics.sans.org/blog/2016/12/20/how-do-you-say-ground-hog-day-in-ukrainian y http://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA

[22] Véase: 2 https://www.slideshare.net/MarinaKrotofil/new-wave-of-attacks-in-ukraine-2016

[23] Véase: https://motherboard.vice.com/read/ukrainian-power-station-hacking-december-2016-report

período, Reuters informó de diferentes ataques contra los Ministerios de Finanzas y Defensa de Ucrania[24]. Según las investigaciones, en casi todos los casos las infecciones habrían ocurrido al abrir correos electrónicos de *phishing*.

De forma similar, las redes de energía eléctrica de Arabia Saudí, así como ciertas agencias gubernamentales y parte del sector financiero, también fueron víctimas de ciberataques en 2017, empleándose para ello el código dañino *Shamoon*[25].

4.4 Actividades de ciberespionaje (adquisición de información)

En 2017 las agencias gubernamentales holandesas AIVD (Servicio General de Inteligencia y Seguridad) y MIVD (Servicio Militar de Inteligencia y Seguridad) sufrieron varios ataques persistentes y a gran escala de ciberespionaje[26]. En algún caso, ataques dirigidos a empresas con un alto nivel en I+D+i tuvieron éxito, siendo capaces de exfiltrar información comercial confidencial.

Esta problemática ha afectado durante 2017 a todos los países de nuestro entorno occidental. Varias han sido las campañas de ciberespionaje de motivación económica que se han venido desplegando durante años[27] y la mayoría ha atacado repetidamente a varias empresas españolas o residenciadas en España. Importantes datos de investigaciones avanzadas en materia de tecnologías de la información, marítima, energética y de la Defensa se han exfiltrado en estos ataques, además de datos personales, en ciertos casos. Como se ha repetido, tales ataques son una amenaza para el desarrollo económico y la capacidad de defensa militar y confirman el interés de los atacantes en la información sensible de las empresas e instituciones españolas y, en general, occidentales[28].

Una electrónica vulnerable dirigida al consumidor final también ha contribuido al despliegue de ataques de este tipo.

---

[24] Véase. http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC

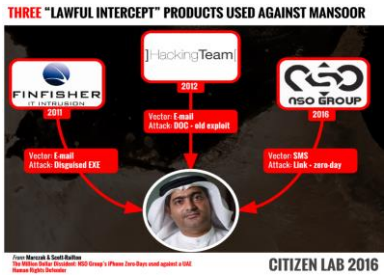
[25] Véase: https://securingtomorrow.mcafee.com/business/shamoon-returns-bigger-badder/

[26] También el Ministerio de Asuntos Exteriores y el Ministerio de Defensa fueron atacados varias veces, incluso -así se manifestó- por países que no habían sido identificados previamente como una amenaza para las redes del gobierno holandés.

[27] Un ejemplo: LinkedIn fue atacado en 2012, exfiltrándose datos de las cuentas de 167 millones de usuarios (nombres, direcciones de correo electrónico y los *hash* de las contraseñas). En mayo de 2016, tal conjunto de datos se puso a la venta públicamente. En junio de 2016, Fox-IT informó sobre campañas de phishing en algunos países, personalizadas según los datos obtenidos de LinkedIn.

[28] Algunos ejemplos: En junio de 2016, el periódico Volkskrant publicó un artículo sobre el ciberataque a la empresa de defensa germano-holandesa Rheinmetall. Según el periódico, agentes chinos habrían estado atacando a esta compañía desde 2012. Por otro lado, en diciembre de 2016, se anunció que se había sustraído información comercial sensible de la empresa alemana ThyssenKrupp como consecuencia de varios ciberataques a principios de ese año.

Por ejemplo, el iPhone del activista de derechos humanos Ahmed Mansoor fue atacado en agosto de 2016 utilizándose tecnología gubernamental de vigilancia. La instalación del software espía Pegasus permitió al atacante espiar el micrófono, la cámara y las comunicaciones, así como seguir los movimientos del teléfono.



En este ataque investigadores de seguridad descubrieron tres vulnerabilidades desconocidas en algunos productos de Apple con un valor de mercado estimado de un millón de dólares. Esto provocó la reacción de la compañía estadounidense, que tuvo que implementar la correspondiente actualización crítica de seguridad en todo el mundo[29].

Otros productos dirigidos a consumidores finales, aunque menos sofisticados, también son vulnerables. Así lo demostró una investigación realizada por la Asociación de Consumidores de Noruega, que reveló que los agentes de las amenazas habían usado la muñeca infantil *'My Friend Cayla'* como dispositivo de escucha[30].

4.5 Actividades dirigidas a obtener beneficios económicos

Los proveedores de servicios gestionados señalan que las medidas de prevención y respuesta al ransomware se han convertido en uno de los ejes centrales de su preocupación. Lo que más allá de la práctica generalizada de la realización de copias de seguridad evidencia que la resiliencia a las infecciones por ransomware aún deja mucho que desear.

[29] Véase: https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ y https://support.apple.com/en-us/HT207130

[30] Véase: https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws

Por ejemplo, en marzo de 2017, la Cámara de Representantes holandesa tuvo problemas con una infección por ransomware, distribuida por correo electrónico a varios miembros del Parlamento[31].

El denominado "fraude al CEO" parece estar en aumento en todos los países, especialmente en el sector financiero, donde los proveedores de servicios gestionados también informaron en 2017 de un aumento en el número de intentos de acciones de esta clase. En este tipo de fraude los delincuentes intentan que el departamento financiero de una organización deposite dinero en la cuenta de un cómplice mediante un correo electrónico que pretende ser de un Directivo o Jefe de Departamento. Para ello utilizan nombres de dominio muy similares al nombre de dominio de la empresa en cuestión.

Los ciberataques a entidades financieras continúan y el 7 de noviembre de 2016 Tesco Bank suspendió los medios de pago online a todos los titulares de sus cuentas tras detectarse 9.000 transacciones fraudulentas por un valor total de 2,5 millones de libras esterlinas[32] en los días anteriores. El 3 de febrero de 2017 investigadores informaron sobre una serie de infecciones de malware en el sector financiero polaco. Los delincuentes parecían haber utilizado el sitio web del Supervisor Financiero como la fuente principal para la distribución de *malware* (Watering hole) a los sistemas internos de varios bancos[33].

En enero de 2017, la policía italiana detuvo a dos individuos sospechosos de ciberpiratería. Los cuerpos policiales señalaron que los individuos querían invertir basándose en la información robada. En el ataque se habrían visto comprometidas cuentas pertenecientes a despachos jurídicos, inversores, sindicatos, la propia policía, funcionarios del Ministerio de Asuntos Económicos y el Vaticano, entre otras[34]. La compañía Kaspersky analizó el *malware* utilizado en el ataque, calificando a los acusados como unos "aficionados muy efectivos"[35].

Investigadores de seguridad de la empresa MedSec trabajaron en conjunto con la compañía inversora Muddy Waters LLC para estudiar las vulnerabilidades en los marcapasos del American St. Jude Medical. La compañía inversora Muddy Waters LLC especuló sobre una caída anticipada en las cotizaciones en la bolsa tras la publicación

[31] Véase: https://twitter.com/KeesVee/status/846613127559106560 y http://nos.nl/artikel/2165391-software-die-computers-gijzelt-aangetroffen-in-tweede-kamer.html

[32] Véase: https://www.theguardian.com/business/2016/nov/08/tesco-bank-cyber-thieves-25m

[33] Véase: https://baesystemsai.blogspot.nl/2017/02/lazarus-watering-hole-attacks.html

[34] Véase: http://www.reuters.com/article/us-italy-cybercrime-idUSKBN14U1K2?il=0

[35] Véase: https://blog.kaspersky.com/eyepyramid-spyware/13838/

de un informe que daba cuenta de estas vulnerabilidades, lo que dio lugar a un proceso penal[36]. Las vulnerabilidades descubiertas podrían haberse usado para interferir en el funcionamiento de marcapasos y desfibriladores. Pese a las medidas adoptadas, la American Food&Drugs Administration (FDA) remitió en abril de 2017 una advertencia al St. Jude Medical señalando que las medidas para mejorar la seguridad no habían sido suficientes[37].

5. AGENTES DE LAS AMENAZAS

En este epígrafe van a examinarse los agentes de las amenazas que de forma intencionada han desarrollado -o pretendido- ataques durante el periodo temporal considerado. Centrando la atención en la intención perseguida, en sus capacidades y en los cambios que se han observado respecto de comportamientos precedentes.

Como siempre, la atribución, esto es, determinar con precisión quién está detrás de un ciberataque, puede ser muy complicado: no solo por la propia dificultad intrínseca de la operación, sino, especialmente, cuando el autor deja tras de sí pistas falsas tratando de garantizar su ocultación. A principios de 2017, se comprobó que ciertos grupos de atacantes de entidades financieras habían utilizado textos en ruso dentro de su código dañino -que incluían significativos errores gramaticales, lo que dejaba claramente en entredicho este origen geográfico-. Otra realidad que dificulta la atribución de la autoría se da cuando varios actores usan herramientas similares. Finalmente, en muchas ocasiones, la intención final de un actor en un ataque no siempre está clara. Por ejemplo, un ataque DDoS puede tener lugar para interrumpir procesos, pero también como excusa para realizar otras actividades (como el chantaje, por ejemplo).

5.1 Los Estados como agentes de las amenazas

Crecimiento y especialización del ciberespionaje

En los últimos años, ha crecido enormemente el número de países que ha adquirido la capacidad de recopilar inteligencia del ciberespacio. El ciberespionaje es un método relativamente económico, rápido y con menos riesgos que el espionaje tradicional porque, dada la dificultad de atribución de la autoría, siempre cabe la posibilidad de negar su uso. Durante 2017, las agencias gubernamentales de muchos países del mundo -incluyendo España- fueron repetidamente víctimas de persistentes

[36] Véase: http://www.muddywatersresearch.com/research/stj/mw-is-short-stj/ y https://www.theregister.co.uk/2016/09/07/st_jude_sues_over_hacking_claim/

[37] Véase: https://threatpost.com/fda-demands-st-jude-take-action-on-medical-device-security/124972/ y https://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2017/ucm552687.htm

ataques de espionaje digital a gran escala, originados en terceros países, incluidos algunos que no habían sido previamente identificados como una amenaza para las redes de los gobiernos atacados.

Puede afirmarse que en la actualidad más de 100 países tienen la capacidad de desarrollar ataques de ciberespionaje y su especialización sigue creciendo, de la misma manera que lo hace la amenaza que representa. Esta amenaza, utilizada principalmente por Servicios de Inteligencia, está dirigida tanto al sector público como al privado y suele provenir de países que desean posicionarse de manera más favorable, desde los puntos de vista político, estratégico o económico.

La inversión creciente de los estados en capacidades ofensivas

Los Servicios de Inteligencia occidentales han identificado que muchos países están invirtiendo en la creación de capacidades digitales ofensivas (esencialmente: ciberguerra o "guerra híbrida"). El objetivo parece claro: influir en las operaciones de información. Así, se atacan cuentas de usuario para recabar información confidencial que luego se publica por un tercero (aparentemente) independiente, con el objetivo de sembrar confusión y división en los oponentes. Además de ello, se ha evidenciado que muchos países están invirtiendo notablemente en la creación de capacidades digitales destinadas a un (eventual o futuro) sabotaje de procesos críticos.

Los ciberataques a las centrales eléctricas ucranianas en diciembre de 2015 fueron seguidos en el mismo mes del año siguiente por un nuevo ataque a la infraestructura crítica ucraniana. En Arabia Saudí, por su parte, varias agencias gubernamentales y empresas han sido también víctimas del código dañino *Shamoon* 2.0[38]. Estas acciones ilustran tanto el potencial de los ciberataques para infligir daño político y físico, como la disposición de los estados para usar estas herramientas.

La ocultación de los atacantes también se ha profesionalizado. Los Servicios de Inteligencia han observado que varios actores estatales están utilizando estructuralmente compañías privadas de TI como tapaderas para disfrazar sus actividades de espionaje. Además de ello, es sabido que las empresas de TI y las instituciones académicas son utilizadas por muchos estados para desarrollar código dañino, lo que incrementa el potencial de los actores estatales para perpetrar ciberataques.

[38] Según señaló el Ministro de Asuntos Exteriores, más de 9000 ordenadores fueron infectados en Arabia Saudí.

A la búsqueda de nuevos métodos

Los actores estatales -análogamente a las organizaciones delincuenciales- se encuentran en una permanente búsqueda de nuevos métodos que les permitan infiltrarse en las redes sin ser detectados, muchas veces en combinación con los métodos tradicionales. Aunque buena parte de los ciberatacantes aún usan memorias USB y mecanismos de *spear phishing* o *Watering hole* para obtener acceso a una red informática a través de infecciones previas de código dañino, los métodos de los estados son cada vez más sofisticados y, en consecuencia, más difíciles de detectar.

En la actualidad, los esfuerzos parecen centrarse en el hardware, los routers, o en la inyección de malware a través de redes wifi, siendo así que un ataque podría, incluso, estar libre de código dañino. No olvidemos que los protocolos en los que se soporta la funcionalidad de Internet fueron diseñados originalmente para transportar datos de la manera más eficiente posible, sin prestar demasiada atención a la seguridad. No sería extraño que los estados dirigiesen su atención a explotar las vulnerabilidades en estos protocolos para sustentar el ciberespionaje.

Finalmente, una infraestructura TI desarrollada sigue siendo atractiva como puerto de tránsito para los ciberataques. Los Servicios de Inteligencia han detectado varios actores estatales que explotan la infraestructura tecnológica de determinados países europeos para atacar a terceros países, convirtiéndose en cómplices involuntarios de tales acciones que persiguen perturbar los intereses económicos, militares y políticos de aquellos países.

5.2 Profesionales del ciberdelito: Ciberdelincuentes.

La amenaza que las organizaciones profesionalizadas en el ciberdelito representan para la seguridad de todo el mundo continúa creciendo a un ritmo acelerado. Los ciberdelincuentes siguen explorando incesantemente “modelos de negocio” más lucrativos, desarrollando nuevos escenarios y atacando objetivos cada vez menos tradicionales.

La diversificación delincuencial al socaire del ransomware

El desarrollo de nuevos métodos de ataque se está evidenciando, entre otros, en nuevos y más lucrativos modelos de ingresos por ransomware[39]. Además de los ataques no dirigidos (sin una víctima concreta), los ciberdelincuentes están empleando el ransomware, cada vez con mayor frecuencia, para atacar a aquellas organizaciones

[39] Véase: http://www.itpro.co.uk/security/26993/ransomware-is-the-most-profitable-cybercrime y https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml

concretas en las que el impacto de un ataque de este tipo sería mayor y, en consecuencia, más inclinadas a satisfacer un rescate de mayor cuantía[40].

En 2017, esta tendencia se confirmó en todo el mundo, poniendo el foco, especialmente, en las escuelas, los hospitales y otras instituciones sanitarias[41].

A portion of the alert posted to the NHS's home page.

Además de lo anterior, estos ataques tienen también un significativo impacto en la vida cotidiana, puesto que procesos o servicios habituales pueden, asimismo, verse afectados[42]. Diferentes equipos de investigación han demostrado que el ransomware también puede usarse contra los **Sistemas de Control Industrial (ICS)** y, como se ha señalado con anterioridad, la electrónica de consumo -como parte del ***Internet of Things***[43]-. Por todo ello, es de esperar que los ciberdelincuentes apunten también a estas áreas en un futuro próximo.

Mayor frecuencia y sofisticación en los ataques a las entidades financieras

Con mayor frecuencia que en años precedentes, los ciberdelincuentes han dirigido sus ataques contra los sistemas de empresas, bancos y otras instituciones financieras (los llamados *objetivos de alto valor*), en lugar de dirigirse solo a los consumidores y analizando cómo explotar al máximo el acceso a la red y convertir tal acceso en dinero. El incremento de la sofisticación de tales ataques también ha sido más que evidente[44].

---

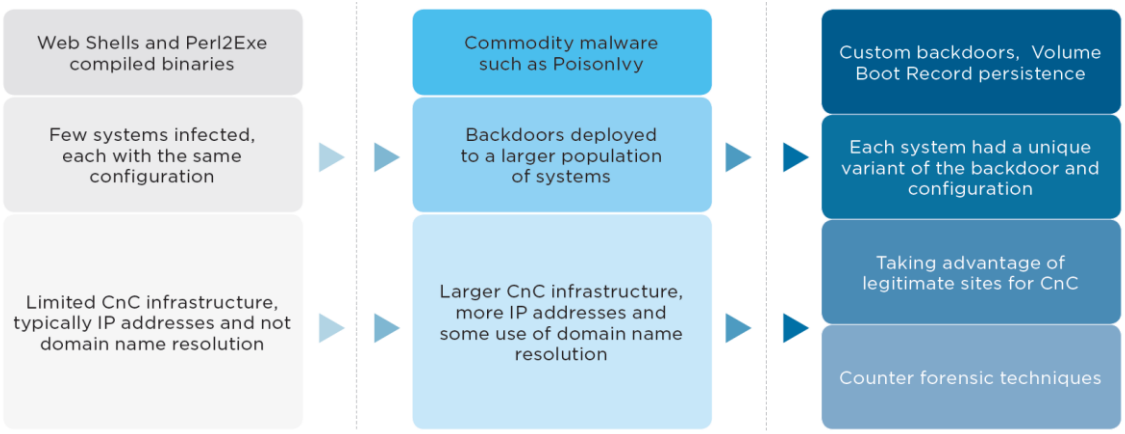
[40] Véase: https://www.wired.com/2017/02/ransomware-turns-big-targets-even-bigger-fallout/

[41] Véase: http://money.cnn.com/2016/04/04/technology/ransomware-cybercrime/ , https://krebsonsecurity.com/2016/11/computer-virus-cripples-uk-hospital-system/ y http://www.csoonline.com/article/3099852/security/health-care-organizations-114-times-more-likely-to-be-ransomware-victimsthan-financial-firms.html

[42] Algún ejemplo de esto fueron los ataques ransomware que afectaron al sistema de pago en el transporte público de San Francisco (véase: http://www.sfexaminer.com/hacked-appears-muni-stations-fare-payment-system-crashes/ y https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked/#more-37060) y el ataque a los sistemas en un hotel austriaco que impidió que las tarjetas de acceso funcionaran (Véase: https://motherboard.vice.com/en_us/article/luxury-hotel-goes-analog-to-fight-ransomware-attacks)

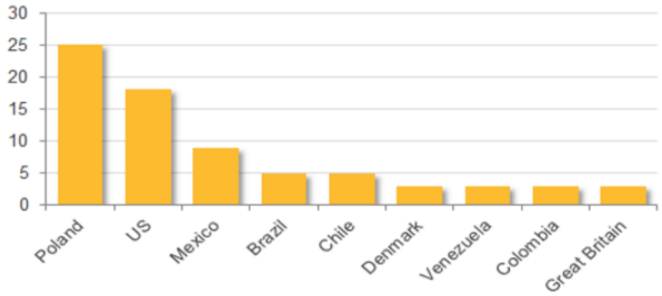
[43] Véase: http://www.securityweek.com/simulation-shows-threat-ransomware-attacks-ics

[44] Véase: FireEye: M-Trends 2017.



Varios bancos europeos han sido blanco de los cibercriminales en 2017. La entidad británica Tesco anunció la suspensión temporal de todas las transacciones on-line después de que 9.000 de sus clientes fueran víctimas de transferencias fraudulentas[45]. Además, un grupo delictivo, autodenominado *Cobalt*, se infiltró en las redes de un par de bancos europeos. Días más tarde, una gran cantidad de cajeros automáticos se vaciaron usando *mulas*[46].

Además de todo ello, se han perpetrado robos en diferentes bancos de todo el mundo, obteniendo y explotando el acceso al sistema SWIFT (pago). Varias empresas de investigación han sugerido la participación de Corea del Norte en tales ataques[47].



Countries in which three or more organizations were targeted by attackers

En septiembre de 2016, en respuesta a los ataques, SWIFT anunció los requisitos globales de seguridad de la información para los bancos adheridos[48]. Finalmente, grupos

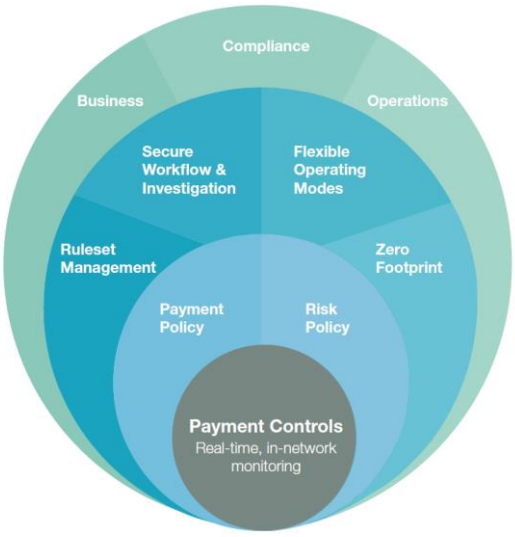
[45] Véase: https://yourcommunity.tescobank.com/t5/News/Message-for-Current-Account-customers/td-p/6599

[46] Véase: http://www.reuters.com/article/us-cyber-banks-atms-idUSKBN13G24Q?il=0

[47] Véase: https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0

[48] Véase: https://www.swift.com/news-events/news/swift-launches-new-anti-fraud-payment-control-service-for-customers

de ciberdelincuentes también explotaron el acceso a los sistemas de un banco en Liechtenstein para extorsionar a los titulares de cuentas extranjeras[49].



Payment Controls complements an institution's existing fraud prevention controls and is designed for seamless integration with existing business, compliance and operational processes.

La conclusión de todo ello parece clara: aunque los ataques dirigidos consumen más tiempo y recursos a los delincuentes, la ganancia económica es mayor que los simples e innominados ataques a los consumidores.

5.3 Terrorismo y ciberyihadismo

Los grupos yihadistas, junto con el uso de Internet por grupos terroristas, constituyen en la actualidad la principal amenaza de este tipo. En los últimos meses de 2016 y durante 2017, las manifestaciones en el ciberespacio de acciones de ciberterrorismo de raíz fundamentalista fueron principalmente debidas a simpatizantes de Daesh-ISIS.

Intención de montar ataques cibernéticos

Aunque los yihadistas todavía no parecen ser capaces de desarrollar ciberataques sofisticados, no es menos cierto que el Daesh, parece estar decidido a desarrollar esta vía de agresión, aun cuando, hasta el momento, los resultados más evidentes han sido las desfiguraciones[50] y los ataques DDoS[51], todos ellos de naturaleza propagandística. Estas características también se encuentran en las listas que han

[49] Véase: https://www.theregister.co.uk/2016/11/29/liechtenstein_bank_breaches/

[50] Véase, por ejemplo, 'Western Countries | Understanding pro-IS hacking capabilities', Risk Advisory, 27 de Septiembre de 2016. (https://news.riskadvisory.net/2016/27/western-countries-understanding-pro-is-hacking-capabilities/)

[51] Véase: 'United Cyber Caliphate Maken Threats in "Message to America," Claims DDoS Attacks', Site Intelligence Group, 27 de Diciembre de 2016.

publicado, conteniendo información sobre individuos a los que el autoproclamado Estado Islámico animaba a asesinar y que el movimiento terrorista afirmó haber obtenido mediante ciberataques[52]. No obstante, gran parte de la información publicada podía encontrarse en Internet[53].

Además de lo anterior, los grupos yihadistas también pretenden desarrollar ciberataques dirigidos al desenvolvimiento diario de los ciudadanos mediante tácticas violentas o en la perturbación social, aunque no se han producido manifestaciones en tal sentido.

Según las estimaciones de los expertos, los ciberyihadistas -y los terroristas en un sentido más amplio- aún no son capaces de organizar ataques sofisticados y complejos[54]. No obstante, su poder ofensivo unido a su capacidad para el reclutamiento podría aumentar como consecuencia de la constitución por un buen número de activistas y grupos de activistas radicales del "United Cyber Caliphate"[55], ganando experiencia con el acometimiento de ciberataques simples.

Por otro lado, la presencia de productos y servicios para desarrollar ciberataques, fácilmente accesibles en foros concretos, incrementa la preocupación, por lo que tal realidad supondría la reducción del umbral de ataque yihadista. Sea como fuere, lo que parece demostrado es que el Dáesh, en comparación con años precedentes, cuenta con menos fondos que hacen menos creíbles las oportunidades económicas para adquirir los productos y servicios más sofisticados[56].

Finalmente, hay que añadir que los ataques llevados a cabo hasta ahora por estos grupos mostraban una importante aleatoriedad. La planificación y el desarrollo de este tipo de ataques dirigidos y sofisticados requiere más experiencia en TI de la que han venido demostrando en los perpetrados hasta ahora; sin perjuicio de la sensación de miedo que puede llegar a generar en los ciudadanos incluso el más simple de tales ataques.

---

52 Véase la referencia citada: 'Pro-IS Hacking Group CCTA Identifies German Pilot to Kill', Site Intelligence Group, 14 de Marzo de 2017.

53 Véase: 'Western Countries | Understanding pro-IS hacking capabilities', Risk Advisory, September 27 2016. (https://news.riskadvisory.net/2016/27/western-countries-understanding-pro-is-hacking-capabilities/)

54 No es necesaria una gran experiencia y muchas y sofisticadas herramientas para los limitados ciberataques que los grupos yihadistas han llevado a cabo hasta el presente.

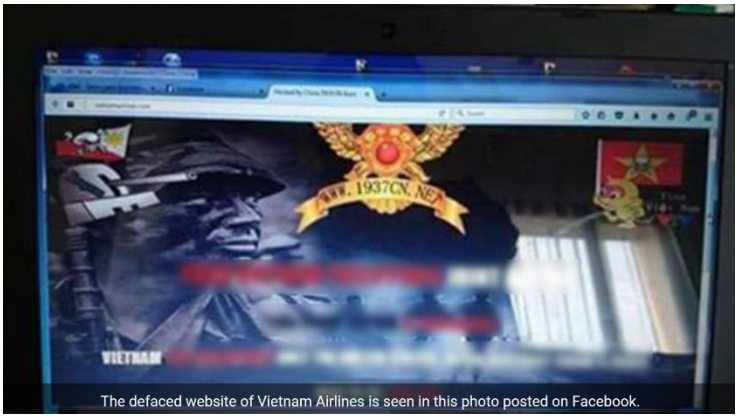
55 Véase 'UCC Announces Merger with Cyber Kahilafah, Claims "Kill Lists" arte Forthcoming', Site Intelligence Group, 24 de Diciembre de 2016.

56 Véase: 'Caliphate in Decline: An Estimate of Islamic State's Financial Fortunes', ICSR & EY, Londres, 2017.

5.4 Los hacktivistas en el ciberespacio

Como es sabido, por regla general, los grupos hacktivistas llevan a cabo sus ciberataques por razones ideológicas. Un par de ejemplos recientes: en marzo de 2017, la creciente tensión diplomática con Turquía fue la razón por la cual varios grupos desarrollaran ciberataques (a pequeña escala) aduciendo activismo político o motivaciones nacionalistas[57]. Seis meses antes, en julio de 2016, en Vietnam, las pantallas de información en varios aeropuertos mostraron lemas anti-vietnamitas y anti-Filipinas en relación con el conflicto en el Mar del Sur de China. Los medios de comunicación apuntaron su autoría al grupo hacktivista *1937CN*[58].

Sea como fuere, aun cuando el acometimiento de ciertos ciberataques exige un importante conocimiento, la amenaza que supone el hacktivismo podría crecer a la vista de la cada vez mayor disponibilidad de productos, servicios y herramientas para desarrollar ataques con un significativo impacto social.



The defaced website of Vietnam Airlines is seen in this photo posted on Facebook.

5.5 Cibervándalos y *script kiddies*

El motivo que anima a estos individuos o grupos para llevar a cabo sus acciones suele ser la broma o el desafío para demostrar sus propias capacidades. Dada la enorme variedad de tipologías personales que los componen, sus expectativas y capacidades pueden también variar ampliamente de unos a otros.

La disponibilidad pública de herramientas para la comisión de ataques también tiene especial incidencia en las acciones de estos grupos. Un ejemplo de esta disponibilidad -de significativo impacto- fue el ataque DDoS a gran escala contra el proveedor de Servicios DNS Dyn. El vector de ataque utilizó el código de la botnet *Mirai*, públicamente disponible[59]. La autoría de este ciberataque fue reivindicada por un grupo desconocido autodenominado *New World Collective*, y cuya intención, según propia

[57] Véase: http://nos.nl/artikel/2163055-turkse-hack-was-waarschijnlijk-online-vandalisme.html

[58] Véase: http://tuoitrenews.vn/society/36243/alleged-chinese-hackers-compromise-hanoi-airport-system-vietnam-airlines-website

[59] Véase: https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

manifestación, era *probar* la seguridad de los sitios web[60], aunque tal afirmación nunca pudo verificarse.

5.6 Actores internos

Con respecto al Informe del pasado año, las amenazas derivadas de las acciones de los actores internos (*insiders*) no han cambiado sustancialmente.

Como es sabido, cuando se trata de acciones intencionadas, la motivación suele ser de naturaleza personal (razones económicas, políticas o estrictamente personales, como la venganza tras un despido). No obstante, las amenazas de los actores internos también pueden provenir de comportamientos inconscientes, descuidos o negligencias.

5.7 Organizaciones privadas

Las características y, correlativamente, los motivos de los ciberataques desarrollados por organizaciones privadas son de distinto tipo: los que se dirigen a la disponibilidad o la confidencialidad de los sistemas de sus competidores, los que se perpetran para obtener beneficios económicos, los que intentan mejorar su posición competitiva o, simplemente, los que se dirigen a explotar comercialmente la información obtenida ilícitamente.

En abril de 2017, el Congreso de los EE. UU. aprobó una ley que despeja el camino para que los proveedores de servicios puedan comerciar con el comportamiento de navegación de los usuarios[61]. De esta manera se responde al comportamiento de ciertas organizaciones privadas, que pueden obtener una enorme cantidad de datos de sus clientes al ofrecer determinados productos o servicios que, con posterioridad, pueden usar o vender a terceros.

Aunque los usuarios, generalmente, deberían conceder los oportunos permisos para permitir este comportamiento empresarial, en 2016, 2017 y los meses transcurridos de 2018, han abundando las noticias de prensa en relación con empresas que han usado comercialmente datos (o que los cedían a terceros) sin que quedara suficientemente claro si el cliente había otorgado el permiso para hacerlo. Otros ejemplos han sido el uso comercial de información de los usuarios de televisores inteligentes, la cesión de datos de WhatsApp a su empresa matriz Facebook, la transmisión de detalles de las redes wifi, de Windows 10 o la cesión de datos de **Facebook** a **Cambrige Analytica**[62].

[60] Véase: http://www.cbsnews.com/news/new-world-hackers-claims-responsibility-internet-disruption-cyberattack/

[61] Véase: https://www.theregister.co.uk/2017/03/28/congress_approves_sale_of_internet_histories/

[62] Véase: http://www.bbc.com/mundo/noticias-43472797

6. VULNERABILIDADES

Se desarrollan seguidamente las vulnerabilidades más significativas de 2017.

6.1 Las vulnerabilidades en los navegadores y en la infraestructura web

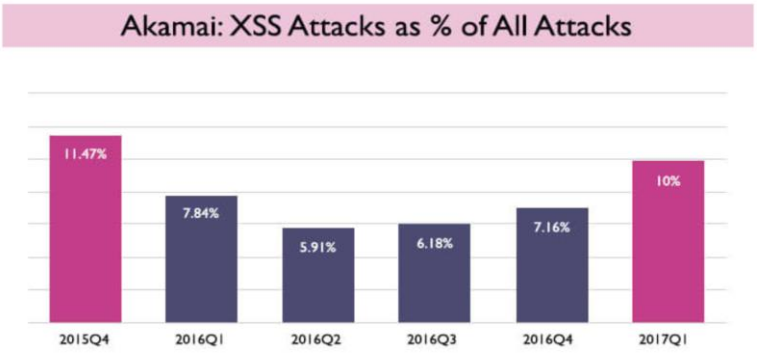
Las vulnerabilidades de los navegadores siguen representando una significativa amenaza. En un reciente informe del Google *Proyect Zero*, se muestra que todos los navegadores de escritorio conocidos tienen vulnerabilidades de seguridad asociadas.

Safari lidera la lista con 17 vulnerabilidades y la cierra Chrome con 2[63].

Vendor	Browser	Engine	Number of Bugs	Project Zero Bug IDs
Google	Chrome	Blink	2	994, 1024
Mozilla	Firefox	Gecko	4	1130, 1155, 1160, 1185
Microsoft	Internet Explorer	Trident	4	1011, 1076, 1118, 1233
Microsoft	Edge	EdgeHtml	6	1011, 1254, 1255, 1264, 1301, 1309
Apple	Safari	WebKit	17	999, 1038, 1044, 1080, 1082, 1087, 1090, 1097, 1105, 1114, 1241, 1242, 1243, 1244, 1246, 1249, 1250
Total			**31**	

La presencia de vulnerabilidades en los navegadores es incesante: en cada nuevo concurso de recompensas por el hallazgo de brechas de seguridad se descubren nuevas vulnerabilidades. Como sucedió en el certamen *Pwn2Own 2017,* en el que se evidenciaron ciertas vulnerabilidades significativas de Microsoft Edge[64].

Por su parte, los ataques por *Cross-site Scripting* (XSS) crecieron un 166% en 2017. Solo en el primer trimestre de 2017, el NIST informó de vulnerabilidades XSS en significativas versiones de algunos de los sistemas software de nivel superior[65].



[63] Véase: https://googleprojectzero.blogspot.ro/2017/09/the-great-dom-fuzz-off-of-2017.html

[64] Véase: http://blog.trendmicro.com/pwn2own-2017-day-three-schedule-results/

[65] Véanse: https://nvd.nist.gov/vuln/detail/CVE-2016-6037 , https://nvd.nist.gov/vuln/detail/CVE-2017-8801 y https://nvd.nist.gov/vuln/detail/CVE-2017-3008

Las vulnerabilidades de los sistemas de gestión de contenidos siguen siendo una importante fuente de ataques. La importante adopción de CMS por parte de sitios web los convierte en objetivos especialmente tentadores para los atacantes. Por ejemplo, en febrero de 2017 se informó de que una vulnerabilidad de *WordPress* (el CMS mundial más utilizado, con el 70% de la cuota de mercado), había posibilitado a los atacantes infiltrarse y desfigurar alrededor de dos millones de sitios web[66]. Muchos de ellos, basados en CMS, son vulnerables debido a la utilización de plugins o extensiones vulnerables y/o desactualizados, tales como *WP Statistics* (plugin de WordPress), que se consideraron vulnerables a la Inyección SQL en junio de 2017[67].

6.2 Las vulnerabilidades del hardware y el firmware

En 2017 prosiguieron las amenazas en el hardware y firmware, con algunos casos especialmente significativos[68].

Este tipo de vulnerabilidades constituyen un enorme aliciente para actores sofisticados. Aunque no es conocido el código dañino capaz de explotar tales vulnerabilidades, su profundidad en la arquitectura del hardware hace que sea muy difícil de detectar y prevenir.

Aunque los fabricantes implicados ya han anunciado su respuesta a estas vulnerabilidades, la eficacia de las actualizaciones de seguridad no podrá evidenciarse de forma inmediata.

7. MÉTODOS DE ATAQUE

Aunque 2017 fue un año especialmente activo en ciberataques que se sirvieron de dispositivos del Internet of Things, las técnicas más consolidadas, como el ransomware o las APTs, siguen siendo las preferidas por los grupos delincuenciales y los estados, respectivamente. En todo caso, siempre a la búsqueda de nuevas formas más eficaces de emplear estas herramientas para obtener mayores beneficios económicos o estratégicos.

Este epígrafe describe los desarrollos en las herramientas que los actores de las amenazas han venido utilizando en el período considerado para llevar a cabo sus ataques.

---

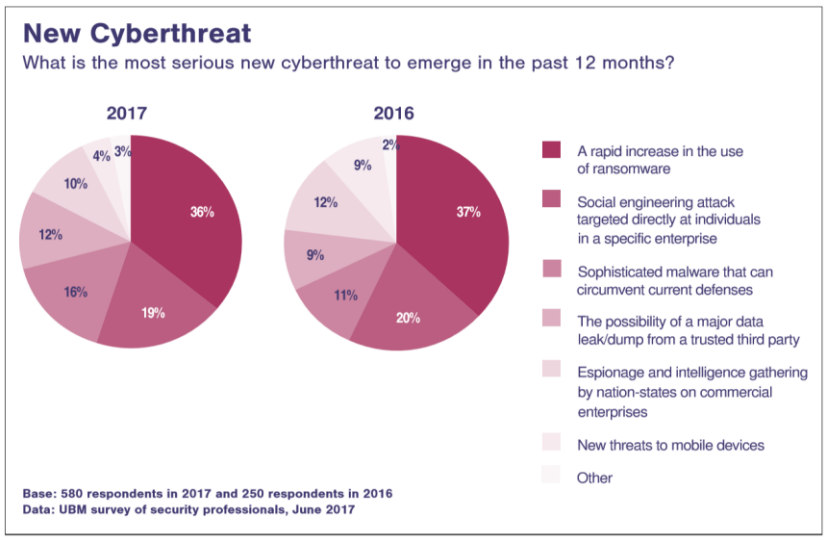
66 Véase: http://www.cbronline.com/news/cybersecurity/breaches/wordpress-security-weak-spot-lets-hackers-infiltrate-and-vandalise/

67 Véase: https://blog.sucuri.net/2017/06/sql-injection-vulnerability-wp-statistics.html

68 Véanse: https://www.blackhat.com/docs/us-17/wednesday/us-17-Matrosov-Betraying-The-BIOS-Where-The-Guardians-Of-The-BIOS-Are-Failing.pdf , https://security-center.intel.com/advisory.aspx?intelid=intel-sa-00086&languageid=en-fr y https://arstechnica.com/information-technology/2017/11/intel-warns-of-widespread-vulnerability-in-pc-server-device-firmware/

7.1 Software para ciberespionaje

En 2017, muchos investigadores han señalado que las organizaciones más importantes de todo el mundo consideran el ciberespionaje una de las amenazas más graves para sus actividades[69].



En agosto de 2016, autores desconocidos autodenominados *Shadow Brokers,* afirmaron haber puesto en peligro una campaña de espionaje de EE. UU. En su comunicado, sostuvieron haber sustraído código dañino para espionaje por intrusión. Para reforzar su mensaje, publicaron parte de este código, así como herramientas de hacking y exploits, señalando que todo ello provenía de los servicios de inteligencia de los EE. UU. Además, cierto material no divulgado se puso a la venta a través de una subasta pública, publicándose más tarde parte de ellos. Los archivos revelados contenían software de ciberespionaje que facilita los ataques a los firewalls, incluidos los de las empresas Cisco, Fortigate y Juniper. Parte del arsenal era malware asociado con el grupo *Equitation Group*; que, según afirma Kaspersky Labs, mantienen estrechas relaciones con los servicios de inteligencia norteamericanos[70].

En marzo de 2017, WikiLeaks publicó datos sobre otra filtración[71] en la que mencionaban una wiki interna perteneciente a la CIA que publicaba la lista de herramientas de hacking y el código dañino usado por esta agencia norteamericana, aunque las propias herramientas y el código no se publicaron. WikiLeaks se comprometió a compartir esta información con los proveedores de aquellos productos o servicios con vulnerabilidades que estuvieran siendo explotadas[72].

---

69 Véanse: http://newsroom.trendmicro.com/press-release/company-milestones/cyber-espionage-tops-list-most-serious-threat-concern-global-busine y https://www.blackhat.com/docs/us-17/2017-Black-Hat-Attendee-Survey.pdf

70 Véase: http://arstechnica.com/security/2017/01/nsa-leaking-shadow-brokers-lob-molotov-cocktail-before-exiting-world-stage/

71 Véase: https://wikileaks.org/vault7/darkmatter/

72 Véase: http://www.usatoday.com/story/news/world/2017/03/09/wikileaks-provide-tech-firms-access-cia-hacking-tools-assange/98946128/

En abril de 2017, *Shadow Brokers* volvió a publicar malware para espionaje afirmando que también en este caso tenía su origen en los servicios de inteligencia norteamericanos. Las herramientas más comentadas fueron: *EternalBlue*, un exploit que aprovecha el protocolo de intercambio de archivos SMB en sistemas Windows y *DoublePulsar*, una puerta trasera que puede instalarse en sistemas infectados para ejecutar diferentes códigos maliciosos[73].

Code Name	Solution
"EternalBlue"	Addressed by MS17-010
"EmeraldThread"	Addressed by MS10-061
"EternalChampion"	Addressed by CVE-2017-0146 & CVE-2017-0147
"ErraticGopher"	Addressed prior to the release of Windows Vista
"EsikmoRoll"	Addressed by MS14-068
"EternalRomance"	Addressed by MS17-010
"EducatedScholar"	Addressed by MS09-050
"EternalSynergy"	Addressed by MS17-010
"EclipsedWing"	Addressed by MS08-067

Hay que mencionar que la vulnerabilidad explotada ya había sido revisada por Microsoft un mes antes en una actualización de seguridad para Windows[74].

Finalmente, a principios de mayo de 2017, la vulnerabilidad explotada por *EternalBlue* se utilizó a gran escala. El ransomware *WannaCry* utilizó esta vulnerabilidad, afectando de manera muy significativa a muchas organizaciones en todo el mundo, entre ellas la compañía española Telefónica, FedEx y el Servicio Nacional Británico de Salud (NHS)[75].

Ataques de ciberespionaje más significativos

APT33[76]: En septiembre de 2017 se descubrió que este grupo estaba detrás de un supuesto espionaje a empresas de los EE. UU., Medio Oriente y Asia. La mayoría de las compañías pertenecen a la industria petroquímica, militar y de aviación comercial.

[73] Véase: https://arstechnica.com/security/2017/04/10000-windows-computers-may-be-infected-by-advanced-nsa-backdoor/

[74] Véase: https://arstechnica.com/security/2017/04/purported-shadow-brokers-0days-were-in-fact-killed-by-mysterious-patch/

[75] Véase: https://www.theregister.co.uk/2017/05/12/spain_ransomware_outbreak/ y https://www.theregister.co.uk/2017/05/13/wannacrypt_ransomware_worm/

[76] Advanced Persistent Threat 33 (APT33) es un grupo de actores identificado por FireEye como compatible con el gobierno de Irán.

APT32[77] (Ocean Lotus Group): Es un grupo de ciberespionaje del sudeste asiático que amenaza a compañías multinacionales que operan en Vietnam. En 2017, se descubrió que este grupo desarrolló una campaña contra dos filiales de empresas norteamericanas y filipinas de venta de productos de consumo ubicadas en Vietnam.

APT28[78] (también conocido como *Fancy Bear, Pawn Storm, Sofacy Group, Sednit* y *Strontium*): Se trata de un grupo de ciberespionaje probablemente patrocinado por el gobierno ruso. A principios de julio de 2017, se descubrió una nueva campaña contra varias compañías de hostelería, incluyendo hoteles de, al menos, siete países europeos y un país de Oriente Medio.

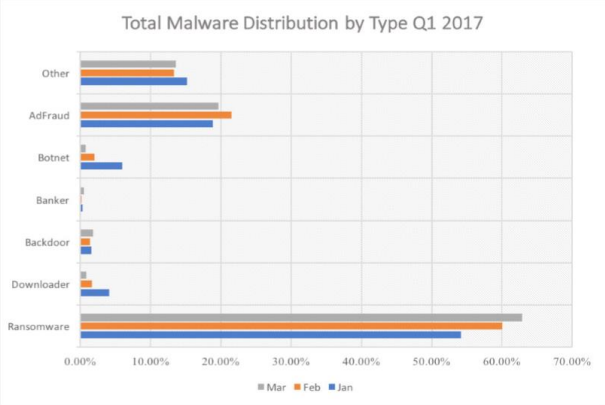
APT29[79] (conocido también como *Cozy Bear*): Es un grupo ruso, presumiblemente asociado a los servicios secretos. En 2017, este grupo se vio involucrado en el ataque a varias instituciones públicas de Noruega (Ministerio de Defensa, Ministerio de Asuntos Exteriores y el Partido Laborista) y de Holanda (varios ministerios, entre ellos el Ministerio de Asuntos Generales).

APT17[80]: Es un grupo con base en China que ha realizado intrusiones de red contra entidades gubernamentales de los EE. UU., la industria de la Defensa, bufetes de abogados, empresas de tecnología de la información, empresas mineras y organizaciones no gubernamentales. Los investigadores han analizado la posibilidad de que el ataque a CCleaner fuera impulsado por un actor estado-nación, probablemente este grupo chino.

7.2 Ransomware

Durante los últimos años, esta actividad delictiva se ha mostrado como una de las más lucrativas[81].

Según las fuentes consultadas, aproximadamente, el 60% del código dañino presente en los ataques de 2017 era ransomware[82].



77 Véase: https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

78 Véase: https://en.wikipedia.org/wiki/Fancy_Bear

79 Véase: https://en.wikipedia.org/wiki/Cozy_Bear

80 Véase: https://attack.mitre.org/pre-attack/index.php/Group/PRE-G0025

81 Véase: http://www.itpro.co.uk/security/26993/ransomware-is-the-most-profitable-cybercrime

82 Véase: https://www.malwarebytes.com/pdf/labs/Cybercrime-Tactics-and-Techniques-Q1-2017.pdf

Por otro lado, en 2017 se ha observado un incremento de los ataques dirigidos a objetivos concretos[83], especialmente a organizaciones financieras, habiéndose registrado peticiones de rescates por importe de 500.000 dólares, lo que, obviamente, incrementa el potencial lucrativo de tales ataques.

Además del método de pago del rescate habitual -bitcoin-, en los últimos años se han incrementado otros tipos de pago, tales como las tarjetas-regalo de iTunes o de Amazon[84].

Greetings,

We'd like to apologize for the inconveniences, however, your computer has been locked. In order to unlock it, you have to complete the following steps:

1. Buy iTunes Gift Cards for a total amount of $400.00

2. Send the gift codes to the indicated e-mail address

3. Receive a code and a file that will unlock your computer.

Please note:,

- The nominal amount of the particular gift card doesn't matter, yet the total amount have to be as listed above.

- You can buy the iTunes Gift Cards online or in any shop. The codes must be correct, otherwise, you won't receive anything.

- After receiving the code and the security file, your computer will be unlocked and will never be locked again.

Sorry for the inconveniences caused.

Más allá de las instituciones financieras y del sector público, las investigaciones mundiales sobre la penetración del ransomware han mostrado que el sector sanitario es el más atacado por esta amenaza[85]. Por otro lado, en 2016 y 2017 se ha evidenciado que, además de los clásicos ataques a las estaciones de trabajo usando el correo electrónico, se han incrementado los ataques que usan exploits para infectar los servidores[86]. Lo que ha sucedido, por ejemplo, en bases de datos mal protegidas, como fue el caso de los ataques a MongoDB[87].

Además, estos ataques también se han extendido a otras tecnologías de servidor, como los servidores ElasticSearch, Hadoop, CouchDB, Cassandra y MySQL.

"We have your data. Your database is backed up to our servers. If you want to restore it, then send 0.15 BTC [$650] and text me to email, just send your IP-address and payment info. Messages without payment info will be ignored."

No cabe duda de que la penetración del ransomware se debe a la facilidad con la que se pueden organizar campañas de este tipo. Es frecuente ver cómo los

83 Véase: https://www.kaspersky.com/about/press-releases/2017_kaspersky-lab-identifies-ransomware-actors-focusing-on-targeted-attacks-against-businesses

84 Véase: https://www.bleepingcomputer.com/news/security/decrypted-alpha-ransomware-accepts-itunes-gift-cards-as-payment/

85 Véase: http://www.csoonline.com/article/3099852/security/health-care-organizations-114-times-more-likely-to-be-ransomware-victimsthan-financial-firms.html

86 Véase: http://www.faronics.com/news/blog/server-side-ransomware-rise-heres-beat/

87 Véase: https://www.welivesecurity.com/la-es/2017/09/07/ataques-extorsivos-bases-de-datos-mongodb/

ciberdelincuentes compran código dañino mediante procedimientos de *Ransomware-as-a-service* para distribuirlo ellos mismos[88].

En abril de 2017, se publicó un informe de la variante del ransomware *Karmen* como *ransomware-as-a-service* que se vendía por 175 dólares[89]. Otro ejemplo es el caso del ransomware *Philadelphia*[90] -cuya autoría se atribuye un grupo llamado *The Rainmaker Labs*-, y que en la actualidad se vende en la Darkweb por 389 dólares.

Por otro lado, el ransomware ha proseguido a su sofisticación en los últimos años. Por ejemplo: en mayo de 2016 se descubrió *Petya*[91], que no solo cifraba los datos almacenados, sino que también sobrescribía el registro de inicio maestro (MBR) del disco duro, lo que hacía que los ordenadores infectados no pudiesen arrancar el sistema operativo. En junio de 2017, se identificó una versión modificada de *Petya*, llamada *NotPetya*, que usaba múltiples técnicas de difusión, entre ellas, el mecanismo de actualización de un producto de software ucraniano llamado *MeDoc*, una versión modificada del exploit *EternalBlue* utilizado por *WannaCry* un mes antes[92], técnicas de propagación en redes locales utilizando herramientas integradas de Microsoft (*WMI* y *PSEXEC*) y la captura de credenciales utilizando herramientas personalizadas similares a *Mimikatz*[93].

88 Véase: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-satan-offered-asransomware-as-a-service

89 Véase: https://www.recordedfuture.com/karmen-ransomware-variant/

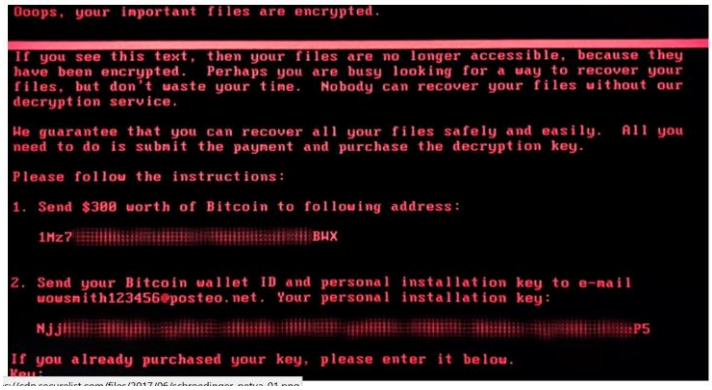
90 Véase: https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/RaaS-Philadelphia.pdf

91 Veáse: https://www.kaspersky.com/about/press-releases/2017_petrwrap-criminals-steal-ransomware-code-from-their-peers

92 Véase: https://securelist.com/schroedingers-petya/78870/

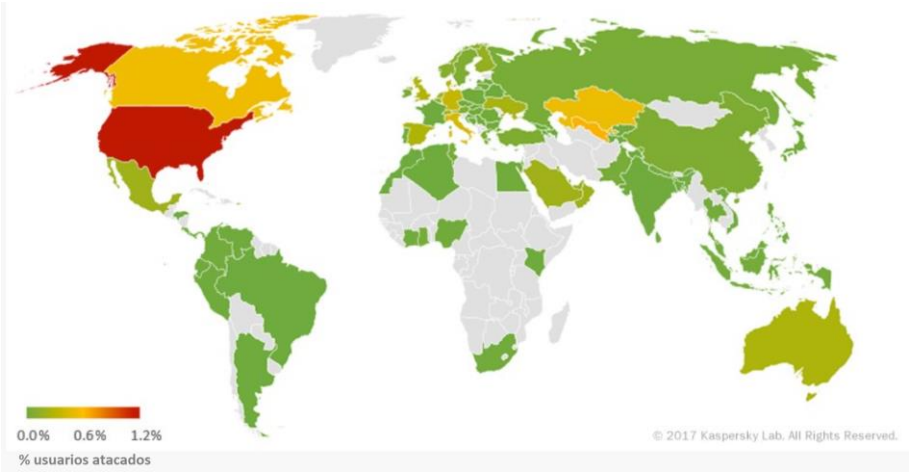
93 Véase: https://www.crowdstrike.com/blog/fast-spreading-petrwrap-ransomware-attack-combines-eternalblue-exploit-credential-stealing/

Uno de los aspectos más significativos en relación con *WannaCry* y *NotPetya* es que, a diferencia del ransomware tradicional, se usaron como vectores de ataque exploits filtrados y supuestamente desarrollados por la NSA norteamericana[94].



En lo que respecta al ransomware para dispositivos móviles, se ha apreciado un incremento en 2017[95], especialmente en equipos Android, debido habitualmente a la instalación o actualización de aplicaciones, exigiendo el pago de un rescate a través de tarjetas de prepago tras lo cual, habitualmente, el dispositivo se libera.

Según las fuentes consultadas, el volumen de ransomware móvil creció más de tres veces durante los primeros meses de 2017, detectándose 218.625 muestras en el primer trimestre. Sea como fuere, el ransomware en dispositivos móviles parece tener menos impacto que en ordenadores convencionales probablemente debido a que estos equipos suelen disponer de una copia de seguridad automática en la nube. El alcance potencial del ransomware en teléfonos inteligentes es, sin embargo, mayor que en otros dispositivos; a la vista de la tendencia de usar el smartphone como medio de acceso a Internet, superior a los ordenadores portátiles en muchas regiones del mundo.

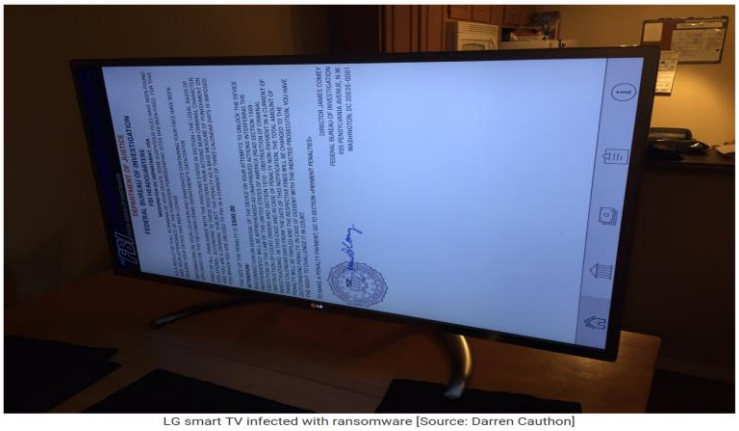


94 Véase: https://www.symantec.com/connect/blogs/equation-has-secretive-cyberespionage-group-been-breached

95 Véase: https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-reports-mobile-ransomware-dramatically-increased-in-q1-2017

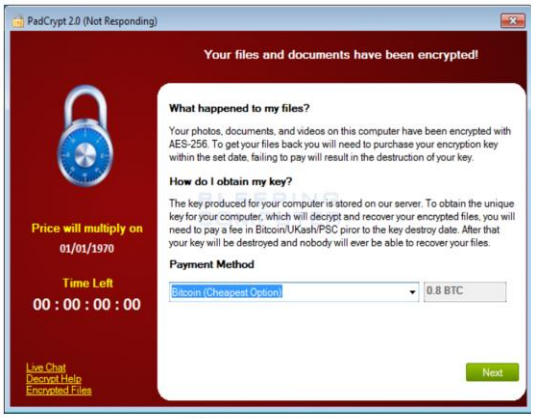
Una nueva forma de infectar con ransomware los equipos es mediante un ataque al *Remote Desktop Protocol* (*RDP*). Este tipo de ataque se usa para obtener acceso al sistema, que posteriormente será infectado. Para diseminarse, el ransomware *WannaCry* explota una vulnerabilidad en el protocolo de intercambio de archivos SMB.

La sofisticación, creatividad y ánimo de lucro de los delincuentes ha quedado patente en 2017 al apreciarse casos de ransomware en la infección de televisores convencionales[96].



LG smart TV infected with ransomware [Source: Darren Cauthon]

Los mecanismos de ataque no solo son cada vez más sofisticados desde el punto de vista tecnológico; son también más meditados o audaces, siempre a la búsqueda de mejores oportunidades para alcanzar los objetivos, persiguiendo el contacto directo con sus potenciales víctimas en algunos casos. Por ejemplo, a principios de 2016 se evidenció la presencia de un chat en vivo en el que los atacantes suministraban soporte técnico a las víctimas para el pago del rescate y para recibir la clave de descifrado[97].



PadCrypt Ransomware Screen

Otro ejemplo: además de la opción de pago para obtener la clave de descifrado, a las víctimas del ransomware *Popcorn Time* se les dio la opción de infectar a otras dos víctimas para eludir tal pago y obtener la clave de descifrado de forma gratuita, siempre que las dos nuevas víctimas finalmente satisficieran la extorsión[98].

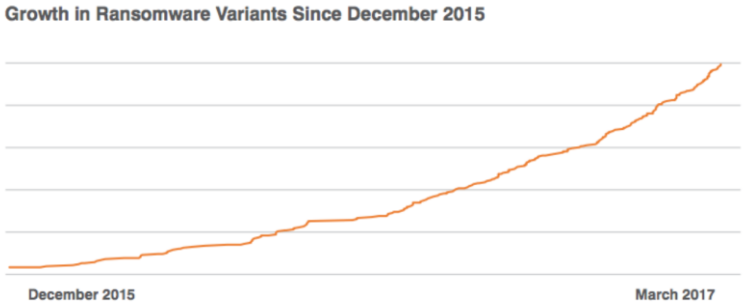
96 Véase: https://www.bleepingcomputer.com/news/security/android-ransomware-infects-lg-smart-tv/

97 Véase: https://www.bleepingcomputer.com/news/security/padcrypt-the-first-ransomware-with-live-support-chat-and-an-uninstaller/

98 Véase: https://www.wired.com/2016/12/popcorn-time-ransomware/

Otro ejemplo más: a finales de 2016 a las víctimas del ransomware *CryptXXX* ransomware se les ofreció un descuento en la compra de la clave de descifrado, como si se tratara de una oferta navideña, tal y como se ve en la presente imagen.[99].

Pese a las nuevas modalidades mencionadas, el correo electrónico ha seguido siendo el medio más utilizado para distribuir ransomware[100].



La inexistencia de un método universalmente adecuado para proteger el correo electrónico permite a los delincuentes llegar fácilmente a un gran número de víctimas potenciales, al tiempo que resulta muy difícil para un usuario medio determinar si el remitente es o no auténtico. Los mensajes de *phishing* distribuidos por medio de email cada vez más refinados y profesionales constituyeron en 2017 el medio para iniciar un ciberataque en el 91% de los casos[101]. Un ejemplo: a principios de abril de 2017 se publicó un informe sobre la campaña *Cloud Hopper*, un ataque particularmente dirigido a los proveedores de servicios gestionados. Los correos electrónicos de *spearphishing* contenían código dañino diseñado para obtener acceso a las redes de estos proveedores. Tras la infección, el ataque desarrolló una búsqueda de datos confidenciales pertenecientes a clientes, tales como propiedad intelectual y detalles personales. La información encontrada se desviaba, en primer lugar, a la red del proveedor, para transmitirse después a la propia infraestructura del atacante.

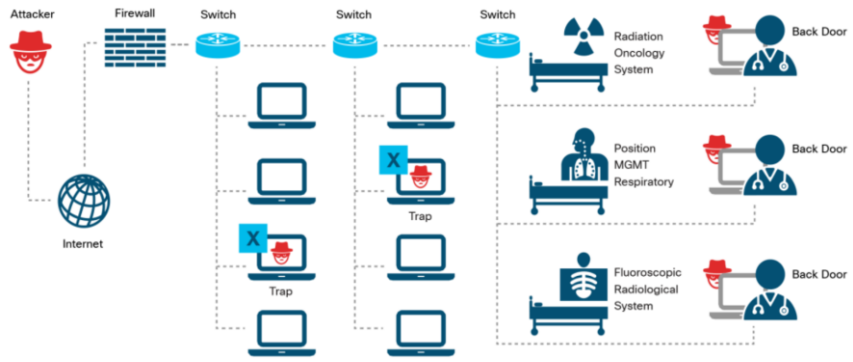
Por último, como adelantábamos en nuestro informe del pasado año, la amenaza del *ransomware* ha alcanzado a los dispositivos médicos. La integración entre las TIC

99 Véase: https://blogs.forcepoint.com/security-labs/merry-cryptmas-cryptxxx-ransomware-offers-christmas-discount

100 Véase: https://blog.barkly.com/ransomware-statistics-2017

101 Véase: http://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704

tradicionales y la tecnología sanitaria y quirúrgica es una tendencia que se observa también en el sector de la salud[102], provocando lo que se ha llamado *MEDJACK* o "dispositivo médico secuestrado". Es previsible que esta amenaza lo sea aún más en el futuro, toda vez que un hospital de tamaño pequeño o mediano, con cinco o seis unidades quirúrgicas, puede tener entre 12.000 y 15.000 dispositivos que pueden verse potencialmente comprometidos, tal y como se desprende del siguiente esquema.



Oncology System Exploit

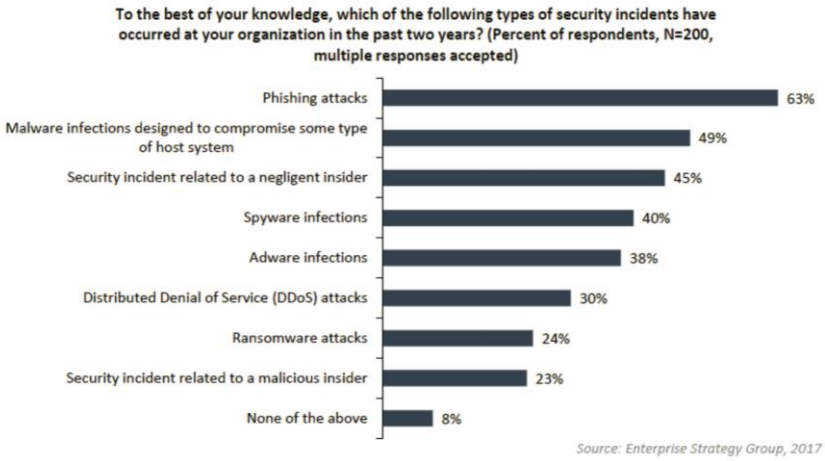
Si bien todas las amenazas y herramientas señaladas siguen usándose extensa y lucrativamente, los ciberdelincuentes no abandonan su permanente búsqueda de nuevas herramientas o nuevas formas de utilizar las existentes, especialmente cuando aumenta la resiliencia de los sistemas atacados a tales métodos.

7.3 Phishing y spamming

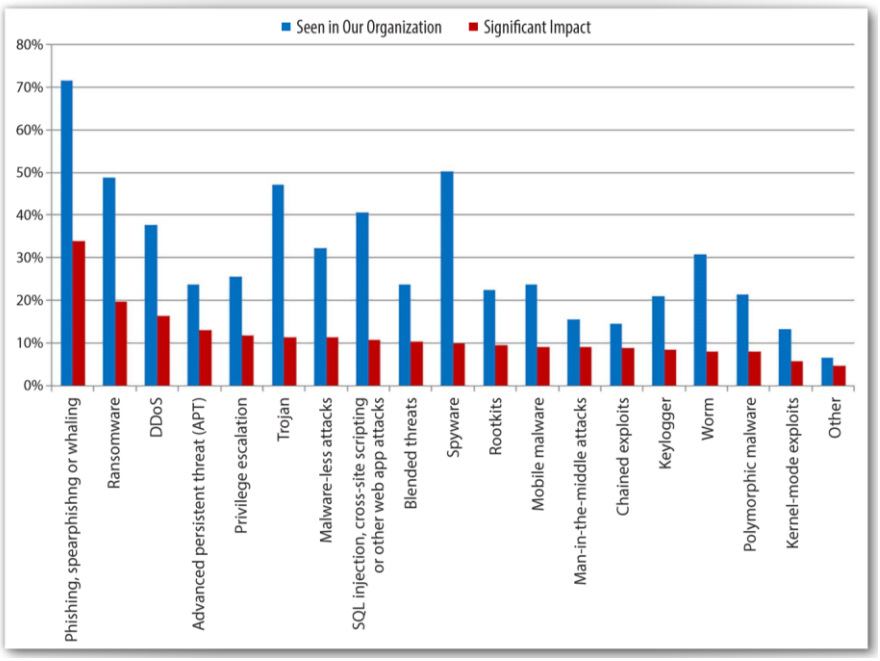
Muy ligado al *ransomware*, el *phishing*, es un método que utiliza principalmente ingeniería social para atacar a los usuarios finales, advirtiéndose en 2017 muestras muy sofisticadas y muy difíciles de detectar. Según las fuentes consultadas[103], las campañas de *phishing* en 2017 aumentaron tanto en volumen como en sofisticación.

102 Véase: http://www.networkiq.co.uk/ransomware-medical-devices-medjack/

103 Véanse: https://securelist.com/spam-and-phishing-in-q2-2017/81537/ y https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf



Como es sabido, el *phishing* es muy usado como primer paso en los ciberataques y constituye el vector de infección más exitoso, tanto en ataques dirigidos (ciberespionaje) como innominados (*ransomware*)[104]. Además, 2017 ha sido testigo de la aparición de un nuevo método de ataque: el *Phishing-as-a-service*[105].



104 Una encuesta (véase: https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910) evidenció que, en 2017, el 74% de las ciberamenazas se introdujeron en los sistemas como un archivo adjunto o un enlace de correo electrónico.

105 Véase: https://www.netskope.com/blog/phishing-service-phishing-revamped/

Originariamente[106] los ataques de *phishing* se desarrollaban a través de masivas campañas de spam sin objetivos concretos, persiguiendo convencer a las víctimas para hacer clic en un enlace dañino o descargar un archivo adjunto para, en última instancia, acceder a sus credenciales, instalar malware o exfiltrar datos.

Sin embargo, en la actualidad, los ataques buscan objetivos concretos, volviéndose más específicos y sofisticados[107]. Así, el denominado *Spear-phishing* se utiliza para atacar a una entidad concreta, muy adaptado al objetivo (generalmente basado en todo tipo de información pública recopilada, por ejemplo, las redes sociales), lo que dificulta enormemente determinar su naturaleza dañina. ENISA publicó un informe al respecto[108] en el que se describe el denominado "compromiso comercial por correo electrónico - BEC". Esta técnica de *phishing* (también conocida como *whalling* o "caza de ballenas"[109]) se refiere a ataques de *spear-phishing* contra ejecutivos de alto nivel[110], generalmente con el objetivo de sustraer dinero de sus organizaciones-víctima o realizar ciberespionaje.

Además de todo lo anterior, hay que señalar que se han observado ataques de este tipo contra industrias[111] de los sectores de la metalurgia, la energía eléctrica y la construcción, lo que aumenta el riesgo de acceso no autorizado a las redes corporativas y los equipos industriales.

La debilidad humana

Con frecuencia, el éxito del *phishing* se debe al sentido de urgencia que le impone a la víctima. Los correos electrónicos de suplantación de identidad, generalmente, instan a la víctima a actuar sobre algo en un periodo de tiempo limitado[112]. Por ejemplo: actuar sobre una supuesta violación de datos, sobre la entrega de un producto, sobre un recordatorio de caducidad de contraseñas, la perentoriedad para

106 Véase: https://www.enisa.europa.eu/publications/info-notes/phishing-on-the-rise

107 Véase: https://www.eff.org/deeplinks/2017/09/phish-future

108 Véase: https://www.enisa.europa.eu/publications/info-notes/how-to-avoid-losing-a-lot-of-money-to-ceo-fraud

109 Véase: https://www.insedia.com/articles/whales-guppies-when-a-company-s-top-bottom-1-are-equally-exposed

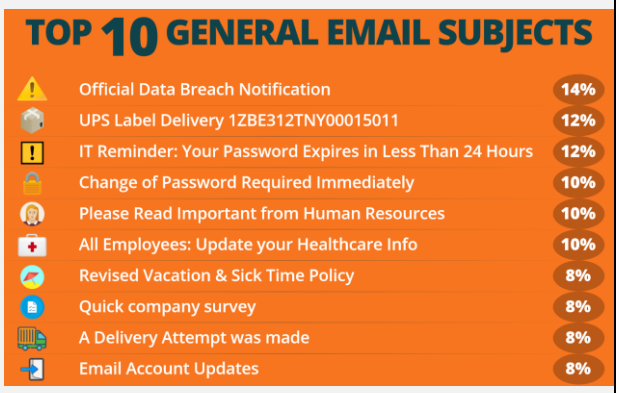
110 Véase: https://www.scmagazineuk.com/ceo-sacked-after-aircraft-company-grounded-by-whaling-attack/article/530984/

111 Véase: https://securelist.com/nigerian-phishing-industrial-companies-under-attack/78565/

112 Véase: https://mediaserver.responsesource.com/press-release/85178/Q32017+Infographic.pdf

descargar lo que constituye software dañino[113], supuestamente reparador de virus, o a través de aplicaciones móviles dañinas que falsifican notificaciones del sistema operativo[114]. Todo ello con el propósito de obtener las credenciales de usuario.

Aprovechando el impacto mediático de *Wannacry*, en 2017 un atacante envió notificaciones falsas, en nombre de proveedores de software, instando a las víctimas a actualizar el software respectivo alegando que los sistemas de las víctimas estaban infectados[115].



La sensación de urgencia impuesta por los ataques de *phishing* suele estar ligada a correos electrónicos bastante convincentes y sitios web falsos que suplantan hábilmente a entidades legítimas.

A menudo, estos sitios web pueden parecer idénticos, tanto en términos de contenido como en una semejanza -inapreciable- del nombre de dominio, que se encuentra en la barra de direcciones URL de cada navegador. En concreto, los agentes de las amenazas usan frecuentemente caracteres no latinos[116] muy parecidos a los latinos, que pueden pasar desapercibidos para un ojo no entrenado[117].

Por otro lado, según las fuentes consultadas[118] y con el objeto de dificultar la atribución de la autoría, las campañas de *phishing* se basan en múltiples y efímeros sitios web, lo que dificulta la adopción de técnicas *antiphishing* tradicionales. Por ejemplo, listas de bloqueo, que no son suficientes contra un número cada vez mayor de dominios dañinos.

113 Véase: https://twitter.com/msftmmpc/status/918012087351283712

114 Véase: https://krausefx.com/blog/ios-privacy-stealpassword-easily-get-the-users-apple-id-password-just-by-asking

115 Véase: https://securelist.com/spam-and-phishing-in-q2-2017/81537/

116 Véase: https://www.theguardian.com/technology/2017/apr/19/phishing-url-trick-hackers

117 Véase: https://gerryk.com/node/68

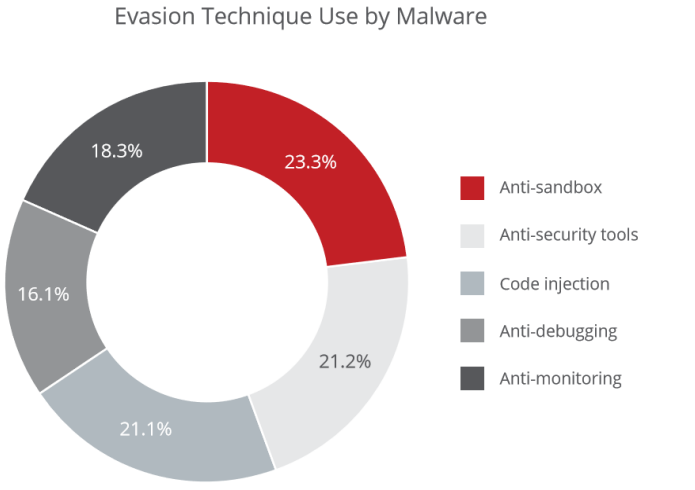
118 Véase: https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf

En algún caso, además, se han detectado correos electrónicos de *phishing* que adjuntaban archivos protegidos con contraseña[119], lo que hacía suponer a las víctimas que se encontraban ante un corresponsal conocido y, por lo tanto, fiable.

Por su parte, el spam, que se remonta a los albores de Internet, permanece como una amenaza significativa, toda vez que sigue siendo el principal medio para la entrega innominada de código dañino a través de archivos adjuntos y URL dañinas. Como es sabido, el spam representa un importante volumen de los correos electrónicos en todo el mundo y se distribuye principalmente por grandes *botnets*. La mayoría de los mensajes de spam persiguen publicitar productos o servicios y, aunque su número parece estar en descenso, ha ganado en calidad (para engañar a las víctimas y/o para evadir el filtrado del correo no deseado).

7.4 Código dañino y Exploits kits

En 2017, el código dañino siguió evolucionando en términos de sofisticación y diversidad, aunque puede apreciarse una ligera disminución en términos de frecuencia. Algunas cifras: Avira detectó más de 4 millones de muestras diarias y Mcfee, más de 700 millones de muestras en el primer trimestre de 2017[120], incorporando en muchas ocasiones sofisticadas técnicas de evasión.



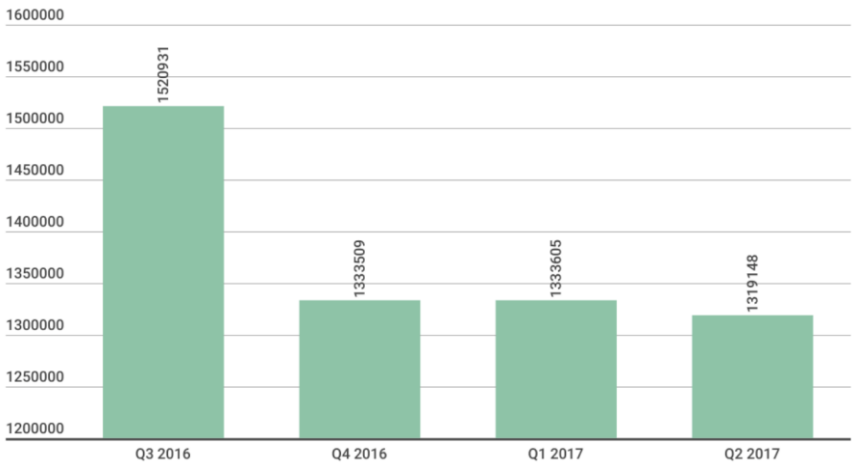
Source: Virus Total and McAfee, 2017.

Por su parte, el código dañino para dispositivos móviles, que en 2017 ha podido descender en cuanto a número absoluto (1,3 millones de muestras en el primer y

119 Véase: https://securelist.com/spam-and-phishing-in-q2-2017/81537/

120 Véanse: https://www.avira.com/en/threats-landscape y https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-jun-2017.pdf

segundo trimestre de 2017, en comparación con 1,5 millones en el tercer trimestre de 2016), ha incrementado claramente su nivel de sofisticación[121].



Las filtraciones de herramientas y exploits han configurado también la realidad de 2017. La filtración de determinado código dañino -cuyo desarrolló originario se atribuyó a actores estatales[122]- dieron lugar a los ataques *WannaCry* y *NotPetya*.

WannaCry es un ejemplo representativo de la tendencia a utilizar como vectores de infección exploits de ejecución remota (como *EternalBlue*) y ataques de fuerza bruta RDP, eliminando la necesidad de una acción directa del usuario, tal como acudir a una URL o abrir un archivo infectado[123].

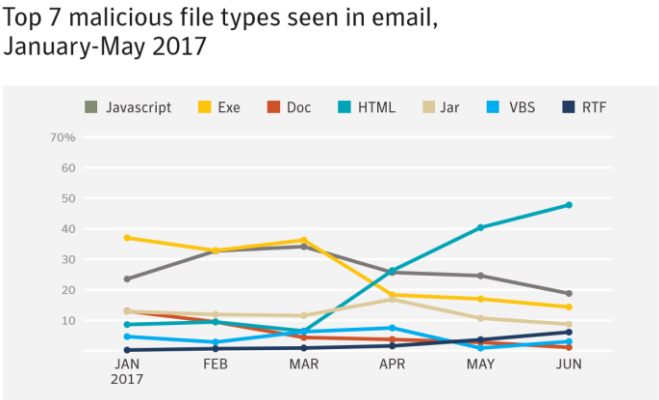
Como adelantábamos en el informe del pasado año, se están desarrollando nuevos mecanismos de ataque, utilizando herramientas que ya están instaladas en los ordenadores de las víctimas, tales como PowerShell, PSExec o WMI. O ejecutando scripts simples y shellcode directamente en la memoria de las máquinas, lo que hace más difícil su detección porque posibilita la ocultación del atacante entre las herramientas habituales de administración del sistema [124].

121 Véase: https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/

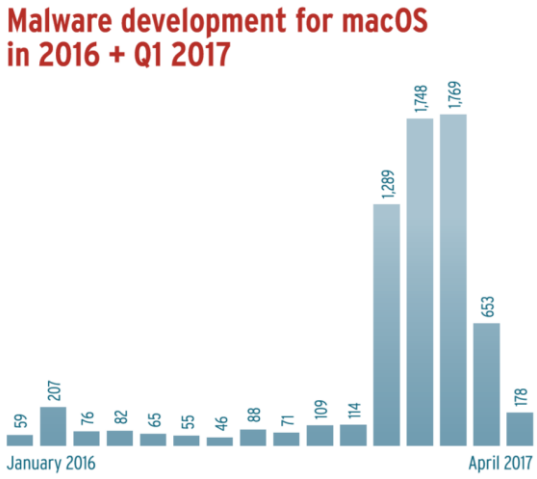
122 Véase: https://blog.rapid7.com/2017/04/18/the-shadow-brokers-leaked-exploits-faq/

123 Véase: https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/

124 Véanse: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/increased-use-of-powershell-in-attacks-16-en.pdf , https://usa.kaspersky.com/about/press-releases/2017_destined-for-deletion-apts-harness-wipers-and-fileless-malware-targeted-attacks y https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf



Por su parte, sigue en crecimiento el código dañino para MacOS y Linux[125], duplicándose en el primer trimestre de 2017, con respecto al año anterior.



Por otro lado, como se ha señalado[126], muchas campañas de malware usan algoritmos de generación pseudoaleatoria de nombres de dominio de dominios (DGA) para dificultar su detección. Aunque los dominios generados por DGA suelen tener una corta vida útil, a veces pueden durar meses, lo que comporta que el bloqueo heurístico sea más difícil como mecanismo de defensa.

Lo más probable es que esta tendencia se deba a que los atacantes se encuentran impelidos a realizar ataques capaces de evitar el mecanismo de defensa y permanecer sin descubrir durante un largo período de tiempo. Además, este es un mecanismo que ayuda a los atacantes a evitar listas de bloqueo, aunque no tan rápidamente como para que los defensores puedan bloquear todos los dominios nuevos. En la mayoría de los casos, los algoritmos utilizados por el código dañino de generación DGA utilizan solo dos elementos al crear dominios: la longitud del nombre de dominio y los posibles dominios de nivel superior que puede usar.

125 Véase: https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2016-2017.pdf

126 Enisa: Threat Landscape Report 2017.

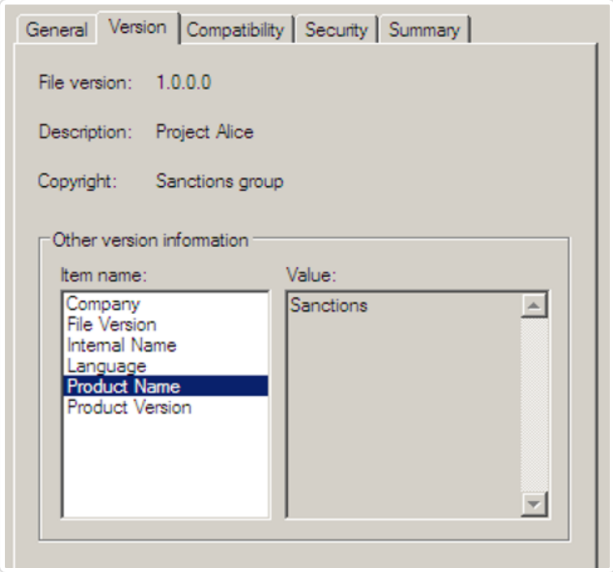
Finalmente, los ataques a la cadena de suministro constituyen cada vez más una de las amenazas más significativas. Efectivamente, una infraestructura comprometida puede afectar a muchas organizaciones. Como reveló el ataque a RSA, las agresiones a la cadena de suministro pueden maximizar el impacto con un mínimo esfuerzo de los atacantes.

Código dañino contra el Sector Financiero

Las entidades financieras de todo el mundo están aprendiendo cómo combatir el fraude bancario en Internet de manera cada vez más efectiva. En la actualidad, los ciberdelincuentes no solo dirigen sus acciones contra clientes o consumidores (que siguen representando la mayoría de los ataques), sino que también lo hacen contra las propias entidades (en menor medida, aunque utilizando herramientas más sofisticadas), lo que en muchos casos comporta un rendimiento económico del ataque mucho mayor[127].

Un informe de la empresa de seguridad Group-IB sobre el grupo delincuencial denominado *Cobalt*, cuyas acciones se dirigieron contra cajeros automáticos, reveló que se utilizaron correos electrónicos de *spear phishing* dirigidos a varias entidades para obtener acceso a la red local de la entidad, lo que permitió a *Cobalt* infectar la red de cajeros automáticos, vaciando una gran cantidad de tales máquinas en un corto período de tiempo.

Efectivamente, también las empresas de seguridad TrendMicro y FireEye han percibido un aumento en el uso de código dañino para cajeros automáticos. Estas compañías han publicado informes que apuntan a nuevas variantes de *malware* dirigidas al *middleware*, una plataforma de software que permite atacar cajeros automáticos de diferentes fabricantes. En concreto, TrendMicro publicó un informe sobre el código dañino para ATMs *Alice*, descubierto en un proyecto de investigación conjunto con Europol EC3[128].



127 Véase: http://www.reuters.com/article/us-usa-cyber-swift-exclusive-idUSKBN1412NT

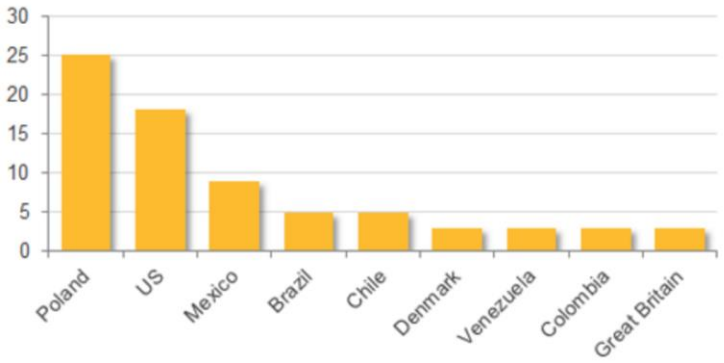
128 Véase: https://blog.trendmicro.com/trendlabs-security-intelligence/alice-lightweight-compact-no-nonsense-atm-malware/

Por su parte, FireEye detectó el *malware* para ATMs *Ploutus-D*, una variante nueva del ya conocido *Ploutus*, en una investigación en América Latina[129], señalando que este tipo de *malware* será más eficaz en países con medidas de protección física menos estrictas en los cajeros automáticos. No está claro si *Alice* y *Ploutus-D* están relacionadas o no.

Por otro lado, hay que señalar que el código dañino financiero se sustenta, esencialmente, en ataques basados en web. La mayoría de los *malware* financieros conocidos (*Zbot, Gameover Zeus, SpyEye, Ice IX, Citadel, Carberp, Bugat* y muchos otros) utilizan exploits del navegador, así como el reciente *Disdain*[130] y las técnicas del *man-in-the-browser.*

Country	Hits	Exploited	Percentage
FR	7028	557	7.93 %
GP	10	0	0 %
RE	6	0	0 %
MQ	6	0	0 %
NL	3	0	0 %
RO	1	0	0 %
ES	1	0	0 %
US	1	0	0 %
Total:	7056	557	7.89 %

Finalmente, los ataques por *watering-hole* contra el sector financiero (muy difíciles de investigar, por su especificidad) están en aumento. Cada vez más sitios web comprometidos se utilizan para lanzar este tipo de ataques. El *malware* se descarga en las máquinas de los visitantes de los sitios web sin su conocimiento, generalmente utilizando *exploits kits*. Según las referencias que se señalan, los ataques en 2017 de este tipo intentaron infectar a más de 100 organizaciones en 31 países diferentes[131], la mayoría de las cuales eran instituciones financieras. Se ha observado un comportamiento común: los usuarios son infectados o redireccionados a diferentes sitios solo si tienen una versión específica de navegador (o sistema operativo), usan una dirección IP concreta (asignada a una organización específica) o son de una región específica.



129 Véase: https://www.fireeye.com/blog/threat-research/2017/01/new_ploutus_variant.html

130 Véase: https://www.intsights.com/blog/new-disdain-exploit-kit-may-signal-reemergence-of-the-popular-hacker-tool

131 Véase: https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0

Exploits kits

Como es sabido, los exploits kits tienen la capacidad de identificar vulnerabilidades en el navegador del usuario o en aplicaciones web y explotarlas automáticamente[132]. Frecuentemente, se dirigen a complementos del navegador (tales como Java o Adobe Flash).

Aunque en 2017 el número de exploits kits se redujo significativamente, se mantiene la técnica del *Malware-as-a-service* que 2017 evidenció que el exploit kit *Disdain* se siguiera alquilando al precio de 80 dólares, detectándose incluso versiones más sofisticadas[133].

En 2017, algunas de las campañas de código dañino más significativas utilizaron exploits kits para comprometer sus objetivos[134]. Puesto que los exploits kits siguen siendo una buena y confiable herramienta para la diseminación de código dañino, es de esperar que el *ransomware* siga usándolos como vectores de infección.

Uno de los exploits kits más utilizados sigue siendo *RIG* que, en 2017, fue utilizado en varias campañas, aunque se evidenciaron comportamientos diferentes en cada una de ellas. Recientemente, ha comenzado a ocuparse del software de minería de criptomonedas[135].

Finalmente, es importante señalar que en 2017 se detectó un nuevo exploit kit, denominado *Terror EK*, que contiene mecanismos muy sofisticados, tales como cargas de *Metasploit* y otros exploits kits -como *Sundown* y *Hunter-,* aunque se han observado cambios significativos en el ciclo de infección[136].

---

132 Véase: https://blog.malwarebytes.com/threat-analysis/2017/03/exploit-kits-winter-2017-review/

133 Véase: http://securityaffairs.co/wordpress/62021/malware/disdain-exploit-kit.html

134 Véase: https://blogs.technet.microsoft.com/mmpc/2017/01/23/exploit-kits-remain-a-cybercrime-staple-against-outdated-software-2016-threat-landscape-review-series/

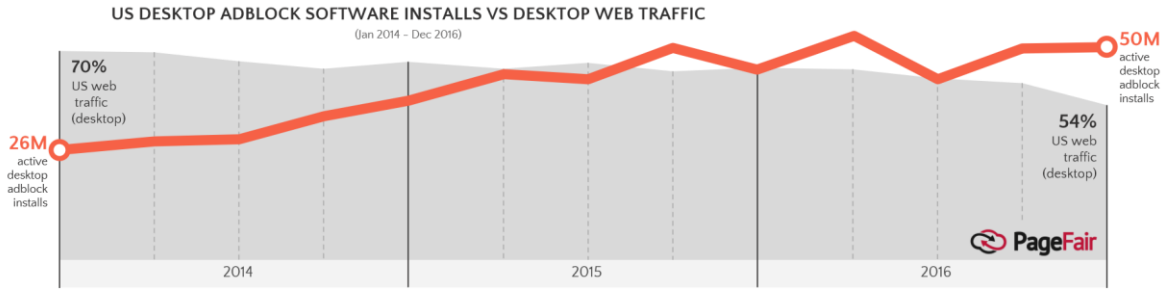
135 Véase: https://www.zscaler.com/blogs/research/top-exploit-kit-activity-roundup-spring-2017

136 Véase: https://www.zscaler.com/blogs/research/top-exploit-kit-activity-roundup-spring-2017

7.5 Ataques contra la Industria de la Publicidad

A finales de 2016 y principios de 2017, los ciberdelincuentes obtuvieron beneficios económicos de la industria publicitaria utilizando la botnet *Methbot*. Para lograrlo, registraron nombres de dominio que parecieran pertenecer a grandes y conocidas organizaciones. Estos nombres de dominio se suscribieron a una red publicitaria para que los anunciantes se publicitasen en ella. El método se valía de una *botnet* para hacer clic automáticamente en el enlace del anuncio, donde el anunciante pagaba por cada clic una cierta suma de dinero al propietario del nombre de dominio. Los usuarios reales se simularon al iniciar sesión automáticamente en cuentas de redes sociales y simular los movimientos del mouse y los clics desde un navegador especialmente desarrollado para este propósito.

Infectar sistemas mediante la distribución de código dañino a través de anuncios en sitios web (lo que se denomina "publicidad dañina" o "*malvertising*") parece seguir en aumento[137]. Efectivamente, la empresa RiskIQ informó un aumento del 132% en el número total de casos de publicidad maliciosa en todo el mundo. Durante 2016 y 2017 se implementaron medidas para prevenir las infecciones por *malvertising,* tanto del lado del usuario como del lado del propietario del sitio web. Según las cifras de PageFair, el uso de *adblockers* ha aumentado en torno a un 20% en los últimos años[138].



7.6 Ataques Web

Ataques basados en web

Como es sabido, los ataques basados en web son aquellos que hacen uso de sistemas y servicios habilitados para la web, tales como navegadores (y sus extensiones), sitios web (incluidos los sistemas de gestión de contenido), los componentes TIC de servicios web y las propias aplicaciones web. Algunos ejemplos: exploits para los navegadores web (o sus extensiones) o servidores web; exploits de los servicios web;

137 Véase: https://www.riskiq.com/infographic/riskiqs-2016-malvertising-report/

138 Véase: https://pagefair.com/downloads/2016/05/2015_report-the_cost_of_ad_blocking.pdf y https://pagefair.com/downloads/2017/01/PageFair-2017-Adblock-Report.pdf

ataques *drive-by* o *wateringhole*, la redirección y los ataques *man-in-the-browser-attacks*.

Como se ha señalado, este tipo de ataques siguió siendo en 2017 una de las amenazas más importantes y lo seguirá siendo en los próximos años[139].

Las primeras extensiones de navegador comprometidas aparecen a mediados de 2017. Varias extensiones de Chrome (incluida *WebDeveloper*, utilizada por desarrolladores web y pen-testers) se comprometieron. El código dañino incluido en *WebDeveloper* permitió a los agentes de las amenazas cargar en el navegador de la víctima código JavaScript servido desde un Dominio DGA[140].

Como hemos mencionado, ciertos servicios de mensajería (Telegram o WhatsApp) sufrieron ataques basados en la web que comprometían los dispositivos, dirigidos a romper el cifrado[141].

Por otro lado, la presencia de JavaScript dañino propicia las descargas *Drive-by*, que pueden infectar un ordenador sin ninguna acción específica por parte del usuario. Según las fuentes que se referencian, dos de las diez amenazas de código dañino más habituales fueron JavaScript[142].

Finalmente, el número de URL maliciosas sigue siendo muy alto. Según los informes que se mencionan[143], en el segundo trimestre de 2017 se identificaron más de 33 millones de URL maliciosas, responsables de la propagación de código dañino en todo el mundo, siendo EE. UU. (32%), Países Bajos (20%), Francia (11%), Finlandia (10%) y Alemania (8%) los países que más alojan recursos dañinos.

Ataques a aplicaciones web

Examinaremos ahora los ataques dirigidos contra aplicaciones web, servicios web y aplicaciones móviles. Su característica común es la pretensión de abuso de las API incorporadas a las aplicaciones web (que, frecuentemente, no están protegidas y contienen numerosas vulnerabilidades).

Las aplicaciones web patrocinadas por el sector financiero y el Sector Público continúan siendo las más atacadas, aunque, en relación con 2016, ha podido observarse un cierto descenso en la frecuencia de tales ataques[144].

139 Véase: https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-sept-2017.pdf

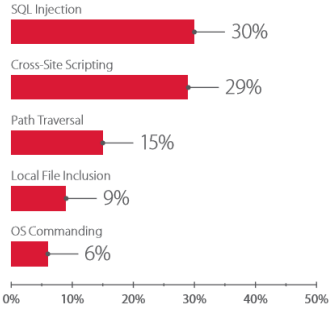
140 Véase: https://www.proofpoint.com/us/threat-insight/post/threat-actor-goes-chrome-extension-hijacking-spree

141 Véase: https://blog.checkpoint.com/2017/03/15/check-point-discloses-vulnerability-whatsapp-telegram/

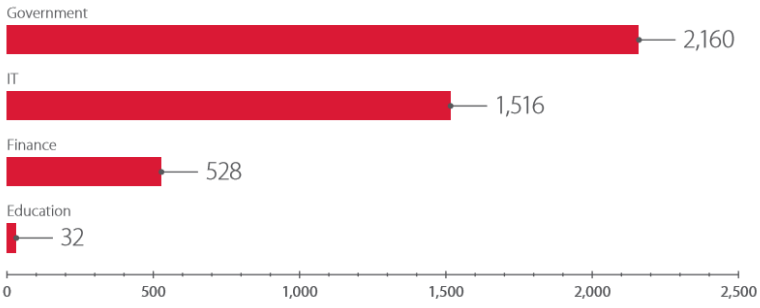
142 Véase: https://www.watchguard.com/wgrd-resource-center/security-report

143 Véase: https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/

144 Véase: https://www.ptsecurity.com/upload/corporate/ww-en/analytics/WebApp-Attacks-2017-eng.pdf

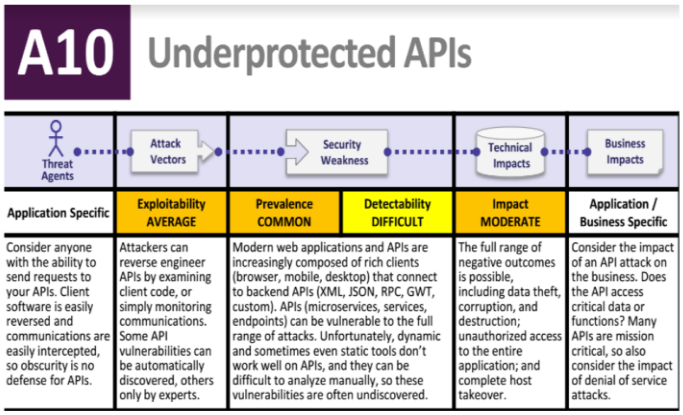


Most common attacks



Average number of attacks per day per company

La Open Web Application Security Project (OWASP) ha incorporado recientemente dos nuevas amenazas a su catálogo[145]: las denominadas *Insufficient Attack Protection* y *Under-protected APIs,* incluyendo, entre otras: SOAP/XML, REST/JSON, RPC y GWT.



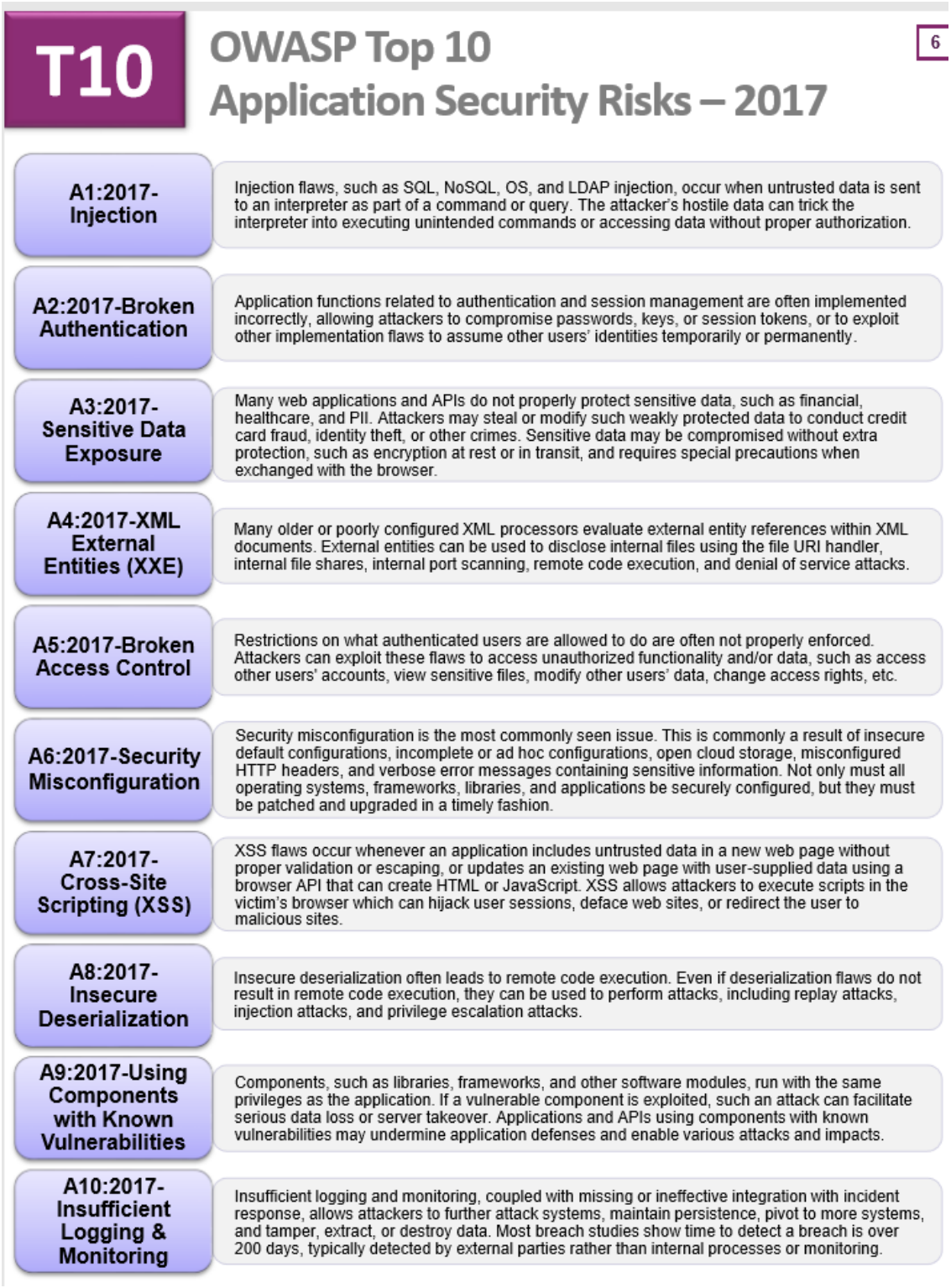
En general, tales ataques se han dirigido contra objetivos conocidos y/o proyectos open-source, tales como plugins de WordPress, sitios de Magento, etc. La forma que tienen de explotar dichos recursos es cada vez más eficiente, construyendo analizadores capaces de explorar y explotar las vulnerabilidades, una vez se han hecho públicas.

Como en años anteriores, la inyección SQL sigue siendo una amenaza importante para las aplicaciones web: los ataques contra APIs están situados en primer lugar de la lista de amenazas OWASP y la protección débil de APIs, en tercer lugar[146].

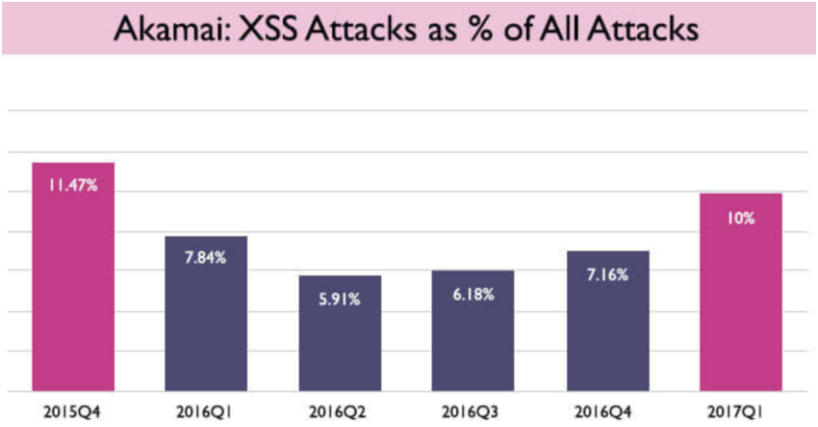
Los ciberataques de tipo inyección (como SQL Injection) siguen siendo la amenaza mejor clasificada por el Open Web Application Security Project (OWASP). En los 10 primeros listados de OWASP, los ataques de API se encuentran en la primera posición, mientras que la protección débil de API ocupa el tercer lugar.

145 Véase: http://sdtimes.com/owasp-adds-unprotected-apis-insufficient-attack-protection-top-ten-2017-release/

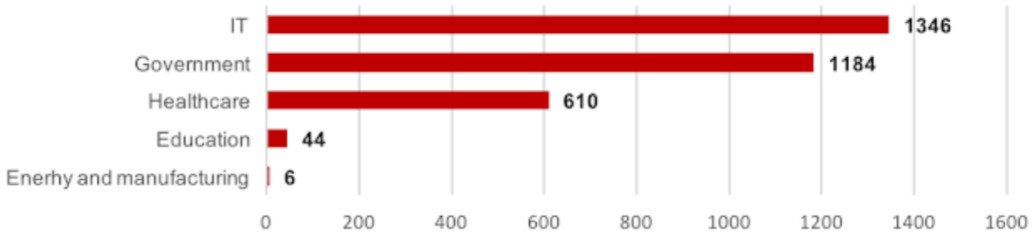
146 Véase: https://www.owasp.org/index.php/Top_10_2017-Top_10


T10
OWASP Top 10
Application Security Risks – 2017
6
A1:2017-Injection
Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2:2017-Broken Authentication
Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
A3:2017-Sensitive Data Exposure
Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
A4:2017-XML External Entities (XXE)
Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
A5:2017-Broken Access Control
Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
A6:2017-Security Misconfiguration
Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.
A7:2017-Cross-Site Scripting (XSS)
XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A8:2017-Insecure Deserialization
Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
A9:2017-Using Components with Known Vulnerabilities
Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
A10:2017-Insufficient Logging & Monitoring
Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Como hemos señalado, los ataques por *Cross-site Scripting* (XSS) crecieron un 39% en el primer trimestre de 2017[147], al tiempo que las vulnerabilidades XSS lo hicieron en un 166% durante 2017.



Finalmente, hay que señalar que durante 2017 los sitios web de las instituciones gubernamentales y las empresas TIC siguen siendo los objetivos preferidos[148]: con un promedio de 1.346 ataques a aplicaciones web en el sector TIC, 1.184 en el sector gubernamental, 610 en el sector sanitario y 44 en el sector educativo.



7.7 Internet of Things-Botnets

Los dispositivos IoT (en muchos casos, electrónica de consumo) disponen, habitualmente, de una seguridad moderada o baja[149]. Además de la escasa robustez en el diseño, esta realidad se debe, entre otras razones, al uso de contraseñas predeterminadas o débiles, a la ausencia de cifrado o a las escasas o inexistentes actualizaciones de software para parchear vulnerabilidades y errores básicos de diseño. Precisamente, estas vulnerabilidades han sido especialmente explotadas en 2017, permitiendo que los dispositivos IoT se hayan utilizado como herramientas para llevar a cabo ciberataques (IoT en botnets), además de para espiar a sus usuarios o para manipular el entorno de los usuarios.

147 Véase: https://snyk.io/blog/xss-attacks-the-next-wave/#high-profile-xss-vulnerabilities-are-not-a-thing-of-the-past

148 Véase: http://blog.ptsecurity.com/2017/09/web-application-attack-statistics-q2.html

149 Véase: http://www.networkworld.com/article/3118759/hackers-found-47-new-vulnerabilities-in-23-iot-devices-at-def-con.html

En septiembre de 2016, se manifestaron los primeros indicios de que los agentes de las amenazas estaban empezando a hacer un uso a gran escala de dispositivos IoT. Ese mismo mes se detectó una botnet IoT que involucraba más de un millón de dispositivos, llevándose a cabo importantes ataques DDoS[150]. Así, el 20 de septiembre de 2016, el sitio web del periodista de seguridad Brian Krebs quedó inactivo debido a un ataque DDoS de 665 Gbps[151], casi dos veces mayor que el ataque más grande conocido. Poco después, el proveedor de hosting OVH sufrió un ataque DDoS de más de 1 Tbps[152].

Aunque los grandes ataques DDoS no son nuevos, lo más significativo de ambas acciones fue que se llevaron a cabo utilizando una gran cantidad de dispositivos IoT comprometidos: routers domésticos, cámaras web y receptores de televisión digital. En 2017 ha habido un par de eventos que confirman esta realidad[153].

Otro aspecto que señalar es la evidencia de que ciertas botnets IoT forman parte de nuevos ataques de ransomware basados en botnets, tales como *Hajime*[154] o muestras más sofisticadas como *Devil's Ivy*[155] o la detección de ataques DDoS-*pulse wave* -capaces de doblar la velocidad de salida de los ataques[156]-.

La posibilidad de perpetrar este tipo de acciones se sustenta en muchas ocasiones en la disponibilidad pública de las herramientas de ataque. Así, por ejemplo,

150 Véase: https://www.strozfriedberg.com/blog/2017-prediction-criminals-harness-iot-devices-botnets-attack-infrastructure/

151 Véase: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

152 Véase: http://securityaffairs.co/wordpress/51726/cyber-crime/ovh-hit-botnet-iot.html

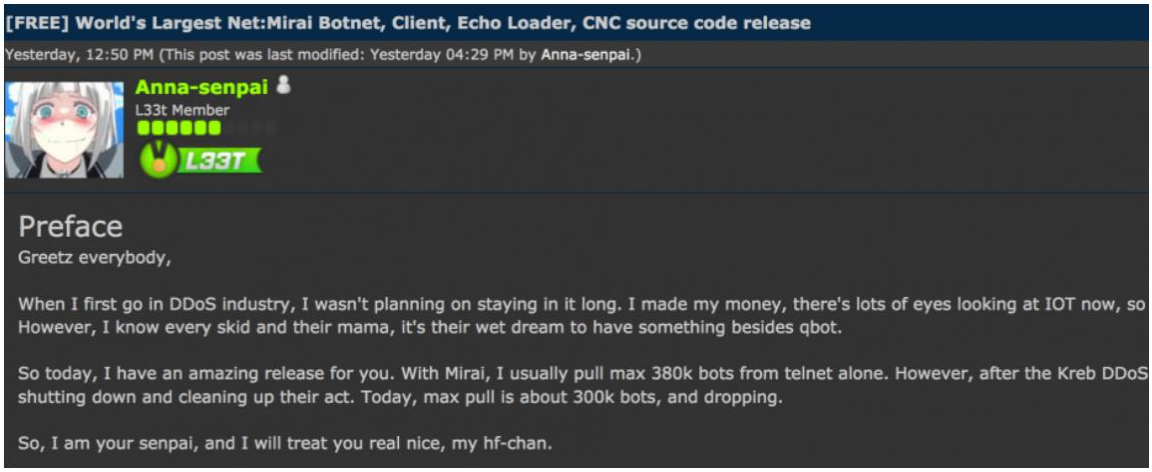
153 Véanse https://arstechnica.com/information-technology/2017/04/brickerbot-the-permanent-denial-of-service-botnet-is-back-with-a-vengeance/ y https://research.checkpoint.com/new-iot-botnet-storm-coming/

154 Véase: https://www.symantec.com/connect/blogs/hajime-worm-battles-mirai-control-internet-things

155 Véase: https://www.wired.com/story/devils-ivy-iot-vulnerability/

156 Véase https://www.incapsula.com/blog/pulse-wave-ddos-pins-down-multiple-targets.html

el código fuente de la botnet *Mirai*, utilizado en el ataque al sitio web de Brian Krebs, se hizo público a finales de septiembre de 2016[157].



Esta difusión pública provocó que los autores del anterior código dañino NyaDrop, menos peligroso, reapareciera, mostrando una técnica de ataque mejorada[158].

En noviembre, 900.000 clientes de Deutsche Telekom fueron víctimas de otra botnet *Mirai*[159], que infectaba los routers Speedport, lo que provocaba la caída de su conexión a Internet. En el mismo mes, se anunció que se había explotado una vulnerabilidad de doce años en OpenSHH para obtener acceso a dispositivos con conexión a Internet[160], que, con posterioridad, se usó para realizar ataques adicionales en otros sistemas.

En el primer trimestre de 2017 se observó un incremento en el uso de botnets y herramientas especializadas de ataque tales como *Ursnif*, *DELoader* y *Zeus Panda*[161]. Por otro lado, la creciente tendencia a la virtualización podría provocar que tales sistemas fueran utilizados como elementos de botnets[162] para eventuales ataques.

Los ataques DDoS perpetrados con la ayuda de dispositivos IoT son muy difíciles de contrarrestar porque, esencialmente, los fabricantes prestan poca o nula atención a la seguridad de tales dispositivos, los usuarios no cambian las contraseñas predeterminadas y el proceso de instalación del dispositivo no lo hace obligatorio. Por

157 Véase: https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

158 Véase: https://www.grahamcluley.com/nyadrop-exploiting-iot-insecurity-infect-devices-malware/

159 Véase: https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/

160 Véase: https://www.theregister.co.uk/2016/10/13/sshowdown_botnet/

161 Véase: https://www.esecurityplanet.com/threats/q1-2017-saw-a-massive-surge-in-botnet-malware-activity.html

162 Véase: https://biztechmagazine.com/article/2017/01/microsoft-warns-hacked-virtual-machines-are-very-real-threat

otro lado, las actualizaciones de software del proveedor para parchear vulnerabilidades todavía no son habituales en dispositivos IoT[163]. Todo ello da como resultado que la creación de botnets IoT sea una empresa relativamente fácil y que puedan permanecer sin ser detectados por el propietario de un dispositivo durante un largo período de tiempo.

A finales de 2017 se descubrió una nueva botnet (denominada *IoTroop*[164]) mediante la acumulación de sistemas de IoT y dispositivos inteligentes como cámaras IP inalámbricas.

7.8 Ataques de Denegación de Servicio (DDoS)

El año 2017 evidenció que los ataques DDoS están en aumento. Según los datos manejados[165], más de un tercio de las organizaciones analizadas se enfrentaron un ataque DDoS, en comparación con el 17% de 2016; una tendencia en alza que evidencia que todas las organizaciones, independientemente del tamaño, están en riesgo de sufrir un ataque DDoS. No obstante, no conviene olvidar que, en ocasiones, este tipo de acciones pretenden ocultar otros tipos de ataques.

Según las mismas fuentes, en la primera mitad de 2017 el 53% de las entidades afectadas por un ataque DDoS afirmaron que se había utilizado para ocultar otros ataques, tales como: infección por código dañino (50%), fuga o sustracción de datos (49%), intrusión de red o piratería (42%) o sustracción económica (26%).

Además, se ha evidenciado que el tamaño de los ataques DDoS se está incrementando y, tal y como se ha mencionado, el número de dispositivos IoT vulnerables contribuyen de manera significativa al aumento en el tamaño de los ataques DDoS[166], sin que sea necesario el uso de técnicas especiales (de amplificación) para aumentar el efecto de tales acciones.

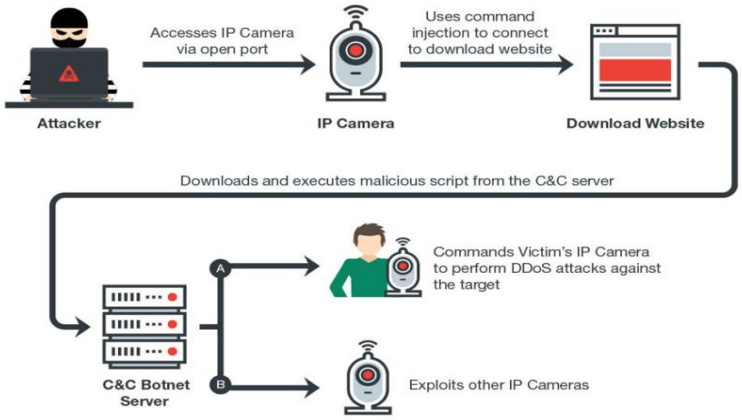
163 Véase: https://www.ietf.org/blog/2016/07/patching-the-internet-of-things-iot-software-update-workshop-2016/

164 Véase: https://research.checkpoint.com/new-iot-botnet-storm-coming/

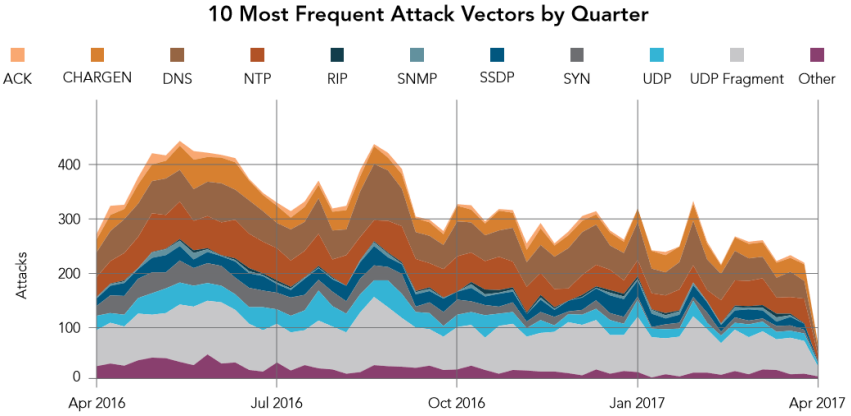
165 Véase: https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-research-shows-ddos-devastation-on-organizations-continues-to-climb

166 Véase: http://www.securityweek.com/iot-botnets-fuel-ddos-attacks-growth-report

En mayo de 2017, TrendMicro informó sobre la botnet *Persirai*, capaz de atacar 100 modelos diferentes de cámaras IP[167] y sustentar ataques DDoS. En la actualidad, se estima que 120.000 cámaras vulnerables están en riesgo de formar parte de una botnet.



A finales de 2017, lal botnet *Mirai* fue protagonista del mayor ataque DDoS de la historia por ancho de banda: más de 1 Tbps[168] contribuyendo de manera decisiva a concienciar a los usuarios a prestar más atención a sus dispositivos IoT y a los propios fabricantes de tales dispositivos. Esto propició que la magnitud de este tipo de ataques volumétricos disminuyera sustancialmente en los meses siguientes, pese al crecimiento anterior de los denominadas "ataques por reflexión" (CLDAP5)[169].



Por otra parte, los ataques DDoS con múltiples vectores de inicialización siguen en aumento. Según las fuentes consultadas[170], el 74% de los ataques DDoS en el segundo trimestre de 2017 utilizó, al menos, dos vectores diferentes[171].

167 Véase: http://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/

168 Véase: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

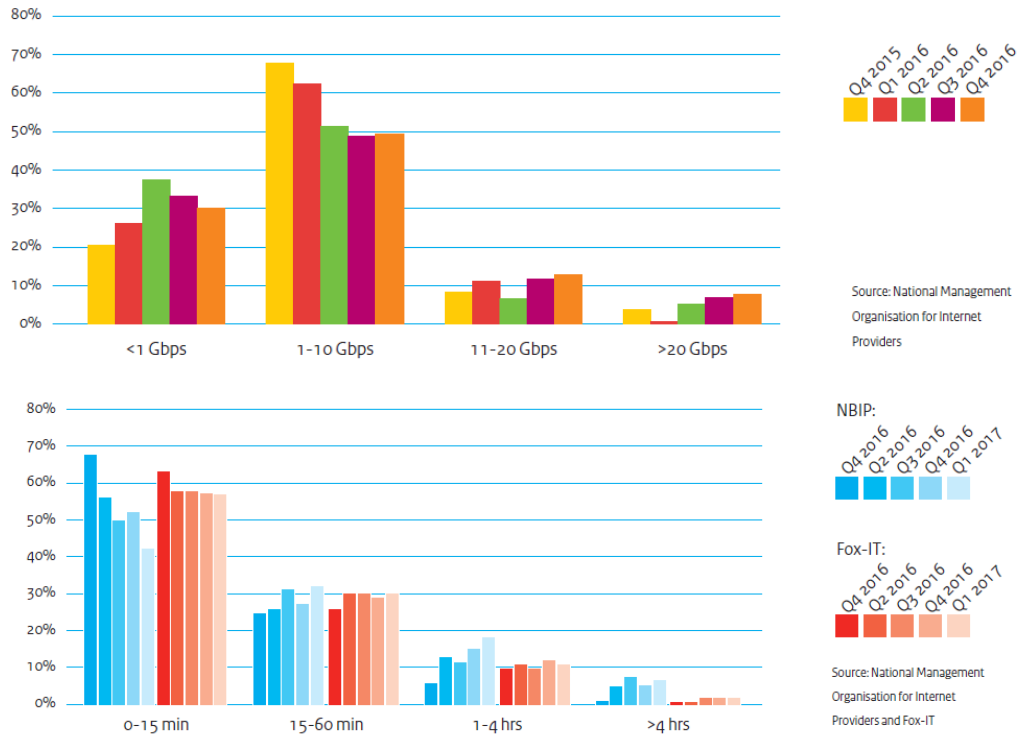
169 Véase: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q1-2017-state-of-the-internet-security-report.pdf

170 Véase: https://www.verisign.com/assets/report-ddos-trends-Q22017.pdf

171 Como fue el caso de la botnet Mirai, que tuvo la capacidad para lanzar múltiples tipos de ataques de inundación TCP y UDP, además de ataques a la capa de aplicación.

Como vaticinábamos en el informe del pasado año, los ataques "*DDoS-as-a-Service*" siguen en pleno desarrollo debido, fundamentalmente, al descenso de los costes de las herramientas precisas para perpetrarlos[172]. Algunos ejemplos fueron los ataques -muy grandes en términos de ancho de banda- al sitio web del periodista Brian Krebs en enero de 2017[173].

Un ejemplo: en 2016 la Organización Nacional de Administración de Proveedores de Internet (NIBP) de Holanda procesó 681 ataques DDoS (casi dos ataques diarios). Más de la mitad de estos ataques tenían un tamaño de entre 1 y 10 Gbps. Aproximadamente, el 5% tenía más de 20 Gbps y alrededor del 30% tenía menos de 1 Gbps. El ataque más grande fue de 53 Gbps y duró 14 minutos. En 2016, más de la mitad de los ataques duró menos de 15 minutos, casi el 5% duró más de cuatro horas y tres de los ataques duraron más de cinco días consecutivos.

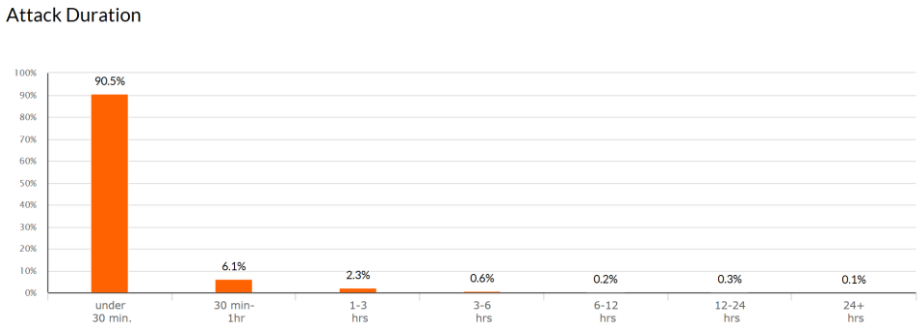


Por otro lado, 2017 evidenció que, aunque el ancho de banda implicado en los ataques DDoS es más pequeño que en años anteriores, se usa de manera más eficiente. Un ejemplo de evolución: si en 2015 el ataque más agresivo se situaba en torno a los 500 Gbps, al final del año 2016 los ataques contra OVH superaron 1Tbps, mientras que

172 Un ejemplo: según https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/ , se estima que los costes de un ataque DDoS de una hora usando recursos de un proveedor de servicios en la nube pueden estar en torno a 4 dólares. Además de ello, algunos operadores ubicados en China ofrecen tales servicios utilizando sitios web que incluyen cuadros de mando que muestran la cantidad de ataques realizados y la cantidad de bots en línea, tal y como se señala en http://blog.talosintelligence.com/2017/08/chinese-online-ddos-platforms.html

173 Véase: https://krebsonsecurity.com/tag/ddos-for-hire/

el ataque de la botnet Mirai contra el sitio de Brian Krebs alcanzó los 620 Gbps. En 2017, en general, pese a que los ataques tendieron a durar menos de una hora -solo ataques muy concretos duraron más de 4 horas-, se utilizaron mecanismos de ráfagas[174], procedimiento que incrementa la tensión en la respuesta de las entidades-víctima.



Finalmente, hay que señalar la identificación de un grupo de hackers turcos que está recompensando a otros para llevar a cabo ataques. Para ello han construido y publicado una herramienta DDoS que otorga puntos a aquellos que atacan un sitio web predeterminado[175]. Así, les permite utilizar el sitio para obtener otras herramientas de hacking.

abdullah-ocalan.com	kurdistanskyscrapers.com	rojavatv.org.uk
bazekurdistan.com	kurdnewshaber.net	rojevakurdistan.org
cmg-team.com	likecin.com	rudaw.net
cmg-team.net	nerinaazad.com	sosyalistforum1.net
dengekobane.com	nextwebtasarim.com	umudayuruyenler.net
gerillatv.net	otherisrael.org	ww7.gerilla.org
halkinbirligi.net	pajk-online.com	www.agire-serhildan.org
hdp.org.tr	pirtukakurdi.com	www.armenian-genocide.org
hezenparastin.net	pkkonline.com	www.breakingisraelnews.com
hpg-photo.com	pkkonline.info	www.cdu.de
jiyan.us	pkkonline-pkk.blogspot.com.tr	www.freeocalan.org
kurd-h-zone.com	rojaciwan.com	www.haberdiyarbakir.net
kurdistana-bakur.com	rojaciwan.eu	yja-star.com

List of targets included in the Surface Defense program [Credit: Forcepoint]

Tras las acciones contra DYN en 2016[176], el año 2017 fue testigo del aumento de los ataques DDoS basados en DNS -ejemplo de ello fueron las acciones contra ciertos medios de comunicación franceses[177]-.

Por otro lado, continúa la penetración de las acciones de extorsión bajo amenaza de ataques DDoS. Por ejemplo, el grupo *Armanda Collective*[178] exigió 315.000 dólares a

174 Véase: https://www.incapsula.com/ddos-report/ddos-report-q1-2017.html

175 Véase: https://www.bleepingcomputer.com/news/security/turkish-hackers-are-playing-a-ddos-for-points-game/

176 Véase: https://blogs.akamai.com/2016/10/dyn-ddos-attack-wide-spread-impact-across-the-financial-services-industry-part-1.html

177 Véase: https://www.bloomberg.com/news/articles/2017-05-10/french-websites-knocked-offline-in-cyber-attack-on-cedexis

178 Véase: https://www.bleepingcomputer.com/news/security/-1-million-ransomware-payment-has-spurred-new-ddos-for-bitcoin-attacks/

siete bancos surcoreanos a cambio de no interrumpir su servicio en línea, mientras que en otras ocasiones los pagos habrían de satisfacerse en bitcoins[179].

Por último, hay señalar que, aunque la mayoría de los ataques son todavía pequeños en comparación con *Mirai*, su volumen ha aumentado en 2017, advirtiéndose que no tienen que ser necesariamente grandes para alcanzar su objetivo final. Debido fundamentalmente a la mayor facilidad para su perpetración, los ataques volumétricos -que representaron en 2017 el 99%- seguirán siendo los más frecuentes frente a aquellos otros dirigidos a la capa de aplicación, cuyo desarrollo exige un conocimiento técnico mayor.

8. MEDIDAS

Aunque todos los países desarrollados están adoptando medidas de seguridad digital, seguir el ritmo de las vulnerabilidades es cada vez más difícil. Este epígrafe describe las principales acciones que se han tomado en el periodo considerado en pos de lograr unos sistemas de información más resilientes.

8.1 Dirigidas a los individuos: empleados y usuarios

Las organizaciones se están involucrando cada vez más en la denominada Shadow IT, esto es, recursos no gestionados directamente por la organización (*Managed Services Providers/Information Sharing and Analysis Center*). Al hacerlo se usan soluciones TIC que no han sido adquiridas a través del procedimiento habitual de compra. La consecuencia es que, en muchas ocasiones, los procesos de gestión no se aplican a tales sistemas, haciendo que su nivel de seguridad no pueda administrarse. El uso de servicios en la nube para Shadow IT comporta riesgos adicionales.

La facilidad de uso, la compartición eficiente de recursos y los ahorros de costes suelen estar detrás de la adopción de soluciones gestionadas. Extendidos ejemplos de ello son el correo electrónico personal, los servicios en la nube (frecuente para el intercambio de archivos), convertidores de archivos on-line y aplicaciones de chat para propósitos comerciales.

Por su parte, los navegadores de Internet están implementando medidas para mantener a los usuarios mejor informados. Por ejemplo, Google Chrome y Mozilla Firefox han anunciado la señalización como inseguros de todos los sitios web que no usen protocolo HTTPS. Inicialmente, los fabricantes de navegadores están optando por mostrar solo comentarios de seguridad cuando una página web HTTP contiene un formulario con un campo de contraseña. Finalmente, los fabricantes pretenden advertir

[179] Por cierto, 2017 fue testigo de nuevos intentos de ataque dirigidos a los exchanges de bitcoin.

del riesgo en todas las páginas http. Aunque al usuario medio puede importarle poco este tipo de notificación en una página web informativa, la medida podría alentar a los propietarios de sitios web a usar https.

Marcar el tráfico HTTP no cifrado como inseguro ayuda a los usuarios a protegerse contra la interceptación de las comunicaciones. Sin embargo, el uso de HTTPS no garantiza que el destino sea quien dice ser. La aparición de certificados *domain validate* garantiza que quien es titular de un nombre de dominio puede solicitar un certificado válido para ese nombre de dominio. Pese a todo, podría engañarse al usuario con nombres de dominio similares a los legítimos.

8.2 Dirigidas a la tecnología

Los mensajes SMS y la autenticación de dos factores

En julio de 2016, el *National Institute of Standards and Technology* (NIST) de EE. UU. publicó un borrador de directrices en el que el uso de mensajes SMS ya no se consideraba adecuado para la autenticación de dos factores[180] alegando que la interceptación de mensajes SMS ha alcanzado un umbral tan bajo para los atacantes que el NIST recomienda considerar otros segundos factores alternativos.

Un ejemplo: en enero de 2017 se detectó un ataque en Asia en el que se interceptaron los códigos TAN para banca-on-line enviados por SMS. El ataque se llevó a cabo utilizando mensajes falsos de acuerdo con el protocolo SS7. La vulnerabilidad de este protocolo se conoce desde hace tiempo y es inherente al tráfico de SMS. Además de interceptar los mensajes SMS mediante la explotación del protocolo SS7, la capacidad de sincronizar mensajes SMS en diferentes dispositivos representa una amenaza en el uso de los SMS para la autenticación de dos factores. Los equipos de investigación han demostrado que tanto Android como iOS son susceptibles a ciberataques en los que se puede acceder a los mensajes SMS recibidos a través del ordenador del destinatario[181].

La explotación de las vulnerabilidades de Internet of Things

Ya se han señalado las vulnerabilidades asociadas a Internet of Things y las consecuencias en el otoño de 2016 de la botnet *Mirai* -consecuencias amplificadas por la publicación del código fuente de la botnet-.

En mayo de 2017, la Comisión Europea publicó una declaración en la que anunciaba medidas para la certificación de dispositivos IoT[182].

---

180 Véase: https://pages.nist.gov/800-63-3/

181 Véase: https://www.vvdveen.com/publications/BAndroid.pdf

182 Véase: https://ec.europa.eu/commission/commissioners/2014-2019/ansip/announcements/statement-vice-president-ansip-pressconference-mid-term-review-digital-single-market-strategy_en

La botnet *Mirai* ha demostrado la posibilidad de desarrollar enormes ataques DDoS, cuyos costes de prevención solo pueden ser asumidos por las grandes organizaciones. Pudiéndose afirmar que todavía no hay una solución clara para los efectos secundarios no deseados de Internet of Things. Pese a los llamamientos hechos para establecer un marco legal para la responsabilidad de los productos involucrados, la falta de sostenibilidad TIC seguirá siendo un problema si el sector no puede regularse a sí mismo[183].

Claridad en las características de seguridad de los productos

La claridad en las medidas de seguridad de los productos es fundamental para garantizar un uso seguro de los mismos. Un ejemplo: en los procedimientos legales contra Samsung, la Asociación de Consumidores Holandesa exigió que se proporcionaran actualizaciones durante, al menos, los dos años posteriores a la compra o cuatro años después de la presentación de nuevos dispositivos Android[184].

Esto es debido a que, conscientes de su importancia, los usuarios sientan exigir requisitos más explícitos y características de seguridad más transparentes. Solo entonces se estará en condiciones de hacer una elección adecuada. Sin la debida transparencia los productos se elegirán, principalmente, en función del precio y la velocidad de introducción en el mercado. Una mayor transparencia brinda a los proveedores la oportunidad de mostrar elementos diferenciadores de la competencia.

Vulnerabilidades esenciales

Pese a que los fabricantes han venido solucionando durante años las vulnerabilidades del software en base a actualizaciones de seguridad, permanece la amenaza de vulnerabilidades más ligadas a la esencia misma del software y que, en consecuencia, son más difíciles de corregir.

Por ejemplo, en agosto de 2016, se anunciaron las vulnerabilidades *QuadRooter*[185] en Android, en los controladores para ciertos chips de diferentes proveedores, entre ellos el chip Qualcomm -muy usual en wifi-.

- BlackBerry Priv
- Blackphone 1 and Blackphone 2
- Google Nexus 5X, Nexus 6 and Nexus 6P
- HTC One, HTC M9 and HTC 10
- LG G4, LG G5, and LG V10
- New Moto X by Motorola
- OnePlus One, OnePlus 2 and OnePlus 3
- Samsung Galaxy S7 and Samsung S7 Edge
- Sony Xperia Z Ultra

Esta vulnerabilidad no puede ser resuelta con un simple parche para Android, sino que debe ser distribuido por el propio fabricante del dispositivo. Puesto que esa

183 Véase: https://d66.nl/content/uploads/sites/2/2016/11/internet-der-dingen-notitie.pdf

184 Véase: https://www.consumentenbond.nl/nieuws/2016/bodemprocedure-tegen-samsung-van-start

185 Véase: http://blog.checkpoint.com/2016/08/07/quadrooter/

circunstancia alarga el tiempo para solucionar el problema, se han hecho públicos algunos consejos dirigidos a los usuarios de Android para mitigar la amenaza[186].

Durante 2016 y 2017 se han publicado diferentes trabajos referidos a la explotación de vulnerabilidades de este tipo. Algunos ejemplos: *Dedup Est Machina* explota la duplicación de memoria para tomar el control de un navegador, *Flip Feng Shui* permite que una máquina virtual atacante penetre en la memoria de otras máquinas virtuales o *ASLR⊕Cache*, que puede usarse para eludir el *Address Space Layout Randomization* (ASLR)[187].

La necesidad del cifrado

La utilización de técnicas de cifrado es cada vez más habitual. Por ejemplo, muchos sitios web ya usan HTTPS, circunstancia que obedece, en parte, al menor coste del hardware y del ancho de banda necesarios y, en algunos casos, la gratuidad de los certificados electrónicos[188]. Conscientes de esta realidad, algún estado europeo (Holanda, por ejemplo) ha decidido hacer obligatorio el uso de HTTPS en todos los sitios web gubernamentales[189].

El uso del cifrado extremo a extremo también se ha extendido a las aplicaciones de mensajería instantánea (WhatsApp o Telegram, entre otras). Esta realidad ha generado una importante demanda de mecanismos de cifrado en todo tipo de aplicaciones.

Por otro lado, el uso creciente del cifrado también requiere la permanente confianza en los proveedores de certificados. Por ejemplo, a finales de 2016, Mozilla, Apple y Google suspendieron la confianza a los proveedores de servicios de certificación WoSign y StartCom.

WoSign estaba infringiendo los acuerdos de confidencialidad al emitir certificados con una fecha de validez pasada sin que, además, diera la suficiente información respecto de la adquisición de su competidor StartCom, lo que obligó a los clientes de ambas compañías a encontrar nuevos proveedores[190].

Pese a todo, el cifrado protege los datos durante un período limitado de tiempo. A medida que los ordenadores son más potentes, el cifrado que alguna vez se consideró

186 Véase: https://www.ncsc.gov.uk/advisory-quadrooter-vulnerability-affecting-android

187 Véanse: https://www.vusec.net/projects/dedup-est-machina/ , https://www.vusec.net/projects/flip-feng-shui/ y https://www.vusec.net/projects/anc/

188 Es el caso de la iniciativa Let's Encrypt. Véase: https://letsencrypt.org/2017/01/06/le-2016-in-review.html

189 Véase: http://www.nu.nl/internet/4399254/plasterk-wil-toch-beveiligde-verbinding-verplichten-alle-overheidssites.html

190 Véase: https://blog.mozilla.org/security/2016/10/24/distrusting-new-wosign-and-startcom-certificates/ , https://support.apple.com/en-us/HT204132 y https://security.googleblog.com/2016/10/distrusting-wosign-and-startcom.html

fuerte deja de serlo. En otras palabras: la implantación de ordenadores cuánticos podría tener importantes consecuencias para los datos actualmente cifrados[191].

8.3 Dirigidas a las Organizaciones

La seguridad de los proveedores

Aunque las grandes organizaciones (públicas y privadas) son, en general, capaces de organizar y gestionar adecuadamente su seguridad a través de políticas, procedimientos y medidas específicas; con frecuencia, sin embargo, hacen uso de proveedores en los que el nivel de madurez es más bajo. Por ejemplo, cuando se adquiere un determinado hardware o software, los requisitos de seguridad suelen estar presentes en los Pliegos o en los Contratos. Sin embargo, los mecanismos de los que pueda disponer los proveedores para garantizar la permanente satisfacción de tales requisitos es, con frecuencia, desconocida, lo que provoca en muchas ocasiones que cambios o actualizaciones posteriores no cumplan con los requisitos de seguridad iniciales[192].

Un caso para la reflexión: La gestión íntegramente en papel de las elecciones en Holanda.

En Holanda, los votos se emiten utilizando papeletas y las papeletas se cuentan manualmente por el Comité Electoral. Por lo tanto, estos procesos no son vulnerables a los ciberataques.

En enero de 2017, se publicaron informes sobre posibles vulnerabilidades en el software de apoyo para elecciones que los municipios, los principales comités electorales y el Consejo Electoral utilizan para procesar los recuentos finales de las mesas electorales[193]. El 1 de febrero de 2017, el Ministro del Interior decidió aplicar medidas para evitar la duda sobre la fiabilidad del resultado de las elecciones[194]. Por lo tanto, se prohibió la transferencia digital de los resultados.

Los ataques por ransomware y DDoS, en el día a día de las grandes organizaciones

Los ataques DDoS o las infecciones por ransomware constituyen ya un lugar común para las grandes organizaciones. Tanto que su mitigación se considera una actividad cotidiana. Estas organizaciones suelen salir airosas de los ataques DDoS invirtiendo en procesos y herramientas de mitigación. Sin embargo, la protección contra ataques a gran escala -como los acaecidos con la botnet *Mirai*- es siempre difícil. Pese a que restaurar desde la copia de seguridad tras una infección por ransomware se ha

191 Véase "Post-quantum cryptography - Protect today's data against tomorrow's threats" Factsheet FS-2017-02 | version 1.1 | 31 August 2017 - NCSC

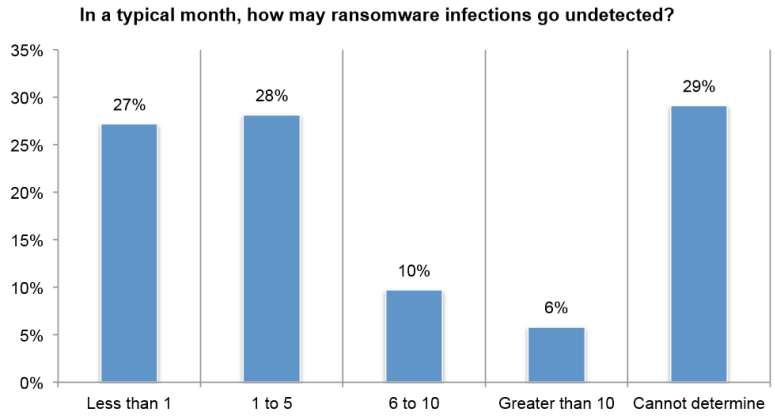
192 Lo que es especialmente delicado en los denominados Operadores de Servicios Esenciales (inlcuyendo las organizaciones del Sector Público) y los Proveedores de Servicios Digitales, en la terminología usada por la Directiva NIS.

193 Véase: https://sijmen.ruwhof.net/weblog/1166-how-to-hack-the-upcoming-dutch-elections,

194 Véase: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2017Z01527&did=2017D03236

convertido en una rutina para muchas organizaciones, estas operaciones de recuperación siguen siendo costosas y lentas y la pérdida de datos no siempre se puede deshacer.

Cuando tales acciones afectan a organizaciones más pequeñas, suele carecerse de la experiencia debida y de los medios económicos para invertir en la mitigación de ataques DDoS y no siempre se cuenta con un mecanismo de copia de seguridad que funcione correctamente para recuperarse de las infecciones por ransomware[195].



Por otro lado, muchas organizaciones pequeñas son vulnerables porque las actualizaciones de seguridad no se instalan a tiempo. Muchos son los estudios que han revelado que estas organizaciones implementan relativamente pocas medidas o son limitadas. Por ejemplo: casi todas las empresas usan software antivirus, pero solo un tercio, o incluso menos, implementan otras medidas tales como tener una política de seguridad de la información, personal capacitado y procedimientos de recuperación para incidentes. Esto es así al mismo tiempo que un altísimo porcentaje de tales empresas sostiene que sus procesos de negocios dependen totalmente de las TIC corporativas.

8.4 El marco estratégico y legal

El marco estratégico europeo en materia de ciberseguridad

A continuación, se muestra la lista de las diferentes estrategias nacionales de la UE con su fecha de su publicación. En ella se aprecia como en 2017 dos estados de la UE (Polonia y Suecia) publicaron una nueva versión de sus respectivas estrategias nacionales de ciberseguridad:

195 Véase: https://www.ponemon.org/local/upload/file/Ransomware%20Report%20Final%201.pdf

Estrategias Nacionales de Ciberseguridad de la Unión Europea[196]

Austria: Austrian Cyber Security Strategy (2013)

Bélgica: Belgian Cyber Security Strategy (2014)

Bulgaria: NCSS of the Republic of Bulgaria (2016)

Croacia: Croatian Cyber Security Strategy (2015)

República Checa: Cyber Security Strategy of Czech Republic 2011-2015 (2011)

Chipre: Cyber Security Strategy of the Republic of Cyprus (2013)

Dinamarca: The Danish Cyber and Information Security Strategy (2015-2016) / Digital Strategy (2016-2020)

Estonia: Estonian Cyber Security Strategy (2014)

Finlandia: Finnish Cyber Security Strategy (2013)

Francia: French National Digital Security Strategy (2015)

Alemania: Cyber Security Strategy for Germany (2011)

Grecia: Greek National Cyber Security Strategy (2017)

Hungría: National Cyber Security Strategy (2013)

Irlanda: Irish National Cyber Security Strategy (2015-2017)

Italia: National strategic framework for cyberspace security (2013)

Letonia: Latvia's Cyber Security Strategy (2014)

Lituania: Programme for the development of electronic information security (cyber security) for 2011-2019 (2011)

Luxemburgo: National strategy on cyber security (2015)

Malta: National Cyber Securty Strategy (2016)

Holanda: National Cyber Security Strategy (2013)

Polonia: National Cyber Security Strategy (2017) / Cyberspace Protection Policy of the Republic of Poland (2013)

Portugal: National Cyberspace Security Strategy (2015)

Rumania: Cyber Security Strategy in Romania (2011)

196 Fuente: ENISA - https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

Eslovaquia: Cyber Security Concept of the Slovak Republic (2015-2020) / Action Plan of Implementation of Cyber Security Concept of the Slovak Republic (2015-2020)

Eslovenia: Slovenian Cyber Security Strategy (2016)

España: The National Cybersecurity Strategy (2013)

Suecia: National Cyber Security Strategy (2017)

Reino Unido: National Cyber Security Strategy (2016-2021)

La lista completa de los países con Estrategia Nacional de Ciberseguridad y sus textos puede encontrarse en este enlace.[197].

El marco legal europeo

El marco legal europeo se está construyendo para imponer obligaciones a los (nuevos) agentes del mercado. Estos agentes están desempeñando un nuevo papel en la sociedad, o están asumiendo parcial o totalmente el papel de actores ya existentes y, a menudo, ya regulados. Por ejemplo, la Comisión Europea ha propuesto reemplazar la directiva **e-Privacy** por una regulación[198] cuyo alcance cubrirá muchos otros servicios de comunicaciones en capas superiores del sistema -como WhatsApp, Facebook Messenger y proveedores de correo electrónico. Además de los tradicionales proveedores de telecomunicaciones[199]-. Con ello se está intentando proteger a los usuarios finales, desarrollando un marco equitativo para los proveedores.

La respuesta, sin embargo, no ha sido pacífica: mientras los actores entrantes se oponen a la regulación, los actores establecidos la apoyan[200]. En los Estados Unidos, por el contrario, la situación es distinta: los actores establecidos están clamando por una menor regulación que les permita competir en el mismo terreno de juego que los recién llegados[201].

El Reglamento Europeo **eIDAS** es un ejemplo de regulación aplicable a los agentes del mercado que desempeñan un papel importante en la sociedad digital: los

197 NATO Cooperative Cyber Defence Centre of Excellence.

198 Véase: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

199 Véase: http://europa.eu/rapid/press-release_IP-17-16_en.htm

200 Véase: https://www.mobileworldlive.com/featured-content/home-banner/facebook-vodafone-in-opposition-over-e-privacy-directive/

201 Véase: https://tweakers.net/nieuws/122729/amerikaanse-senaat-stemt-in-met-verkoop-browsegeschiedenis-door-providers.html

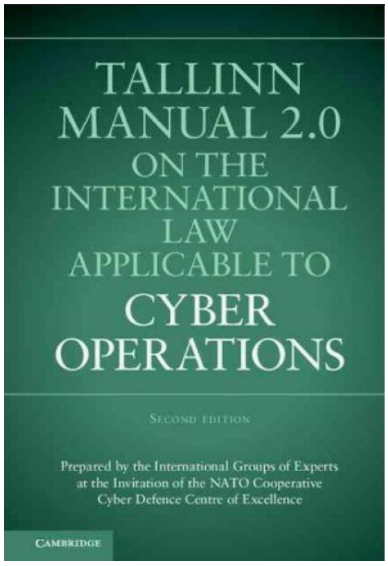
llamados Servicios de Confianza[202]. Este Reglamento constituye la base legal para las firmas electrónicas, sellos, marcas de tiempo, documentos y certificados de sitios web y las responsabilidades de quienes los suministran.

Por su parte, el **Reglamento General de Protección de Datos**, adoptado el 27 de abril de 2016, también comporta nuevas responsabilidades para los procesadores de datos personales, incluso en el ámbito de la seguridad de la información y el diseño de la privacidad[203]. El usuario también tiene derecho a obtener sus datos personales fácilmente y a transferir sus datos a otro proveedor. Un derecho conocido como "portabilidad de datos" que evita el bloqueo del proveedor cuando los usuarios estuvieren vinculados a un único proveedor de servicios.

La importancia de los comportamientos Internacionales en defensa de la democracia

En el período previo a las elecciones al Parlamento de Cataluña, en diciembre de 2017, se manifestaron preocupaciones sobre la posibilidad de que se vieran influenciadas por ciberataques, como ya sucediera en las elecciones presidenciales de EE. UU.

La protección de la soberanía de los países es un principio importante en el derecho internacional. Sin embargo, su interpretación y aplicación en el dominio digital no siempre está clara. El uso del Manual 2.0 de Tallinn sobre la **Ley Aplicable a las denominadas Cyber Operations** puede proporcionar una mayor claridad en la interpretación de las regulaciones actuales[204]. La interpretación de los códigos de conducta puede tener consecuencias de gran alcance. La OTAN ha declarado una vez más que un ataque cibernético podría ser la base para invocar el Artículo 5 (*defensa colectiva*) del Tratado del Atlántico Norte.



La Organización reconoce el dominio cibernético como el cuarto dominio de la guerra[205]. La importancia de las normas internacionales de comportamiento en el ciberespacio está aumentando. Crear mayor transparencia y seguridad jurídica sobre lo

202 Véase: http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32014R0910

203 Véase: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

204 Véase: https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html

205 Véase: http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en

que está permitido y lo que no, así como la respuesta permitida hará que los conflictos futuros sean más manejables.

La transferencia del control de Internet

El 1 de octubre de 2016, el gobierno de EE. UU. transfirió formalmente el control de las funciones esenciales de Internet de la Administración Nacional de Telecomunicaciones e Información de los Estados Unidos a la organización privada ICANN[206]. Para mantener una Internet libre y abierta, se ha establecido una estructura de gestión de la ICANN acorde con el modelo multi-stakeholder, donde -en un intento de lograr una representación equilibrada de diferentes intereses[207]- están representadas las empresas, las autoridades públicas, los expertos técnicos y la sociedad civil.

Sin embargo, no todos los países tienen la misma opinión sobre el papel de los gobiernos en el control de Internet. Los motivos subyacentes suelen ser de naturaleza político-económica y social o las opiniones sobre derechos fundamentales (como la libertad de expresión o los intereses económicos relacionados con la provisión digital global de servicios). Rusia y China, por ejemplo, están persiguiendo un mayor control nacional de la infraestructura de Internet y la información que circula a su través[208]. Según estos países, los estados también deberían ser soberanos en el dominio digital y, por lo tanto, deberían poder ejercer el control.

Sin embargo, todo esto entra en colisión con los principios occidentales sobre seguridad en Internet. En general, los países occidentales (España entre ellos) están a favor de una Internet abierta y sin fragmentar, donde se puedan materializar las oportunidades económicas derivadas de la digitalización global y donde se garanticen los derechos y libertades fundamentales y la seguridad[209].

Disparidad de criterios en torno a la Revelación Responsable de Vulnerabilidades

La revelación de vulnerabilidades de los sistemas, servicios y productos de hardware y software TIC puede tener un impacto importante. La divulgación coordinada de vulnerabilidades o la divulgación responsable es, por lo tanto, un asunto que está

206 Las funciones esenciales de IANA comprenden coordinar y emitir direcciones IP para sistemas autónomos, la gestión de servidores raíz DNS y la gestión de una serie de protocolos de Internet.

207 Véase: https://www.ntia.doc.gov/other-publication/2016/q-and-iana-stewardship-transition-0

208 Véase: https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/

209 Al tiempo de redactarse el presente documento, el Grupo de Trabajo de Derechos Digitales, constituido a iniciativa del Ministerio de Energía, Turismo y Agenda Digital, a través de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, está ultimando la redacción del libro "Derechos Digitales de los Ciudadanos", que se presentará en el Parlamento español. El capítulo 30, redactado por el Dr. Carlos Galán, es el monográficamente dedicado a la Ciberseguridad.

recibiendo una gran atención por parte de todos los actores involucrados. Por un lado, las divulgaciones aseguran que las partes responsables pueden resolver las vulnerabilidades y que los usuarios pueden implementar contramedidas. Por otro lado, las divulgaciones podrían permitir a las partes malintencionadas explotar las vulnerabilidades antes de implementar las debidas soluciones.

El período de tiempo que media entre la revelación de la vulnerabilidad y su solución es un asunto delicado. Por ejemplo, durante el período considerado, *Project Zero* de Google publicó una serie de vulnerabilidades en productos de Microsoft antes de que estuviera disponible un parche[210]. De conformidad con la política de Google *Project Zero*, la publicación automática se produjo 90 días después de que se descubriera la vulnerabilidad y, aunque este hecho podría ir en contra de los intereses de los usuarios al permitir a los agentes de las amenazas explotar las vulnerabilidades detectadas, Google afirmó que su intención es mejorar la velocidad de reacción de la industria; que terminará por beneficiar a todos los usuarios y a la sociedad[211].

Otro punto delicado es la forma en la que se da cierto tipo de informaciones sobre sospechas de vulnerabilidades en los medios de comunicación. Así, por ejemplo, en respuesta a un informe, el diario *New York Times* tuiteó que los servicios de inteligencia podrían eludir el cifrado de WhatsApp, Signal y Telegram, aunque la redacción de la noticia pecó de una excesiva simplificación[212].

Los informes de los medios pueden, por un lado, contribuir de forma importante a la concienciación sobre ciberseguridad, pero, por otro lado, una información poco precisa puede provocar una reacción exagerada de la sociedad que podría reducir la confianza en las tecnologías de la información y en los servicios prestados. Por lo tanto, depende de los medios de comunicación y de los propios periodistas encontrar un adecuado equilibrio entre la importancia que reviste una noticia cuando posee un claro interés público informativo y la introducción de los matices necesarios.

Actualización normativa en España

En España, 2018 ha sido testigo de la publicación de dos nuevas Instrucciones Técnicas de Seguridad:

- Resolución de 27 de marzo de 2018 de la Secretaría de Estado de Función Pública por la que se aprueba la Instrucción Técnica de Seguridad de **Auditoría de la Seguridad** de los Sistemas de Información

210 Véase: https://www.security.nl/posting/505252/Google+onthult+ongepatcht+lek+in+Internet+Explorer+en+Edge

211 Véase: https://googleprojectzero.blogspot.nl/2015/02/feedback-and-data-driven-updates-to.html

212 Véase: https://techcrunch.com/2017/03/07/is-signal-app-safe-wikileaks/

- 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**.

Ambas se suman a las ITS de **Conformidad con el ENS** y de **Informe de Estado de Seguridad**, publicadas con anterioridad.Al tiempo de redactarse este Informe se está culminando el proceso de transposición de la **Directiva (UE) 2016/1148, de 6 de julio, Directiva NIS**, que afectará también al Sector Público, y que, entre otras cuestiones:

- Identificará los Operadores de Servicios Esenciales.
- Las medidas de Seguridad que habrán de aplicar.
- Las Autoridades competentes.
- Identificará los CSIRTs[213] de referencia.
- Asignará al CCN-CERT la coordinación y respuesta técnica en casos de especial gravedad.

Además de ello, y como consecuencia de la plena aplicación del Reglamento (UE) 2016/679, de 27 de abril, de tratamiento y libre circulación de datos personales (Reglamento General de Protección de Datos), se ha elaborado un Proyecto de nueva Ley Orgánica de Protección de Datos que, derogando la vigente, entrará a regular aquellas cuestiones que el RGPD deja a la consideración de los estados miembros.

8.5 La actividad del CCN-CERT

Seguidamente se examinan con brevedad las actividades más significativas de la Capacidad de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT durante 2017. Un servicio que se creó en el año 2006 como CERT Gubernamental Nacional español y cuyas 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

[213] CSIRT: *Computer Security Incident Response Team* (equipo de respuesta a incidentes de seguridad informática). El término CSIRT suele emplearse en Europa en lugar del término protegido CERT, registrado en EE.UU. por el *CERT Coordination Center* (CERT/CC)

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.

Respuesta a los ciberataques

Durante el año 2017, el CCN-CERT, gestionó un total de 26.472 incidentes, frente a los 20. 807 del año 2016 (un 27,22% más) en los sistemas del Sector Público español y de empresas de interés estratégico para el país. Diariamente, el CERT Gubernamental español se enfrentó a cuatro ataques de una peligrosidad muy alta o crítica, en función de la tipología del mismo (tipo de amenaza, origen, perfil de usuario afectado, número o tipología de sistemas afectados, impacto…).

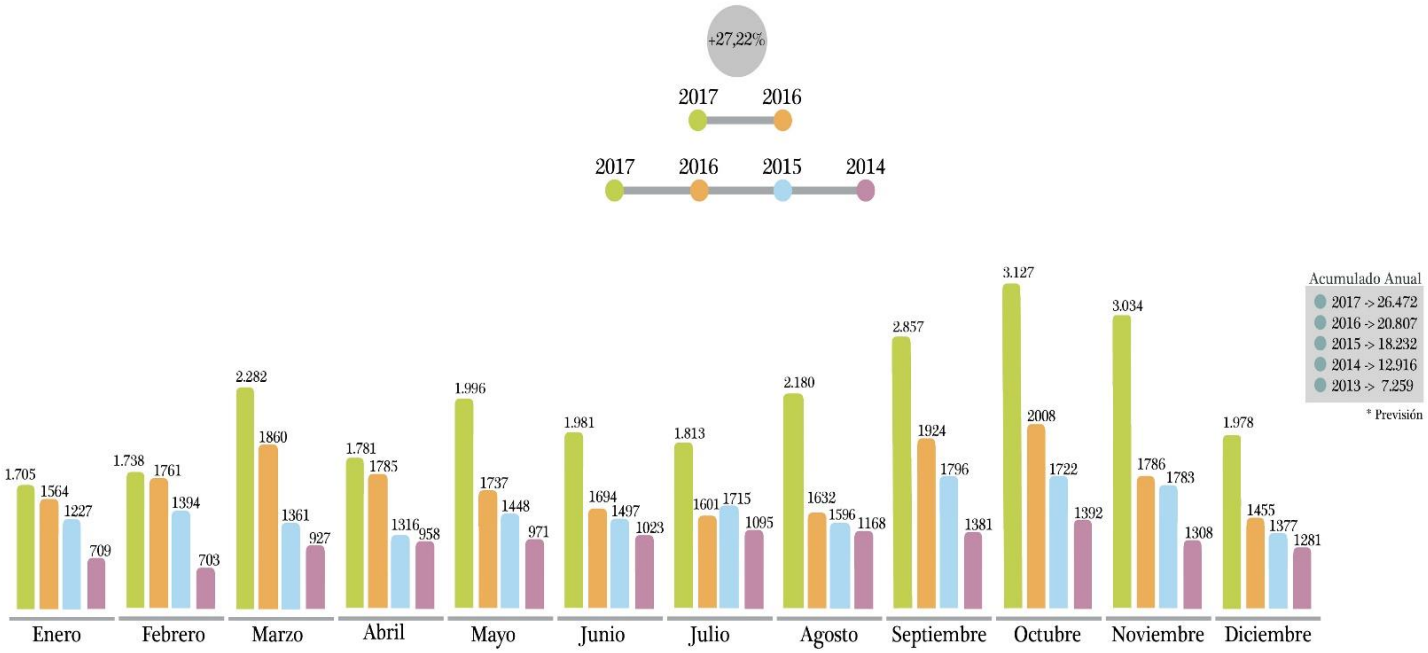
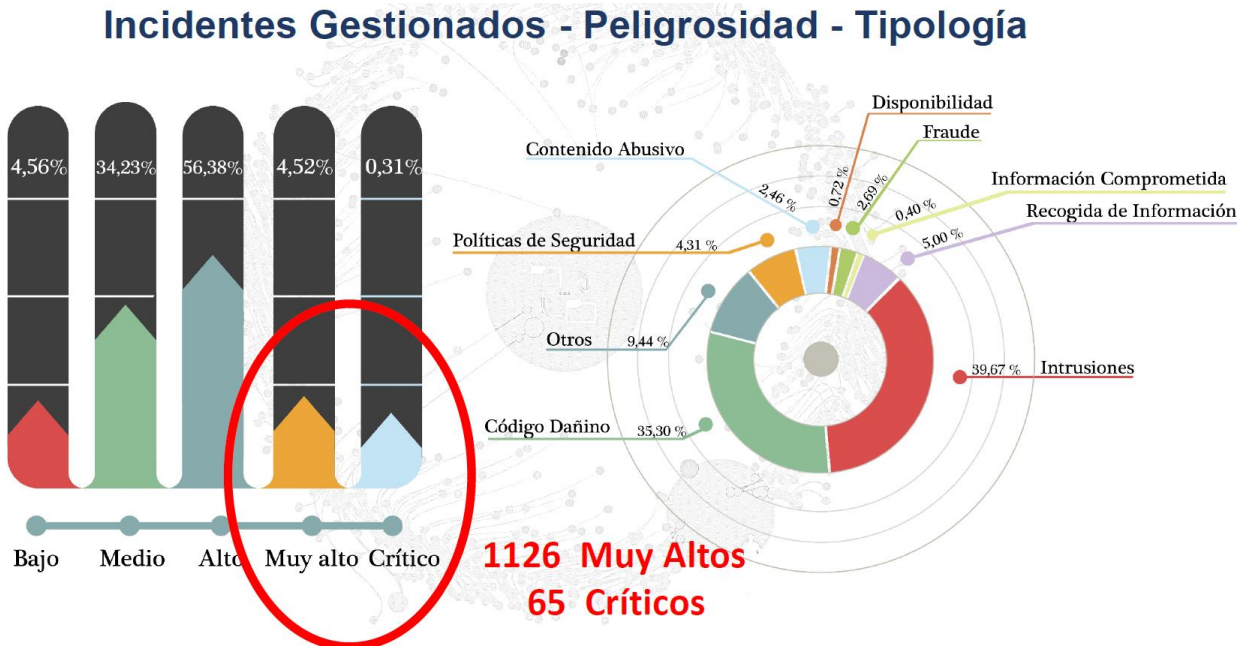


Figura 1. Nº de incidentes gestionados por el CCN-CERT

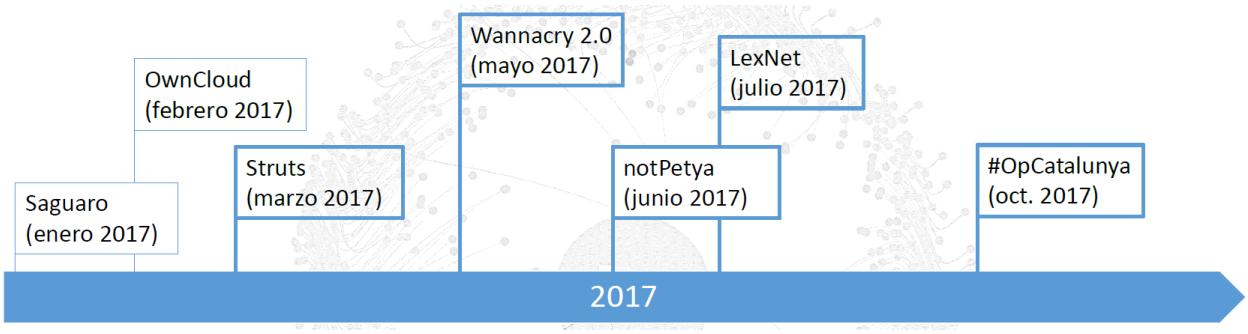
Entre los principales ataques detectados en número, las **intrusiones** (ataques dirigidos a explotar vulnerabilidades e introducirse en el sistema) y el **código dañino** (troyanos, spyaware) fueron los principales vectores de ataque. De hecho, el CCN-CERT ha constatado que la instalación de las actualizaciones o parches de seguridad de las diferentes tecnologías que subsanan las **vulnerabilidades**, es todavía muy lenta. Así, en dos de las crisis más conocidas de este año (la herramienta de desarrollo de aplicaciones web de **Apache Struts** o el ransomware **WannaCry**) los primeros ataques se produjeron dos meses después de conocer la vulnerabilidad. No obstante, son las amenazas persistentes avanzadas, un tipo de ataque que suele estar dirigido y desarrollado con infraestructuras y recursos al alcance de muy pocos, las que más preocupan en el seno del Centro Criptológico Nacional.



Conviene reseñar, además, la eficacia en la actuación del CERT Gubernamental Nacional ante la crisis más mediática de la historia de la ciberseguridad, la infección del ya citado **WannaCry**, el pasado mes de mayo. Entonces, se desarrolló **un parche en tiempo récord,** que fue descargado en más de 50.000 ocasiones en diversos países, entre ellos España, Estados Unidos, Gran Bretaña, Francia, Bélgica o Portugal.

También se registró un incremento importante de ataques de Denegación de Servicio (en gran medida por la campaña contra las Administraciones Públicas y empresas en las cuatro fases de la denominada **#OpCatalunya**) y un aumento del número de variedades de código dañino detectadas, tanto para equipos fijos como, en particular, para las plataformas móviles.

Código dañino



Saguaro (enero 2017) Actor mexicano con intereses económicos y enfocado en el robo de credenciales Uso de múltiples troyanos para crear botnets Varios servidores C2 habían sido registrados en España. Se hizo un DNS sinkholing sobre dichos dominios. ~17.000 bots > 60.000 IPs diferentes afectadas > 36 países afectados	**OwnCloud** (febrero 2017) Suite que permite tener un servidor en una nube privada para compartir archivos, gestionar tareas, reproducir archivos online… Explotación de varias vulnerabilidades, acceso a archivos y ejecución de código... 10 entidades afectadas. Algunas de ellas, siguen siendo vulnerables.
Struts (marzo 2017) Herramienta Apache-Struts El 29 de enero de 2017, se hizo pública una vulnerabilidad con código CVE-2017-5638, que permitiría a un atacante ejecutar órdenes remotas sobre un servidor a través de un contenido subido al componente de análisis JakartaMultipart. El 16 de agosto de 2017 se hizo pública una nueva vulnerabilidad CVE-2017-9805, que afecta a este software, que de la misma forma que la anterior vulnerabilidad, permitiría a un atacante ejecutar órdenes remotas sobre un servidor. Vulnerabilidad que afecta a millones de servidores web conectados a Internet empleados por grandes empresas e instituciones en todo mundo. En España, 75 organismos afectados. 6 de ellos con impacto crítico. 4 equipos desplazados.	**Wannacry 2.0** (mayo 2017) 12.05.2017 se tiene constancia de ciberataque tipo ransomware(WannaCry) 12.05.2017 CERTs nacionales difunden primeras alertas. Primera versión vacuna WannaCry Prevention. Investigación del modo de proceder del código dañino. 13.05.2017 CCN desarrolla vacuna NoMoreCryv0.1. Más de 50.000 descargas. 14.05.2017 se publica informe de código dañino (CCN-CERT ID 17/17 Ransom.WannaCry) Se actualiza NoMoreCrypara WINDOWS XP / 2000. 15/16.05.2015 Vigilancia y coordinación con organismos. Se remiten +90 alertas de conexión a servidores. Se sigue actualizando la herramienta.
NotPetya (junio 2017) Ataque a la cadena de suministro en Ucrania. Propagación desde sedes ucranianas. Destructivo, no ransomware.	**#OpCatalunya** (oct. 2017) Campaña contra AA.PP. y empresas #OpCataluya (4 fases). Más de 70 páginas web atacadas. Ataques de DDoS.

Imposible descifrar los ficheros, aunque se pague el "rescate" Robo de credenciales. ETERNALBLUE para propagación. ¿Demostración de fuerza?	Data Dumps (30 objetivos). Uso de redes sociales e IRC para visibilidad y coordinación. Sin impacto grave (caída breve del servicio web). Ataques: TCPFlood, UDPFlood, HTTP/S Flood, SlowLoris

Centro de Operaciones de Seguridad (SOC) de la Administración General del Estado

En 2017 se crea el Centro de Operaciones de Ciberseguridad (SOC) como instrumento de la Administración General del Estado (AGE) y sus organismos públicos vinculados o dependientes para la consolidación del Servicio Compartido de Seguridad Gestionada. Sus objetivos son:

- Prestación de servicios horizontales de ciberseguridad
- Centralizar servicios, eliminar duplicidades, conseguir un alto grado de especialización y reducir los costes individuales en todos los organismos adheridos.
- Aumentar la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas de información y telecomunicaciones de la Administración
- Mejorar su capacidad de respuesta ante cualquier ataque.

La responsabilidad sobre el Centro de Operaciones de Ciberseguridad corresponde a la Secretaría General de Administración Digital (SGAD) y la operación correrá a cargo del CCN-CERT.

El SOC tiene por objeto proporcionar protección de manera centralizada mediante la dotación de una infraestructura global y única que incluye el equipamiento necesario, así como su configuración, puesta en marcha, mantenimiento, monitorización y gestión de incidentes de ciberseguridad.

- Servicio de Alerta Temprana (SAT).
- Detección, respuesta coordinada y soporte a la resolución de incidentes de seguridad.
- Soporte a la investigación de ciberataques y ciberamenazas.
- Operación, monitorización y actualización de dispositivos de defensa perimetrales: Cortafuegos de nueva generación (NGFW), Acceso remoto por Red Privada Virtual (VPN), Servicio anti SPAM, Cortafuegos de aplicaciones Web (WAF), Resolución segura de nombres de dominio (DNS), Sistema de base común de tiempos (NTP) y Gestión y correlación de eventos de seguridad (SIEM).
- Análisis de vulnerabilidades de aplicaciones y servicios.
- Servicios anti-abuso de identidad digital.

El cronograma previsto de actuaciones es el siguiente:

- Fase1 (1º semestre 2018).
  - Determinación de tecnologías para los diferentes dispositivos del SOC.
  - Definición de los parámetros y niveles de servicio.
- Fase1 (2ºsemestre). Inicio de la instalación del equipamiento.
  - Adquisición e instalación de la infraestructura técnica.
  - Implantación de servicios básicos de ciberseguridad.
  - Incorporación de primeras entidades.
- Fase2 (durante 2019). Extensión del servicio.
  - Extensión del servicio a todo el ámbito de aplicación del Acuerdo del Consejo de Ministros (ACM)
  - Inclusión de nuevos servicios avanzados de ciberseguridad.
- Fase3 (años posteriores a 2019). Mantenimiento y mejora del servicio.

Formación

En el ámbito del Sector Público, el CCN ha continuado concienciando y formando a funcionarios y empleados públicos, a través de tres modalidades de curso: presencial (20 cursos publicados en el BOE y aquellos desarrollados "ad hoc" para algún organismo nacional o internacional), online (seis cursos disponibles en su portal web, con 1.295 horas lectivas) y, su novedad en 2017, formación a distancia, con la Plataforma Vanesa, con la que se ha conseguido llegar al personal de las Comunidades Autónomas y Entidades Locales a los que les costaba desplazarse a Madrid para los cursos presenciales. La nueva plataforma, con 13 sesiones, ha tenido una magnífica acogida, alcanzando en total a más de 1.200 personas (algunos de los cursos, como el de implantación de HTTPS o Actualizaciones de Seguridad en Windows tuvieron que repetirse ante el gran número de solicitudes recibidas).

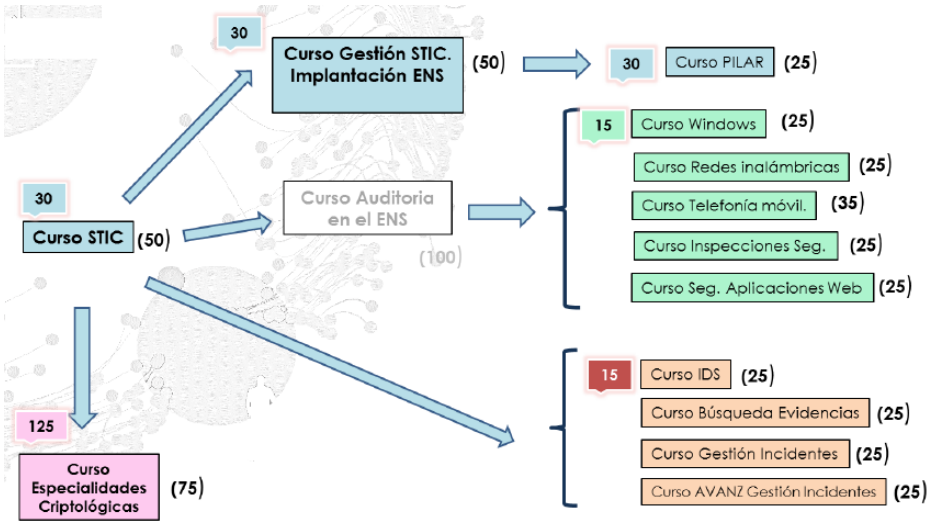
- Cursos:

XIII Curso STIC
XI Curso Básico STIC Infraestructura Red
IX Curso STIC Búsqueda Evidencias
VIII Curso STIC Seguridad App Web
XI Curso STIC Inspecciones Seguridad
XIII Curso STIC Acreditación Windows
XI Curso Básico STIC BBDD
XXVII Curso Especialidades Criptológicas
I Curso STIC Gestión Incidentes
XIII Curso Gestión STIC
XII Curso STIC Detección Intrusos (IDS)
XI Curso STIC Seg. Redes Inalámbricas
VII Curso STIC Herramienta PILAR
V Curso STIC Dispositivos Móviles
II Curso STIC Gestión Incidentes

Curso PILAR Ad-Hoc para el EA
Curso STIC Ad-Hoc para la DGP
Curso STIC Ad-Hoc para el CNI
Curso STIC Ad-Hoc República Dominicana
Curso Ad-Hoc Comunicaciones Seguras México
Curso Acreditación Empresas (ONS)
13 sesiones teleformación plataforma VANESA

Cursos On-Line (Plataforma Web)
Curso básico LINUX
Introducción al ENS
Curso INES
Curso básico WINDOWS
Curso STIC
Curso PILAR

- Itinerarios formativos:



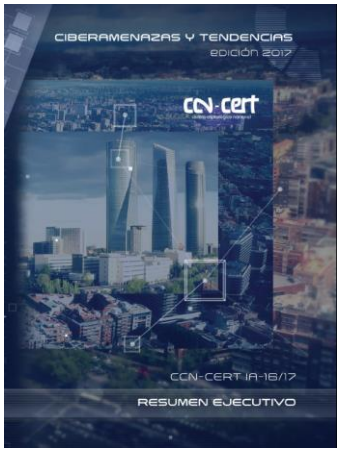
- Formación a distancia: Plataforma Vanesa:

FECHA	CURSO	USUARIOS REGISTRADOS	ACCESOS
17 mayo	Herramienta LUCIA	34	30
5 junio	Código Dañino	35	30
6 junio	Herramienta CLARA	33	30
11 julio	Herramienta PILAR	48	29
13 julio	Herramienta ROCIO	36	20
26 julio	HTTPS	197	150
27 julio	HTTPS	217	153
6 septiembre	Herramienta REYES	74	56
7 septiembre	Actualizaciones Seg. Windows	396	220
9 octubre	Actualizaciones Seg. Windows	391	100
10 octubre	Herramienta MARTA	96	60
11 octubre	Captura de Evidencias	474	132
7 noviembre	Big Data	489	275

Guías CCN-STIC e Informes:

Esta labor de formación se ha completado con la difusión de diferentes informes y boletines de seguridad, mensuales y temáticos, entre los que destacan algunos de los **informes de Buenas Prácticas** (Principios y Recomendaciones Básicas de Seguridad o Recomendaciones de implementación de HTTPS), los de **código dañino** con Indicadores de Compromiso (IoC), de acuerdo a estándares reconocidos por la comunidad internacional o el **Informe Anual de Ciberamenazas 2016 y Tendencias 2017**, en el que se analiza en profundidad el panorama nacional e internacional de la ciberseguridad.

Del mismo modo, este año, y en colaboración con la **Federación Español de Municipios y Provincias (FEMP),** el CCN elaboró **dos Guías de Seguridad para facilitar la implantación del ENS en todas las Entidades Locales** (incluyendo un tomo destinado a Ayuntamientos de menos de 2.000 habitantes).



Asimismo, se ha ampliado la serie de **Guías CCN-STIC**; un conjunto de normas, procedimientos y directrices técnicas necesarias para garantizar la seguridad de las tecnologías de la información en el ámbito de la Administración, que consta actualmente de **296 guías y 441 documentos**. Durante 2017 se han generado o actualizado un total de 51 guías. De este conjunto destaca la serie CCN-STIC 800, que se ha elaborado conjuntamente entre el Ministerio de Hacienda y Función Pública y el CCN, y la nuevas Guías CCN-STIC 101, 105 y 106 relacionadas con el Catálogo de Productos STIC, CPSTIC. Este catálogo, de nueva creación, recoge los "Productos Aprobados" para el manejo de información clasificada y los "Productos Cualificados" para el manejo de información sensible, supervisados por el CCN, de forma que puedan servir de referencia para la Administración Pública.

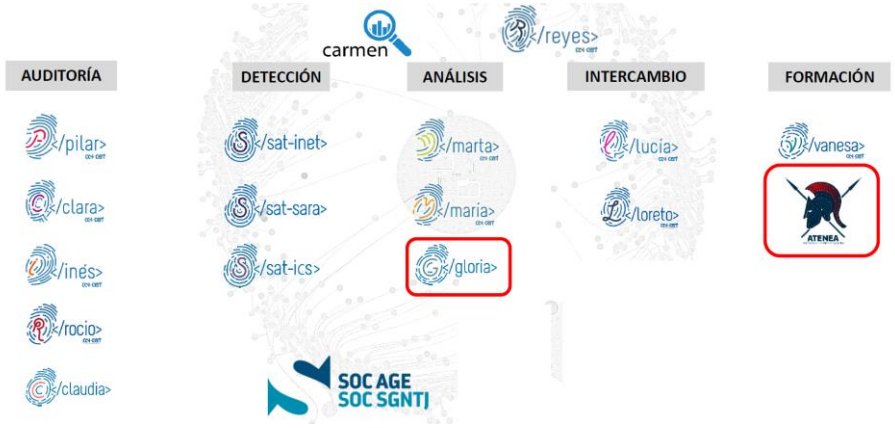
En resumen, fondo editorial:

- 296 Guías CCN-STIC y 441 Informes y documentos especializados.
- 29 nuevas Guías y actualización de otras 22
- 30 Informes de Amenazas.
- 27 Informes de Código Dañino
- 57 Informes Técnicos
- 3 Documentos de Buenas Prácticas
- Guía del ENS para Entidades Locales (auspiciada por la FEMP)

Vulnerabilidades, Alertas y Avisos:

- 20 Alertas
- 19 Avisos
  - Entre ellos: Apache-Struts, Microsoft, NotPetya, WannaCry, Bluetooth, WPA2, #OPCatalunya.

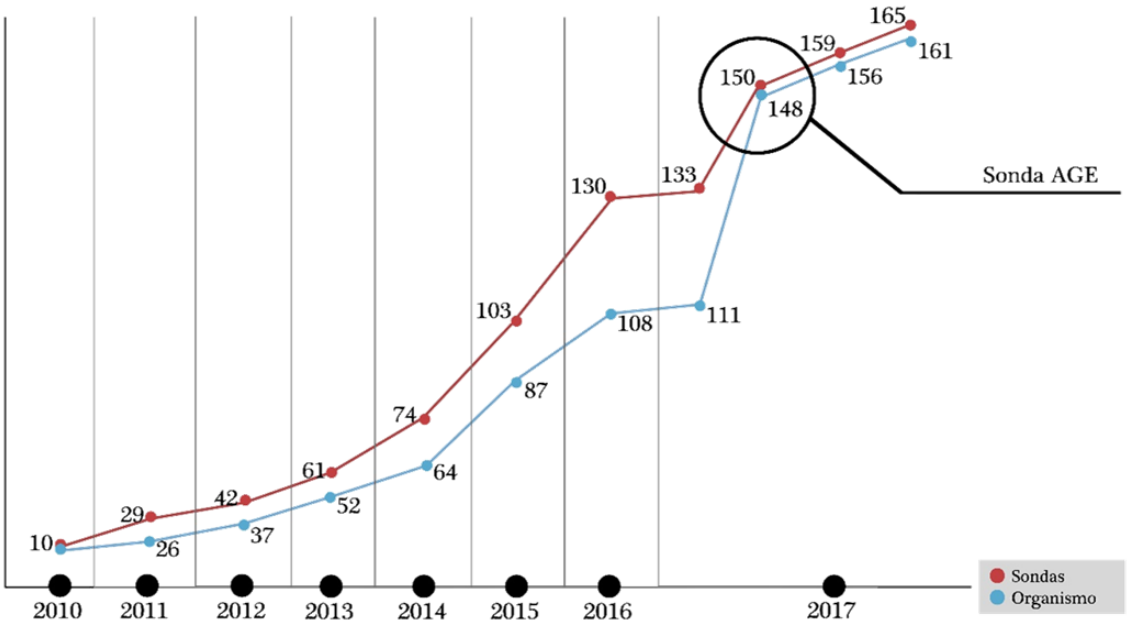
Herramientas de seguridad:



Detección – Sistemas de Alerta Temprana

Para mejorar la capacidad de detección de incidentes e intrusiones, se ha continuado desarrollando el **Sistema de Alerta Temprana (SAT)** en sus dos vertientes: en la intranet administrativa (**SAT SARA**) en la que se ha actualizado la tecnología y se ha desarrollado un nuevo gestor de logs, y en la conexión a Internet de los organismos (**SAT INET**), con la novedad que ha supuesto la puesta en funcionamiento de la Sonda de la AGE (con 25 organismos saliendo a través de ella). Además, se ha desarrollado el **SAT-ICS** para Sistemas de Control Industrial destinado a sectores estratégicos como aguas, puertos, confederaciones hidrográficas y transporte.

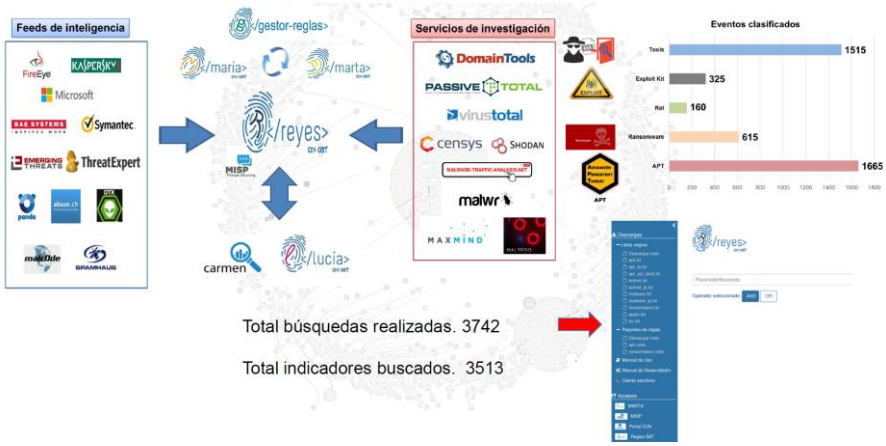
De igual forma, en el SAT INET se ha continuado ampliando el despliegue de sondas en las salidas de Internet de los organismos y empresas estratégicas, orientadas a la detección en tiempo real de las amenazas existentes en el tráfico que fluye entre sus redes internas e Internet. A finales de 2017, este servicio contaba con capacidad de detección en **161 organismos** de las distintas administraciones públicas y organizaciones de interés estratégico, con un total de *165 sondas instaladas* (teniendo en cuenta la mencionada Sonda de la AGE por la que salen 25 organismos). Durante este año se ha ampliado el servicio ofrecido por el SAT de Internet a las Comunidades Autónomas, Entidades Locales y Universidades, una vez completada la adhesión de la mayor parte de los organismos de la Administración Central.



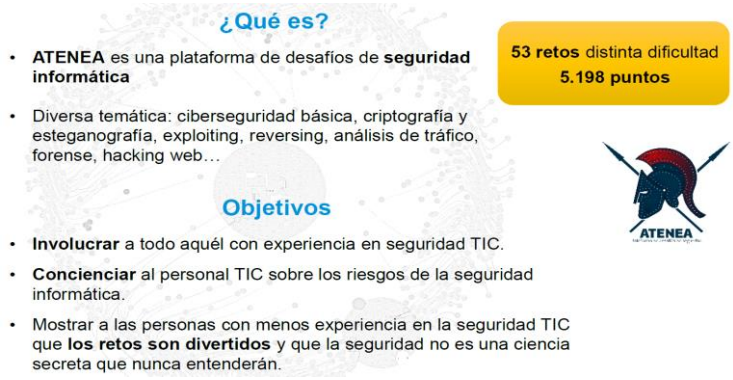
Despliegue de sondas y organismos

Notificación de ciberincidentes – Herramienta LUCIA

Reyes 2.0

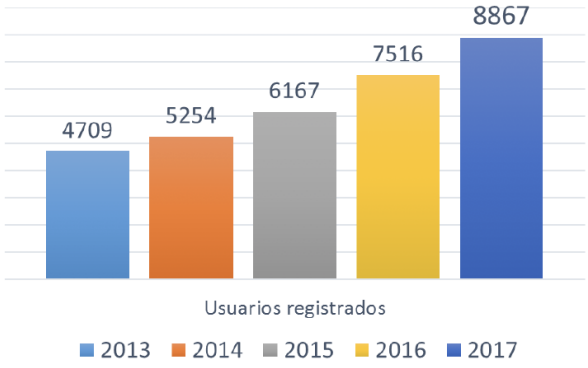


ATENEA



Portal CCN-CERT

Toda la actividad recogida en estas páginas puede consultarse en el portal del CCN-CERT. Un website en la que están registrados cerca de 9.000 personas.



CSIRT.es

Durante 2017, el CCN-CERT promovió el grupo de CSIRT/CERT, una plataforma independiente de confianza y sin ánimo de lucro compuesto por aquellos equipos de respuesta a incidentes de seguridad informáticos cuyo ámbito de actuación o comunidad de usuarios en la que opera, se encuentra dentro del territorio español.

Proteger el ciberespacio español, intercambiando información sobre ciberseguridad y actuar de forma rápida y coordinada ante cualquier incidente que pueda afectar simultáneamente a distintas entidades en nuestro país, es el principal objetivo del Foro CSIRT.es

- Andalucía CERT
- Caixabank CSIRT
- CCN-CERT
- CERTSI
- CertUC3M
- CESICAT-CERT
- CNPIC
- CSIRT.gal
- CSIRT-CV
- CSIRT GLOBAL
- TELEFONICA
- CSUC-CSIRT
- esCERT-UPC
- ESP DEF CERT
- eSOC Ingenia
- EULEN-CCSI-CERT
- Everis CERT
- Guardia Civil
- InnoTec, Entelgy-CSIRT
- MAPFRE-CCG-CERT
- MNEMO-CERT
- NestleSOC
- Policía Nacional
- PROSEGUR CERT
- RedIRIS
- RENFE CERT
- S2 Grupo CERT
- S21sec CERT
- UCIBER - Mossos d'Esquadra

8.6 La actividad europea

De la actividad legislativa de las Instituciones de la UE, en 2017 destacó la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a ENISA, la "Agencia de Ciberseguridad de la UE", y por el que se deroga el Reglamento (UE) n.º 526/2013, y relativo a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación ("Reglamento de Ciberseguridad – *Cibersecurity Act*")

Como se señala en el propio texto, la UE ha adoptado una serie de medidas para incrementar la resiliencia y mejorar su preparación en materia de ciberseguridad. Desde el establecimiento de la Estrategia de Ciberseguridad de la UE, se han producido acontecimientos importantes, en particular el segundo mandato de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) y la adopción de la Directiva NIS sobre seguridad de las redes y los sistemas de información, que constituyen la base de la propuesta citada.

En 2016 la Comisión Europea adoptó la Comunicación "Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora". En ella anunciaron nuevas medidas para intensificar la cooperación, la información y la puesta en común de conocimientos y para incrementar la resiliencia y preparación de la UE, teniendo también en cuenta la perspectiva de incidentes a gran escala y una posible crisis paneuropea de ciberseguridad. En este contexto, la Comisión anunció que presentaría la evaluación y revisión del Reglamento (UE) n.º 526/2013 del Parlamento Europeo y del Consejo relativo a ENISA y por el que se deroga el Reglamento (CE) n.º 460/2004. El proceso de evaluación podría conducir a una posible reforma de la Agencia y a un reforzamiento de sus facultades y capacidades para apoyar a los Estados miembros de manera sostenible. Le conferiría, por tanto, un papel más operativo y central para lograr la resiliencia en materia de ciberseguridad y reconocería en su nuevo mandato las nuevas responsabilidades de la Agencia en virtud de la Directiva NIS.

La propuesta de Reglamento establece un conjunto de medidas que se basan en actuaciones anteriores y fomentan objetivos específicos que se refuerzan mutuamente:

- Aumentar las capacidades y la preparación de los Estados miembros y de las empresas
- Mejorar la cooperación y la coordinación entre los Estados miembros y las instituciones, órganos y organismos de la UE
- Aumentar las capacidades a nivel de la UE para complementar la acción de los Estados miembros, en particular en caso de cibercrisis transfronteriza
- Aumentar la sensibilización de los ciudadanos y las empresas sobre las cuestiones relacionadas con la ciberseguridad
- Aumentar en general la transparencia de la garantía de ciberseguridad de los productos y servicios de TIC, a fin de reforzar la confianza en el mercado único digital y en la innovación digital
- Evitar la fragmentación de los sistemas de certificación en la UE y de los requisitos de seguridad y criterios de evaluación conexos en los distintos Estados miembros y sectores.

Al objeto de establecer y preservar la confianza y la seguridad, la UE considera que es preciso que los productos y servicios de TIC incorporen directamente las características de seguridad en las etapas iniciales de su diseño y desarrollo técnicos (seguridad a través del diseño). Por otra parte, los clientes y usuarios necesitan poder comprobar el nivel de garantía de la seguridad de los productos y servicios que compran o adquieren.

La **certificación** (consistente en la evaluación formal de los productos, servicios y procesos por un organismo independiente y acreditado en función de un conjunto de criterios claramente definidos y la expedición de un certificado que atestigüe la conformidad) desempeña un papel importante a la hora de aumentar la confianza y la seguridad en los productos y servicios. Mientras que la evaluación de la seguridad tiene un carácter bastante técnico, la certificación cumple el objetivo de informar y tranquilizar a los compradores y usuarios sobre las propiedades de seguridad de los productos y servicios de TIC que compran o utilizan.

Como ya se ha dicho, para las Instituciones de la UE esto reviste especial importancia en el caso de los nuevos sistemas que hacen amplio uso de las tecnologías digitales y que requieren un alto nivel de seguridad, como los automóviles conectados y automatizados, la sanidad electrónica, los sistemas de control de la automatización industrial las redes inteligentes.

9. TENDENCIAS

Teniendo en cuenta la evolución de los ciberincidentes en el periodo considerado, es de esperar que los futuros ciberataques incrementen su grado de sofisticación, de virulencia y de osadía. Los siguientes son algunos ejemplos que desarrollan sumariamente las tendencias de un inmediato futuro:

Ataques por Denegación de Servicio (DoS-DDoS):

A la vista de lo ocurrido en 2017 y los primeros meses de 2018, todo apunta al aumento de este tipo de ataques, con algunas variantes: **Denegación de Servicio Permanente (PDoS)** para las operaciones de Centros de Datos y dispositivos IoT, mayor importancia y sofisticación de los **ataques DoS de telefonía (TDoS)** y el aumento de segmentación (e incluso personales) de los ataques de denegación de servicio combinados con ciber-rescate (Ransom-DoS), y con los sistemas de sanitarios como posibles objetivo[214].

Exploits-kits:

A pesar de incluir complejos mecanismos de filtrado para ocultar las actividades dañinas, los agentes de las amenazas que usan exploits-kits descubrieron que escalar sus ataques puede presentar muchos riesgos de detección para las cargas desplegadas. Esto podría justificar la disminución de la tendencia a exploits-kits; que no obstante

[214] Los ataques WannaCry y Petya de 2017 representaron claros ejemplos de la combinación de ataques DoS y Ransomware.

seguirán siendo usados en aquellas regiones geográficas donde no puedan ser monitoreados por los investigadores[215].

Por otro lado, los exploits-kits darán paso a "kits humanos". Teniendo en cuenta que en los últimos años ha venido disminuyendo el número total de vulnerabilidades atacables, los agentes de las amenazas cambiarán su modelo comercial -e, implícitamente, su arsenal- para lograr sus objetivos atacando las debilidades humanas.

Ciberespionaje:

Durante el próximo período, los expertos esperan un crecimiento en el ciberespionaje debido a desencadenantes geopolíticos o sanciones económicas, pero también, debido a los objetivos estratégicos de las naciones. Los agentes de las amenazas, desde el crimen organizado hasta los Estados-nación, están creando nuevas técnicas y herramientas para intentar robar la propiedad intelectual y los secretos de sus objetivos. Estos adversarios seguirán usando APTs.

Ransomware:

Tras la distribución masiva de código dañino, incluso a través de dispositivos móviles, el próximo futuro será testigo del incremento de ataques dirigidos contra objetivos concretos, por ejemplo, contra dispositivos sanitarios tales como marcapasos. Como se ha dicho: "En lugar de solicitar el pago de un rescate para recuperar sus datos, será un rescate para salvar su vida"[216].

Además de ello, TrendMicro ha vaticinado que los atacantes "ejecutarán campañas de extorsión digital y usarán ransomware para amenazar a las organizaciones que no cumplen con RGPD".

Incremento de las brechas de seguridad:

Los casos de brechas de datos de las compañías Uber y Equifax en 2017 no serán casos aislados. Muchos analistas[217] coinciden en señalar que en los próximos meses se producirán significativas brechas de seguridad que podrán afectar, al menos, a 100 millones de cuentas. Una amenaza que según Imperva se extenderá a la filtración masiva de datos en la nube.

Por su parte, la empresa eSentire ha señalado que "los ciberataques de espionaje y de motivación política seguirán aumentando". También se advierten de que "existe el

[215] Véase: https://www.proofpoint.com/us/threat-insight/post/cybersecurity-predictions-2017

[216] Véase: https://www.infosecurity-magazine.com/news-features/cybersecurity-predictions-2018-one/

[217] Entre ellos, Tyler Moffitt, de Webroot.

riesgo potencial de pérdida de vidas humanas como resultado de ciberataques selectivos, especialmente en el sector de la salud ".

El Reglamento General de Protección de Datos:

Desde Digital Pathways se ha señalado que la escasez de personal afectará la adopción del RGPD: "muy especialmente debido a la exigencia del Delegado de Protección de Datos", añadiendo que “solo el 10% de las compañías estarán listas para abordar el RGPD”, por lo que no sería de extrañar que, a finales de 2018, seamos testigos de los cierres de las primeras compañías debido a las significativas sanciones derivadas del incumplimiento del RGPD.”

La adopción de la biometría:

La adopción de tecnología biométrica ha aumentado significativamente en los últimos años, muy especialmente de la mano de la autenticación mediante huellas dactilares y, más recientemente, el reconocimiento facial en los dispositivos móviles. Sobre este particular, el Instituto SANS ha recordado que: "Un gran número de consumidores utiliza de forma rutinaria la autenticación biométrica en sus teléfonos móviles y el 28% de los mismos usa autenticación de dos factores en al menos una cuenta personal".

La empresa Webroot cree que habrá un crecimiento continuo en los servicios biométricos y, como resultado, los accesos a dispositivos basándose en *nombres de usuario* y *contraseñas* se convertirán poco a poco en una segunda opción. Esta misma empresa señala que en los próximos meses veremos los primeros exploits dirigidos al acceso biométrico sustentado en reconocimiento facial o mediante huellas dactilares.

Inteligencia Artificial y Aprendizaje Automático:

Parece claro que las inversiones en tecnología analítica serán mayores a medida que las empresas encuentren nuevas formas de dar sentido a la gran cantidad de datos generados por dispositivos inteligentes. FireEye cree que la industria de la seguridad comenzará a utilizar más automatización, aprendizaje automático e inteligencia artificial para combatir los ciberataques, provocado fundamentalmente por la carencia de personal especializado.

Por su parte, la empresa SolarWinds ha vaticinado que la integración de la inteligencia artificial y las capacidades de aprendizaje automático se percibida como crítica para el éxito empresarial en los próximos años y aunque preparada para ofrecer posibilidades de avance a los líderes empresariales, la inteligencia artificial también aporta una generalizada incertidumbre con respeto al impacto en el trabajo.

Más amenazas móviles:

La empresa Webroot profetiza que, en los próximos meses, veremos la primera gran infección de malware en la App Store de Android. Otras empresas sostienen, por su parte, que 2108 o 2019 será testigo del primer ransomware móvil diseminado, probablemente, a través de SMS/MMS.

La regulación de IoT:

Internet of Things (IoT) podría ser el sector más afectado por las brechas *Meltdown* y *Spectre*, aun cuando muchos especialistas coinciden en que la legislación será el mayor cambio. La empresa Webroot, ha señalado: "La legislación requerirá que los fabricantes de IoT sean responsables de producir productos sin defectos conocidos".

Por otro lado, no es de extrañar que sucesos como los ocurridos con la botnet *Mirai* se repitan, abarcando en esta ocasión tanto a consumidores como a las empresas, pero esta vez con, presumiblemente, poca capacidad de respuesta.

Todo eso, al margen de que la creciente utilización comercial de los dispositivos IoT significará que el interés por controlar este tipo de sistemas aumentará para los atacantes, como se señala desde Palo Alto Networks.

La delincuencia se vuelve más sofisticada:

El avance de las habilidades de los ciberdelincuentes se ha venido vaticinando año tras año lo que -prescindiendo por un momento de la naturaleza poco sofisticada de *WannaCry-*, se ha evidenciado como cierto.

Según ZeroFox: "La inteligencia artificial propiciará ciberataques más sofisticados y convertirá en obsoletos los métodos básicos de protección". Por su parte, la entidad Lastline señaló que en los próximos años podemos esperar un significativo aumento de la sofisticación entre los ciberdelincuentes, que aprovecharán los kits de hacking basados en AI y ML a partir de herramientas que los delincuentes filtraron o sustrajeron de agencias de inteligencia patrocinadas por estados. RiskIQ parece tener la misma opinión cuando señala: "Los actores de las amenazas aumentarán el uso del aprendizaje automático para evadir la detección".

Ataques contra redes sociales:

Es presumible que los próximos meses se desarrollen formas más asequibles para los atacantes gracias a las redes sociales. Así lo ha afirmado Airbus CyberSecurity, señalando que las redes sociales se pueden utilizar para sofisticadas actividades de ingeniería social y reconocimiento que forman la base de muchos ataques a las organizaciones.

"Para protegerse contra los ataques a las redes sociales, las organizaciones deben implementar políticas de seguridad de redes sociales para toda la organización,

lo que incluye el diseño de programas de formación para los empleados sobre el uso de las redes sociales y la creación de planes de respuesta a incidentes que coordinen las actividades de los departamentos legal, de recursos humanos, marketing y TI en caso de una violación de seguridad ", añade.

Código dañino sin archivos:

Lastline ha afirmado que “a medida que se desarrolle una mayor cantidad de código dañino dirigido al firmware y a la memoria hardware de los dispositivos, podemos esperar un mayor incremento de tales acciones”.

En términos de detección, Digital Pathways ha señalado que los "ataques sin archivos" se tomarán más en serio y serán una amenaza tan grande como los troyanos. "Este tipo de código dañino reside en la memoria de la PC y permanece allí hasta que se reinicia. Un antivirus normal no detectará estos ataques".

Por su parte, Palo Alto Networks agregó que, con la creciente popularidad de las criptomonedas, es presumible esperar más código dañino enfocado en el robo de información de las cuentas para vaciar los correspondientes wallets.

El mayor uso de los Proveedores de Servicios Gestionados de Seguridad:

La entidad Resolve señaló que buena parte de las medidas de seguridad vendrán dadas por los Proveedores de Servicios Gestionados de Seguridad (MSSP). Estos serán objeto de un mayor interés por parte de las organizaciones que reconocen que el nivel de esfuerzo y la experiencia interna requerida para un SOC con garantías de éxito está más allá de sus posibilidades.

"Los MSSP inteligentes, aquellos que cuentan con el personal y las herramientas adecuados para generar confianza entre los usuarios, que demuestren la capacidad de cumplir con los requisitos básicos de la empresa y las respuestas más avanzadas a las violaciones de seguridad atraerán la mayor atención".