Ciberamenazas y Tendencias 2019

CCN-CERT IA-13/19
RESUMEN EJECUTIVO

CCN-CERT

IA-13/19
RESUMEN EJECUTIVO

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.05.31 12:17:23 +02'00'

© Centro Criptológico Nacional, 2019

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

Índice

Prólogo

Por undécimo año consecutivo, la Capacidad de Respuesta a Incidentes de Seguridad del **Centro Criptológico Nacional (CCN-CERT)** ha elaborado el ***Informe de Ciberamenazas y Tendencias. Edición 2019***[1]. Un documento extenso, de más de 128 páginas (cuyo extracto presentamos en estas páginas), en el que se realiza un análisis de las ciberamenazas, nacionales e internacionales, de su evolución y tendencias futuras.

Buena parte de la información recogida en dicho Informe es el resultado de la experiencia del CCN-CERT, como **CERT Gubernamental Nacional** que, durante el año 2018, gestionó un total de 38.029 incidentes de ciberseguridad, de los cuales, el 2,7% tenían una peligrosidad "muy alta" o "crítica". Un año, en el que el Centro Criptológico Nacional volvió a constatar cómo los Estados y los grupos patrocinados por ellos siguen representando la ciberamenaza más significativa del panorama internacional.

Junto a ella, los ataques a la cadena de suministro, las acciones de los grupos terroristas, yihadistas y hacktivistas, las noticias falsas, así como los ataques contra los datos personales (con el fin último de cometer ciertos delitos, robar credenciales, suplantación de identidad o espionaje), fueron otras de las realidades más observadas en 2018.

El documento matriz, así como este resumen ejecutivo, analiza **los principales ciberincidentes de 2018**; los **métodos de ataque** empleados por los **agentes de la amenaza** contra sus víctimas; las múltiples **Vulnerabilidades** existentes que facilitan esta situación y los principales objetivos de ataque. Junto a ellos, las medidas necesarias para mejorar la seguridad en empresas e instituciones.

Por último, y teniendo en cuenta la evolución de los ciberincidentes en el período considerado, se abordan algunas **tendencias** de cara a los próximos meses en los que es de esperar que los agentes estatales continúen realizando campañas de intrusión como parte de sus estrategias nacionales.

El objetivo de este Resumen Ejecutivo (así como del Informe general) es resultar de utilidad a los responsables de seguridad de la información de las entidades del sector público español, las organizaciones de interés estratégico y, en general, a las empresas, los profesionales y ciudadanos de nuestro país. Todo ello, con el fin último de fortalecer la ciberseguridad nacional.

[1]CCN-CERT IA 13/19 disponible en el portal del web del CCN-CERT. https://www.ccn-cert.cni.es/

2 Ciberincidentes de 2018

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

2.1.Soberanía digital de los Estados

La utilización de tecnología fabricada en otros Estados constituye una fuente de preocupación para los gobiernos de todo el mundo, muy especialmente, de Europa.

Se entiende por soberanía digital el impulso de un país para recuperar el control sobre sus propios datos y los de sus ciudadanos. En el lado militar, incluye también la posibilidad de un Estado para desarrollar capacidades ofensivas y defensivas de ciberseguridad sin depender de tecnología extranjera. En el aspecto económico, por su parte, abarca cuestiones que van desde la tributación de las grandes empresas tecnológicas hasta la creación de nuevas empresas de origen local.

2.2.Los Estados como principal fuente de las amenazas

Los Estados, y los grupos patrocinados por ellos, y sus acciones contra otros países, sus instituciones, empresas y ciudadanos siguen representando la ciberamenaza más significativa. El objetivo perseguido por este tipo de ataques es siempre el mismo: sustraer información para mejorar su posición estratégica, política, económica o innovadora (espionaje). A este objetivo se ha unido el intento de influir en la opinión pública de los países atacados o interrumpir la normal prestación de servicios esenciales (sabotaje).

En este tipo de ataques suele ser habitual el uso de técnicas muy simples -tales como el phishing, por ejemplo-, que se aprovechan de las vulnerabilidades humanas de la víctima, de la que recaban información sensible o confidencial para un ataque posterior.

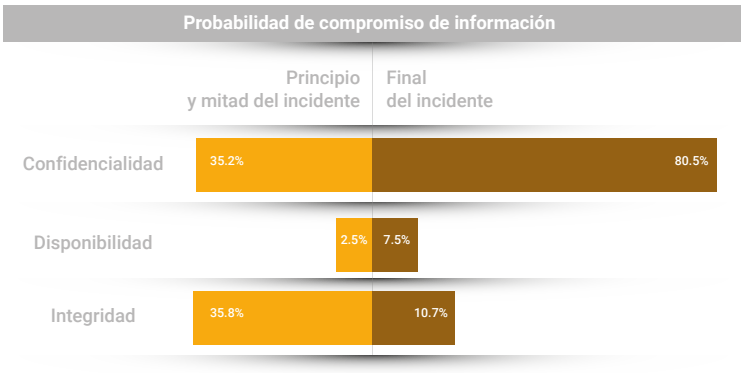
2.3.Ataques a la cadena de suministro

A la vista de la efectividad y los beneficios que comporta para los atacantes, es previsible que este tipo de acciones se mantenga en los próximos años, pues este método presenta dos ventajas para el atacante: puede utilizar un proveedor de confianza como origen de la distribución dañina y acota la superficie del ataque, sin que sea fácil determinar cuáles son, exactamente, los objetivos perseguidos.

2.4.Acciones de los grupos terroristas, yihadistas y hacktivistas

Durante 2018, la amenaza proveniente de grupos terroristas o hacktivistas se ha mantenido estable. Aunque los grupos yihadistas han continuado con sus acciones de propaganda digital, reclutamiento y recaudación de fondos, no han perpetrado hasta ahora ningún ciberataque significativo, más allá de desfiguraciones de páginas web y sustracción de datos.

2.5.Ciberdelincuencia y datos personales



En los últimos años, los ataques contra los datos personales se han incrementado, y no solo por parte de ciberdelincuentes o grupos hacktivistas, sino también por Estados[2]. El objetivo perseguido suele ser la comisión de ciertos delitos, el robo de identidad (credenciales), la suplantación o el espionaje.

La pérdida de la confidencialidad de los datos suele ser el resultado más frecuente de los ataques, hecho que se evidencia en los ataques dirigidos (APT), en relación con acciones de ciberespionaje[3].

2.6.Abuso de datos y noticias falsas

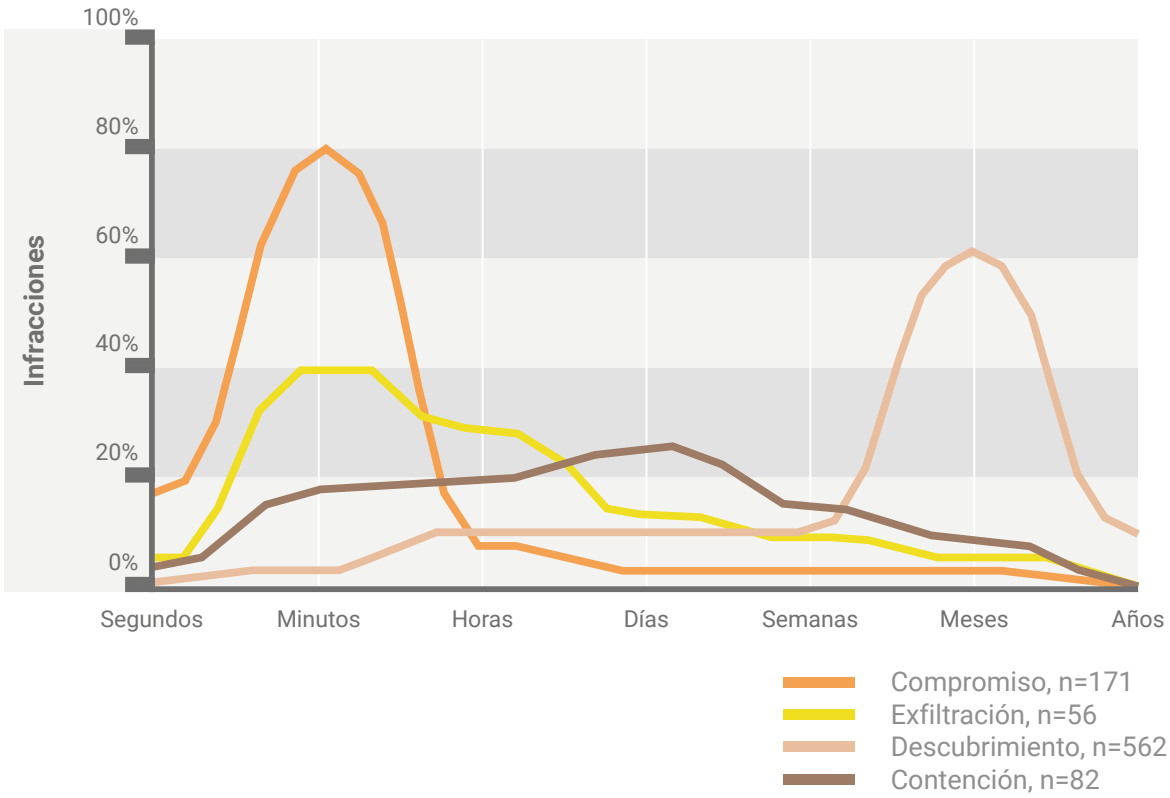
Del mismo modo que las noticias falsas persiguen influir en las opiniones y el comportamiento de los individuos, la información personal distribuida en las redes sociales (Facebook, Twitter, LinkedIn, etc.), una vez analizada y correlacionada adecuadamente, puede posibilitar el desarrollo de sofisticados -e individualizados- ataques de ingeniería social.

2.7.Los tiempos implicados en los ciberataques

En la generalidad de los casos analizados, y cuando los ataques tienen éxito, el plazo para que se vea comprometido el sistema de información sigue siendo muy corto. El tiempo que media entre la primera acción hostil hasta el compromiso de un activo se mide, frecuentemente, en términos de segundos o minutos. Sin embargo, el plazo para su descubrimiento o detección, que depende en gran medida del tipo de ataque, suele expresarse en días, semanas o meses.

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

[3]Fuente de la figura: Verizon: 2018 Data Breach Investigations Report.



Estimación de los tiempos implicados en los ciberataques. Fuente: Verizon

2.8.Elementos facilitadores de los ciberataques

Los elementos facilitadores son aquellas entidades o componentes que incrementan la accesibilidad y/o la efectividad de ulteriores ataques o los métodos usados en su comisión. Tal es el caso, por ejemplo, de los delincuentes que intercambian información sustraída, propiciando posteriores ataques; o las entidades que construyen, alquilan o ponen a disposición de terceros (en la Dark Net) infraestructuras para la comisión de tales acciones (botnets, por ejemplo), posibilitando que agentes de las amenazas con escasos conocimientos puedan perpetrar ataques de forma fácil y a un coste asumible, etc.

La incesante conexión de nuevos dispositivos **IoT** a Internet, propiciando con ello la distribución de código dañino o participando en ataques **DDoS**, constituye también un significativo elemento facilitador de esta problemática. Asimismo, el **cryptojacking**, metodología que persigue obtener ingresos usando la capacidad de proceso de los ordenadores de las víctimas, conformará una de las amenazas más serias de los próximos años.

3

Actores de las amenazas

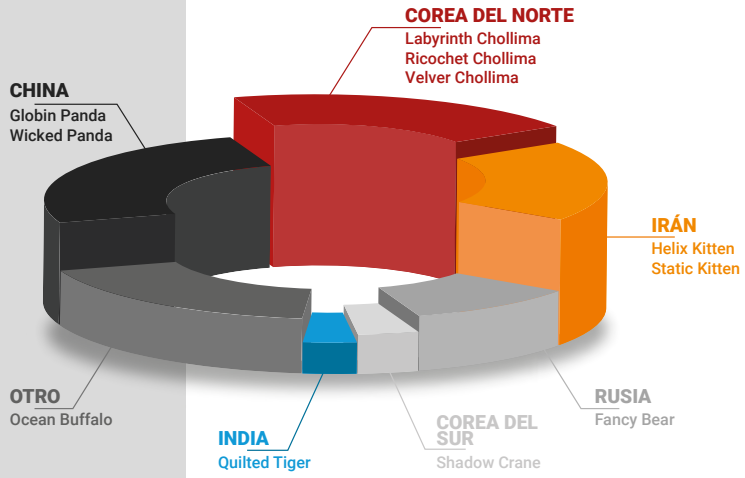
El número de agentes de las amenazas ha aumentado significativamente debido, en parte, al fácil acceso a nuevas herramientas de ataque y a la dificultad permanente para probar la autoría. Además, cada vez es más frecuente que distintos tipos de actores usen las mismas herramientas.

Propagación de código

Más del 60% del tráfico mundial de correo electrónico en 2018 contenía carga dañina y estuvo involucrado en más del 90% de los ciberataques.

3.1.Los Estados

Se ha evidenciado un incremento en el uso de código dañino por parte de los Estados, dirigido a explotar vulnerabilidades de los sistemas de información de las Infraestructuras Críticas.



Intrusiones dirigidas por adversarios en 2018

Principales adversarios reportados

Fuente: : 2019 Global Threat Report.

Frecuentemente, el objetivo de tales ataques ha sido obtener información sobre el grado de implantación de las medidas de seguridad de las organizaciones, al objeto de poseer datos suficientes que les permita planificar ataques futuros. Esta actividad se ha detectado, especialmente, contra objetivos europeos. Además de ello, se sigue empleando el **spearphishing** para ciberespionaje.

3.2.Los ciberdelincuentes

Los ciberdelincuentes continúan siendo uno de los grupos de agentes de las amenazas más activos, con más del 80% de la actividad dañina.

MÉTODOS MÁS USADOS

Propagación de código dañino a través de los correos electrónicos: más del 60% del tráfico mundial de correo electrónico en 2018 contenía carga dañina y estuvo involucrado en más del 90% de los ciberataques.

Uso de malware de **criptojacking/cryptomining** que, según diversas estimaciones, ha podido provocar pérdidas de 880 millones de dólares.

Refinamiento del **phishing** mediante el uso de técnicas de ingeniería social[4] y la innovación permanente para persuadir a los usuarios de la autenticidad de las estafas.

Innovación en las plataformas del **Ciberdelito como Servicio** (Crime as a Service)[5]. Además de las mejoras en los servicios ofertados, estos desarrollos permiten una mayor facilidad de uso, lo que contribuye a extender su popularidad y propiciar ataques más eficientes.

[4]Ver: https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf
[5]Ver: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

3.3.Ciberterrorismo y Ciberyihadismo

La monetización, la propaganda y el reclutamiento son los objetivos principales de este grupo de agentes de las amenazas, que aún mantiene bajas capacidades de acción. No obstante, dada la disponibilidad del Crime-as-a-Service y el potencial para reclutar elementos humanos, los análisis internacionales muestran que el ciberterrorismo aumentará significativamente en los próximos años.

3.4.Los hacktivistas

Los hacktivistas siguen activos en la divulgación de información confidencial recabada en los sitios web atacados, en el desarrollo de acciones DDoS y en la desfiguración de páginas web, con el objetivo de llamar la atención de los medios sin perseguir, en general, la monetización de sus acciones.

Desde el punto de vista técnico, Linux y Apache han sido las principales plataformas web comprometidas en sus acciones[6].

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

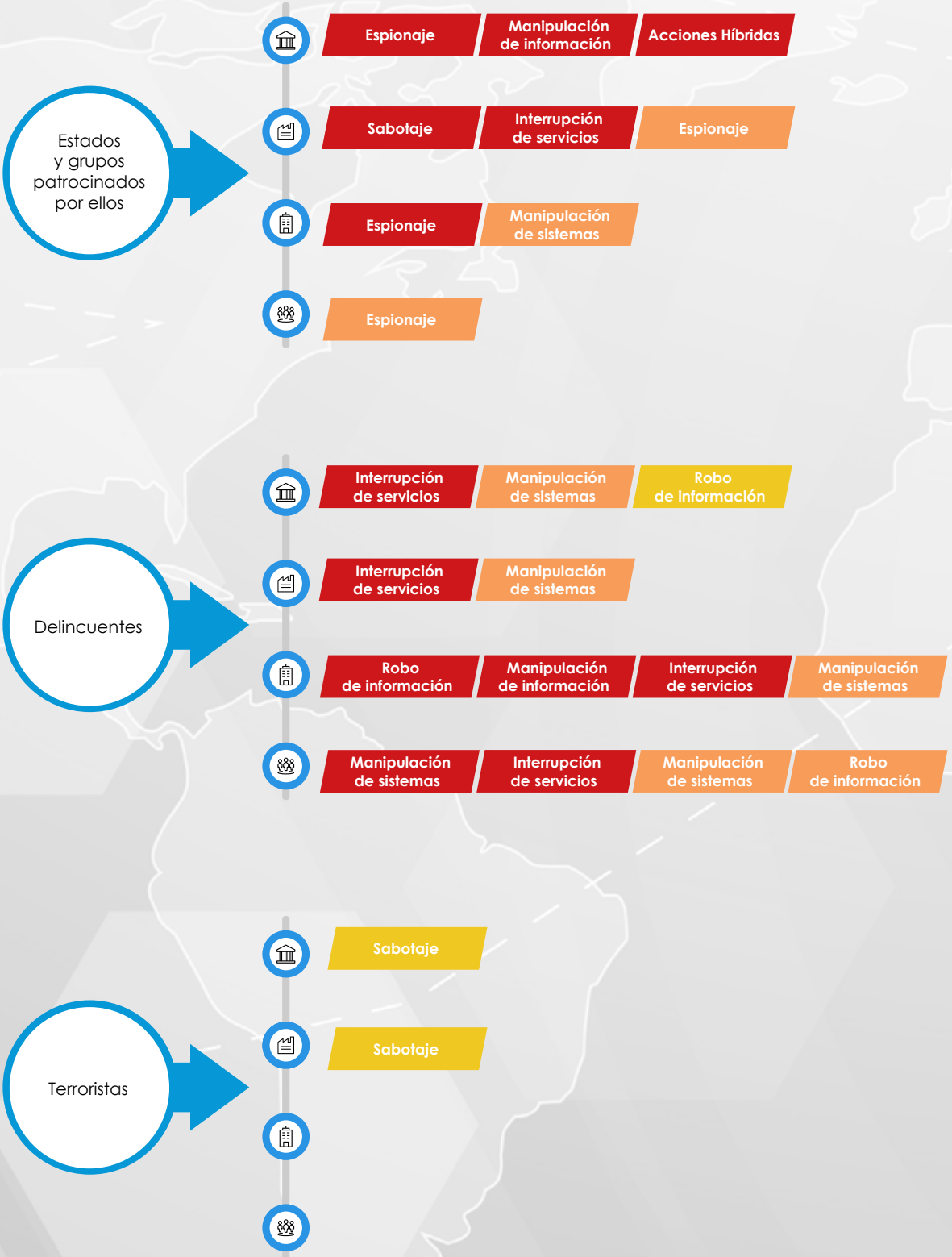
3.5.Actores internos

A este grupo, también conocido como insiders[7], se le atribuyen alrededor del 25% de los incidentes. A pesar de ser percibidos como una de las amenazas más altas, solo el 64% de las organizaciones dice estar invirtiendo en medidas de disuasión.

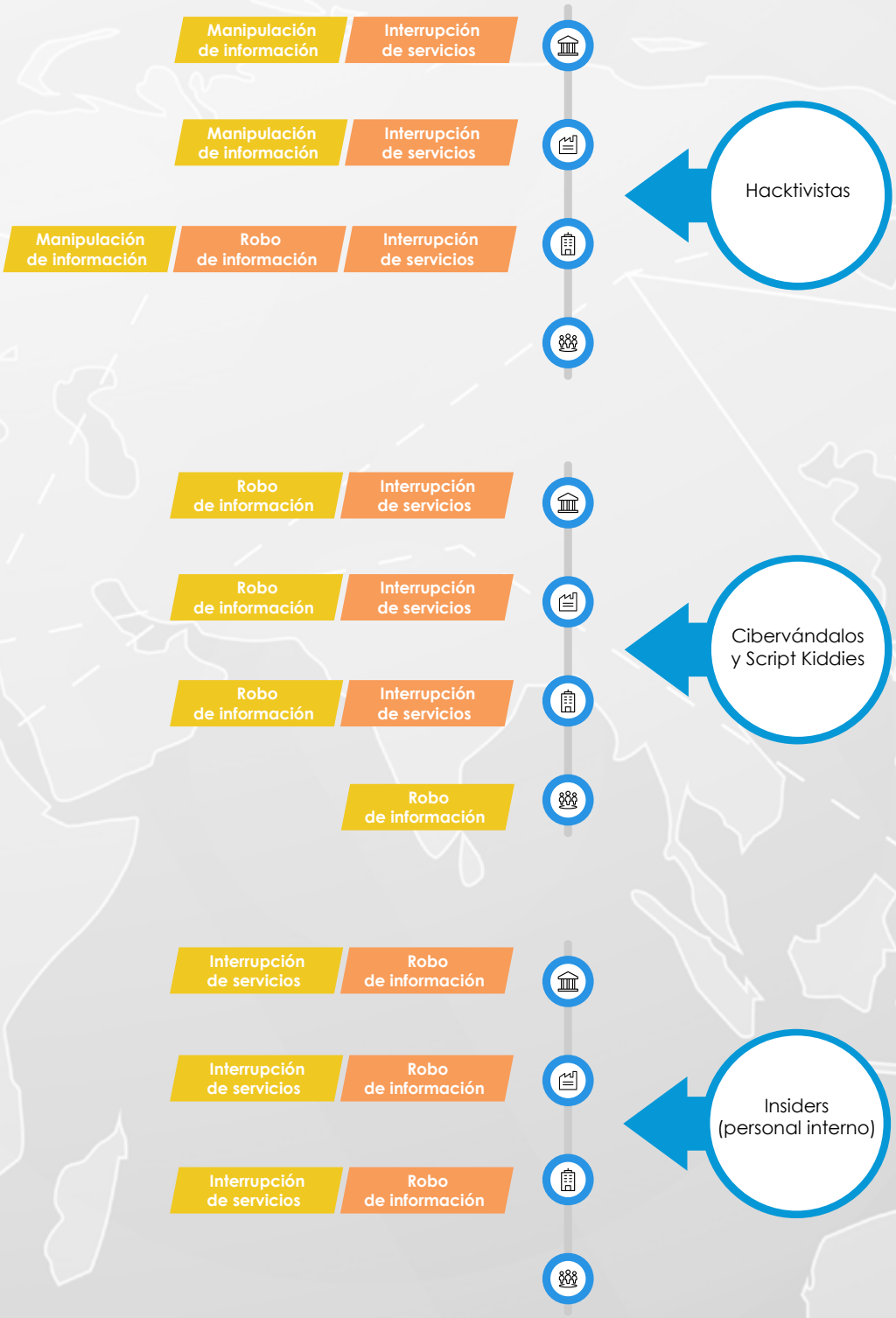
La mayor parte del daño parece ser causado por acciones no intencionadas de los empleados[8], entre las que destacan la divulgación accidental de datos, fallos en el reconocimiento de ataques de phishing o errores debidos a una configuración errónea[9]. Las amenazas internas, que constituyen **la segunda fuente de incidentes**, pueden materializarse también de forma indirecta, con ataques a la cadena de suministro.

[7]Personas con acceso al sistema desde dentro del perímetro de seguridad. Es decir, con cierta autorización para el acceso.
[8]Ver: https://www.doxnet.com/2018/04/insider-use-and-abuse-identifying-internal-threats-and-how-to-mitigate-them/
[9]Ver: https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2017

Ciberamenazas 2018



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



Agentes de la amenaza

Víctima

- Gobierno / Admón. Pública
- Empresas
- Infraestructuras críticas
- Ciudadanos

Peligrosidad

- Alta
- Media
- Baja

4 Vulnerabilidades

Las siguientes son las vulnerabilidades más significativas de 2018

4.1.Vulnerabilidades en el software y en el hardware

El número de vulnerabilidades conocidas en los productos de software ha sido alto y no hay indicios de que esta situación varíe en los próximos años. Son claras ciertas tendencias en el software que afectan a la seguridad del producto final:

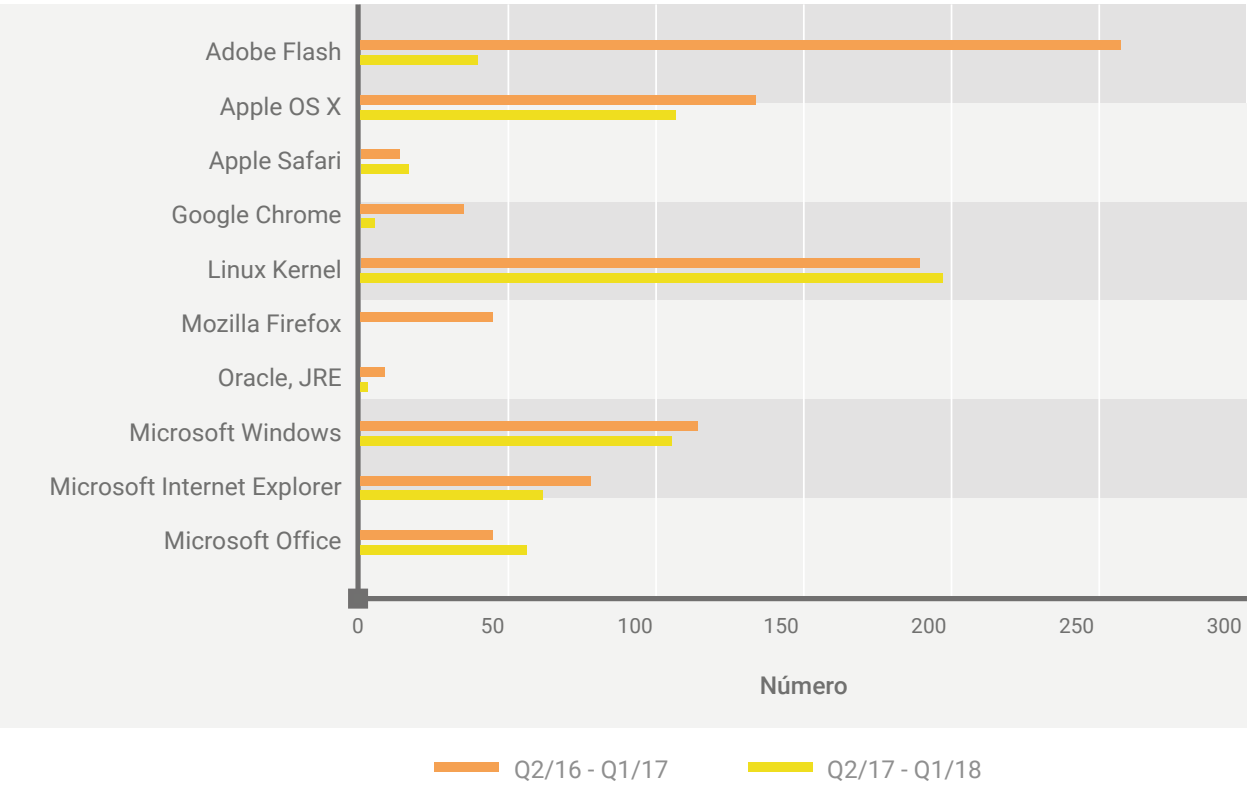
- Mayor complejidad de las aplicaciones de usuario final
- Agrupación de componentes software, parcialmente actualizados
- Integración incontrolada de elementos de origen externo
- Optimizaciones de velocidad a expensas de la seguridad
- Abandono de la resolución de problemas con referencia a medidas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

Entre las más destacadas en el software se han observado anomalías en **Mozzila Firefox** y **Google Chrome**. Ambos navegadores parecen no haber mantenido ninguna entrada en la base de datos de MITRE CVE.

Si bien las entradas están referenciadas en sus propias publicaciones, no se anotan en la base de datos pública de manera que no se proporciona una descripción de la vulnerabilidad, al igual que tampoco se hace referencia al producto afectado.

Asimismo, investigadores de la Universidad de Ciencias Aplicadas de Münster, Ruhr University Bochum y KU Leuven (Bélgica) encontraron serios puntos débiles en la

implementación de los estándares de cifrado de correo electrónico **OpenPGP** y **S/MIME**, que publicaron en mayo de 2018. En base a tales vulnerabilidades, los atacantes podrían manipular correos electrónicos cifrados de tal manera que el contenido del mensaje se podría reenviar en texto plano después de ser descifrado por el destinatario.



CVE críticas del software más utilizado

Un producto que contiene vulnerabilidades conocidas públicamente en el momento de la compra debe considerarse defectuoso desde la perspectiva de seguridad IT. El mantenimiento del software por parte del fabricante, incluida la eliminación de vulnerabilidades, no solo debe ser el procedimiento habitual y el mecanismo para satisfacer la normativa legal aplicable, sino que también debe ser solicitado por el consumidor, como parte del servicio.

4.2.Nuevas formas de explotación

En enero de 2018, equipos de investigación revelaron dos nuevas familias de vulnerabilidades hardware, denominadas ***Spectre*** y ***Meltdown***, que permitirían a los atacantes obtener información confidencial ejecutando el código del programa en el ordenador de la víctima.

Como nueva forma de explotación, cabe mencionar la vulnerabilidad ***GLitch***, publicada por investigadores de la Universidad Libre de Ámsterdam, capaz de perpetrar lo que se conoce como ataques de *Rowhammer* a través del procesador gráfico de un ordenador. Asimismo, mediante la explotación de una vulnerabilidad de **Apache Struts**, la empresa Equifax informó de que los atacantes habían sustraído los datos de 4,9 millones de norteamericanos, el ataque ocasionó a Equifax una pérdida de 87,5 millones de dólares.

4.3.Ataque DDoS a través de sistemas públicamente accesibles

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

Según la compañía Panda, el 28 de febrero de 2018 tuvo lugar el ataque DDoS más

potente de la historia: 1,35 terabits por segundo de tráfico dirigido a GitHub, la plataforma web de proyectos de desarrollo colaborativos. Unos días más tarde, se superó el record con un ataque con picos de tráfico de 1,7 Tbps.

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

4.4.La seguridad de los dispositivos médicos y sanitarios

Varias pruebas en laboratorio, realizadas en Estados Unidos, han demostrado que dispositivos médicos como marcapasos, desfibriladores o respiradores son vulnerables

a ciberataques. En consecuencia, la ciberseguridad debe ser integrada e implementada desde el principio del desarrollo y fabricación de estos dispositivos, con el fin de garantizar su uso.
A menudo, los mecanismos de autenticación en dispositivos médicos digitales no están suficientemente protegidos y las técnicas de cifrado de datos para la comunicación y el almacenamiento son débiles o, incluso, inexistentes. En estas circunstancias, sería posible obtener acceso no autorizado y manipular el dispositivo sin el conocimiento del paciente.

El ataque más potente en 2018

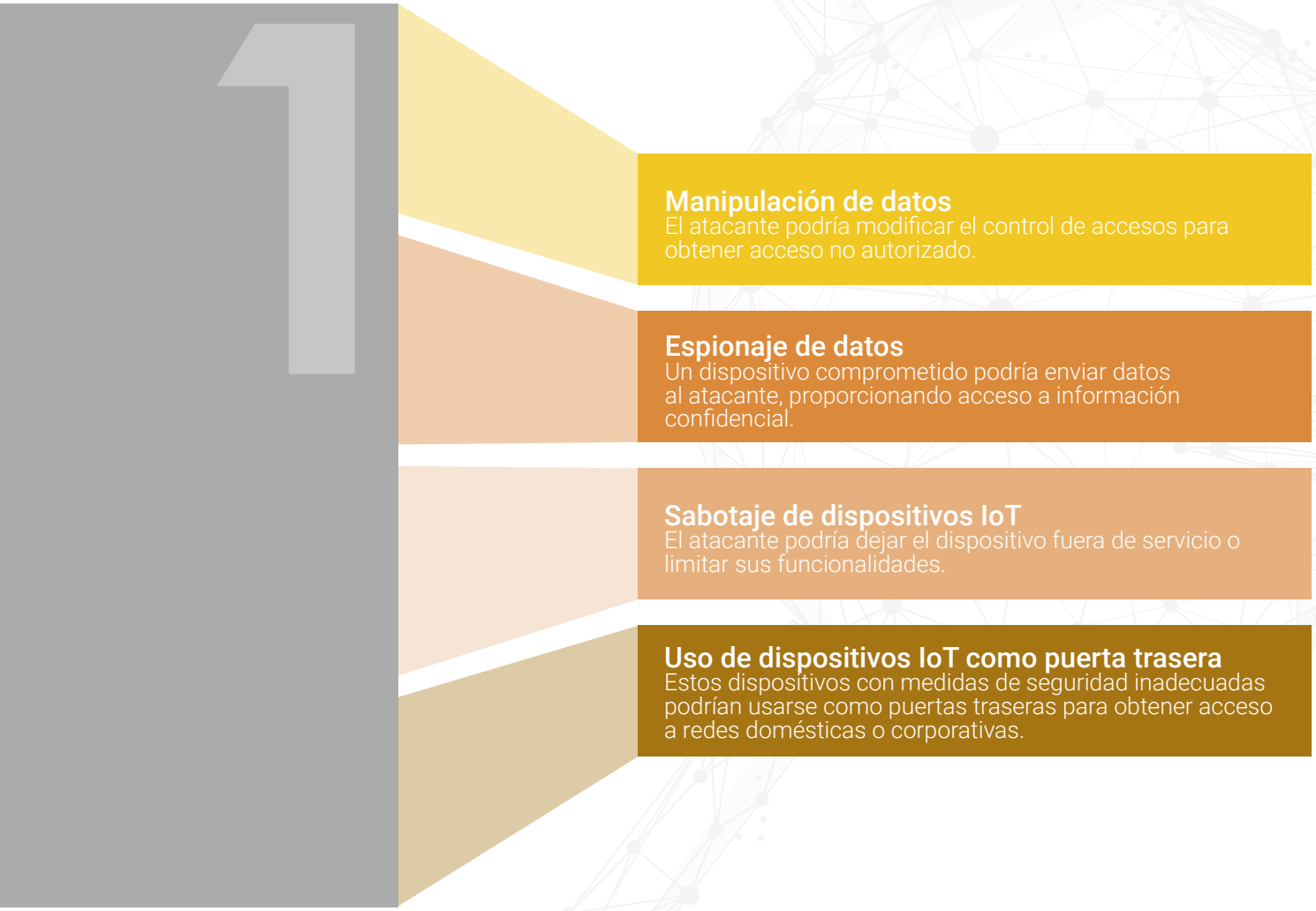
1,35 terabits por segundo de tráfico dirigido a GitHub. la plataforma web de proyectos de desarrollo colaborativos. Unos días más tarde, se superó el record con un ataque con picos de tráfico de 1,7 Tbps.

4.5.La seguridad del mobile-banking

Los pagos por internet se realizan, cada vez con más frecuencia, usando dispositivos móviles, lo que alienta a las entidades financieras a ofrecer apps de banca online para estos dispositivos.
Tales aplicaciones bancarias se complementan con una segunda aplicación, conocida como "aplicación TAN" que genera un número (TAN) para asegurar la transacción ejecutada en la app bancaria.
Para ello, suele utilizarse un único dispositivo en el que se ejecutan la aplicación bancaria y la aplicación que genera el TAN, lo que constituye un riesgo significativo si el dispositivo se ve comprometido, pues el atacante podría obtener el control de ambas aplicaciones. Todo ello deriva en el enorme tráfico ilegal actual de credenciales.

4.6.Domótica e Internet of Things

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



En un segundo escenario de amenazas, el dispositivo IoT se compromete para ser utilizado como medio para atacar otros objetivos. En estos casos, como el equipo no ve alterada su funcionalidad, el ataque suele pasar desapercibido.

2

Construcción de botnets
El secuestro masivo de dispositivos de IoT con deficiente seguridad permite la creación de grandes redes de bots que pueden propiciar ataques DDoS.

Ocultamiento de la identidad
Los dispositivos comprometidos pueden usarse como servidores proxy para ocultar nuevos ataques.

Minería de criptomonedas
Es posible utilizar la potencia de cómputo colectivo de los dispositivos IoT comprometidos para la minería de criptomonedas. En este caso, el ataque es más fácil de detectar, porque se ralentiza el normal funcionamiento del equipo.

***Clic-Fraud* con banners publicitarios**
El atacante usa muchas direcciones IP diferentes de dispositivos IoT secuestrados para generar clics en banners publicitarios, videos o contenido de redes sociales. De esta manera, se puede obtener un beneficio económico con la facturación basada en clics. Además, el anunciante sufre daños directos a través del pago de una comisión por clics simulados.

4.7. Vulnerabilidades en chips

Los componentes que almacenan claves criptográficas o implementan algoritmos criptográficos son esenciales en las aplicaciones de seguridad más importantes, tales como la autenticación segura, la comunicación cifrada o las firmas electrónicas. El almacenamiento seguro de la clave y, en particular, el procesamiento de claves sigue siendo un gran desafío, ya que, inevitablemente, surgen fenómenos físicos medibles que permiten extraer conclusiones sobre las claves.

Asimismo, las debilidades algorítmicas constituyen otro problema. En ocasiones, no se pueden implementar algoritmos criptográficos seguros debido a la limitada capacidad de almacenamiento y proceso de los elementos de seguridad. Las operaciones muy complejas, tales como la generación de claves en RSA, siguen consumiendo mucho tiempo dependiendo de la longitud de la clave. El uso de FastPrime, un algoritmo propietario para construir grandes números primos, acelera la generación de claves; sin embargo, las claves generadas de esta manera son criptográficamente más débiles. Así, con la ayuda del ataque Coppersmith, un módulo RSA se puede factorizar de manera eficiente si se conocen los bits más altos de uno de los números primos.

5 La Ciberamenaza en 2018

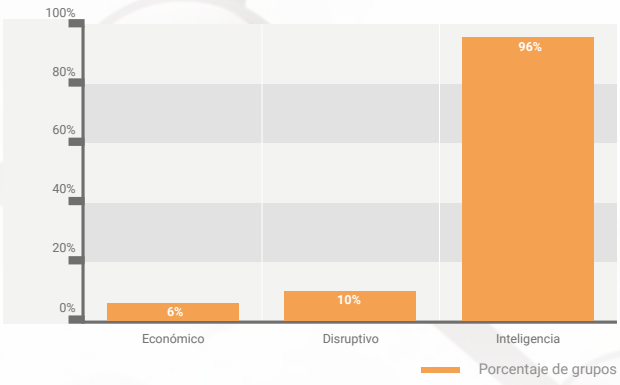
Este epígrafe describe los desarrollos en los métodos, procedimientos y herramientas que los actores de las amenazas han utilizado en el período considerado.

5.1.Amenazas Persistentes Avanzadas (APT)

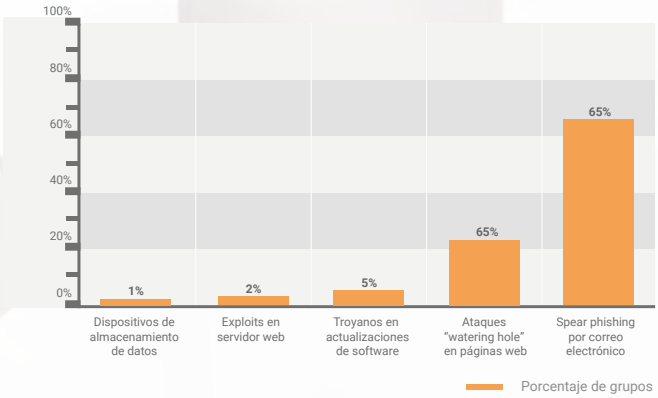
En relación con los dispositivos IoT, caben dos escenarios de amenaza: en un primer escenario, el equipo se compromete para causar daños directos o indirectos al usuario, como los mostrados en el cuadro siguiente.

A este vector de ataque también se le conoce como ataque a la cadena de suministro, puesto que atacan primero a los proveedores del objetivo real, para utilizarlos como puente para alcanzar a la red del objetivo último. Este es otro mecanismo utilizado actualmente por grupos como **APT10** como parte de la campaña Cloud Hopper.

Una fase posterior de las APT es el movimiento lateral, durante el cual los atacantes extienden su influencia dentro de la red de la víctima. Para ello, utilizan herramientas de administración legítimas –como PowerShell o Windows Management Instrumentation, WM– o herramientas disponibles públicamente – como Cobalt Strike, Powershell Empire y Koadic–, lo que dificulta la clasificación de los ataques.



Objetivos de ataques dirigidos



Vectores de infección en ataques dirigidos

Para la protección contra las APT se recomienda tomar las siguientes medidas clave

- Usar autenticación de dos factores para VPN y webmail, como mecanismo de protección contra el phishing.
- Emplear directorios de lista negra que dificulten la ejecución inicial de código dañino de los archivos adjuntos del correo o del navegador.
- Restringir la comunicación entre los clientes a funciones esenciales para que el movimiento lateral sea más difícil para los atacantes.
- El modelo de capas en Active Directory garantiza que los datos de acceso con privilegios elevados no se utilicen en sistemas con bajo privilegio, lo que exige de los atacantes un esfuerzo adicional para obtener datos de acceso con alto privilegio.

Organismos Gubernamentales	Defensa
APT12/ NumberedP , APT28/ Sofacy, APT29/ CozyBear, APT32/Ocean-Lotus APT37/Reaper Bahamut, BlueMushroom, Cadelle/Chafer, Callisto, Charming-Kitten, Dark-Caracal, DarkHotel, Dropping-Elephant, Emissary-Panda, Extreme-Jackal, Gamaredon, Gaza-Cybergang, Greenbug, Hammer-Panda, Infy, KeyBoy, Lapis/TransparentTr., Longhorn, Lotus-Panda, Machete, Micropsia, Muddy-Water, Naikon/OverrideP., Leviathan, OilRig, Operation-Cleaver, Project-Sauron, Shamoon, Snake, Sowbug, Tick, TidePool/Ke3chang, Tonto, Transparent, Tribe, Tropic-Trooper/PirateP, Vermin, Viceroy-Tiger	**APT28/Sofacy, APT37/Reaper, AridViper, BlueMushroom, Callisto, Charming-Kitten, C-Major/ PureStrike, Dark-Caracal, Dropping-Elephant, Gamaredon, Gaza-Cybergang, Hammer-Panda, HelixKitten, Lotus-Panda, Machete Naikon/OverrideP, Leviathan, OilRig, Operation- Cleaver, Project-Sauron, Snake**

Opposition	Medios	Energía
Ahtapot, APT32/Ocean-Lotus, Bahamut, BlackOasis, Bookworm, Charming-Kitten, Dark-Caracal, EnergeticBear, Flying-Dragon, Group5, Infy, Neodymium, Operation-Cleaver, Operation, Manul, Promethium, ScarCruft, Sima, Stealth-Falcon, SunTeam Temper-Panda, ZooPark	APT28/Sofacy, APT32/Ocean-Lotus, Bahamut, BlackOasis, BugDrop, Callisto, Charming-Kitten, Dark-Caracal, DarkHotel, Dropping-Elephant, GazaCybergang, Infy, Olympic-Destroyer, Operation, Manul, Sandworm, ScarCruft, Shrouded-Crossbow, Stealth-Falcon, SunTeam, Tick	APT10APT18/Wekby, APT29/CozyBear, Charming-Kitten, Electric-Powder, Emissary-Panda, Energetic-Bear, Gaza-Cybergang, Greenbug, HelixKitten, Kraken/Laziok, Longhorn, Machete, Muddy-Water, OnionDog, Operation-Cleaver, Sandworm, Shamoon, Tropic-Trooper/ PirateP

Financiero	Vídeo conferencia	ONG	Universidades
APT18/Wekby, APT29/ CozyBear, BlueMushroom, Dark-Caracal, Dropping-Elephant, Emissary-Panda Energetic-Bear, Equation-Group, Gaza-Cybergang, Hammer-Panda, Longhorn, OilRig, Sandworm	APT18/Wekby, Codoso, Emissary-Panda, Hammer-Panda, HelixKitten, Longhorn, Machete, Muddy-Water, OilRig, Project-Sauron, Thrip	APT29/CozyBear, APT37/Reaper, Callisto, Charming-Kitten, DarkHotel, Hammer-Panda, Honeybee, Infy, NilePhish, Operation-, Cleaver, Rocket-Kitten	APT10/menuPass, BugDrop, Charming-Kitten, Codoso, Dark-Caracal, DarkHotel, Greenbug, DarkHotel, Longhorn, Leviathan, Rocket-Kitten

Alta Tecnología	Transporte	Aeroespacial	Salud	Legal
APT18/Wekby, Charming-Kitten, Codoso, LEAD/Winnti, Tick	Cadelle/Chafer, NanHaiShu, OilRig, OnionDog, Project-Sauron, Shamoon	APT28, Dropping-Elephant, Emissary-Panda, Leviathan, Hammer-Panda, Greenbug, Longhorn	APT10/menuPass, Leviathan, LEAD/Winnti	APT29/CozyBear, Codoso, Dark-Caracal, DeepPanda, Leviathan

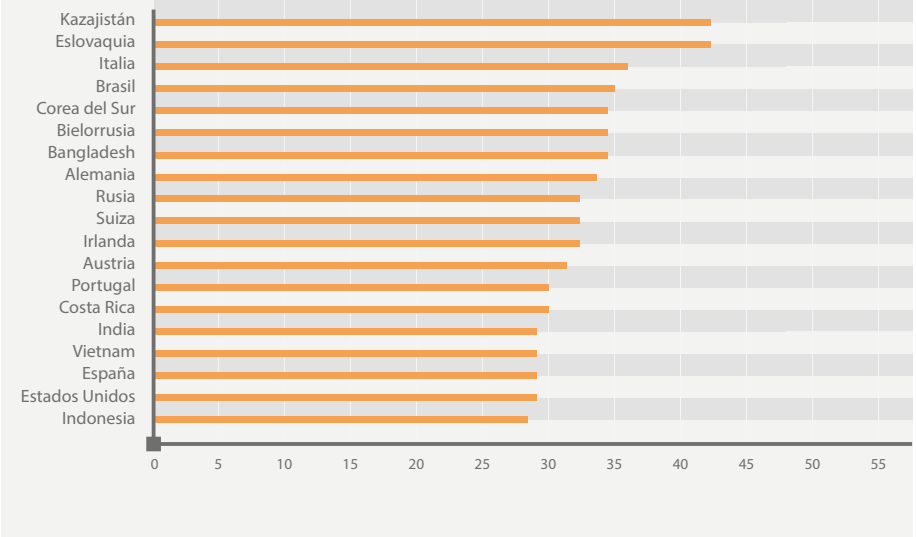
Fuente: BSI, evaluación de informes públicos

5.2.Ciberespionaje

El ciberespionaje se está convirtiendo en una práctica habitual de ciertos Estados, dirigiéndose habitualmente contra sectores industriales, infraestructuras críticas y estratégicas en todo el mundo, con el objetivo de obtener secretos de Estado o beneficios geopolíticos y comerciales.

El número de ciberataques centrados en la economía y patrocinados por Estados ha aumentado a lo largo de 2018. Estas acciones, dirigidas también al uso de IoT, están también aumentando en los sectores de los servicios públicos. Además, el uso de APT indica que muchos ataques dirigidos contra el sector financiero tienen su origen en las tácticas, técnicas y procedimientos del ciberespionaje, usadas por actores tales como *Cobalt Group*, *Carbanak* y *FIN7*.

Las redes de tecnología operacional (OT) de las industrias son un campo de acción idóneo para los actores de las ciberamenazas. Estos agentes utilizan herramientas de administración remota (RAT) que ya están instaladas en los sistemas de control industrial (ICS)



Países en los que se utilizaron RAT en incidentes de espionaje durante el 1 er semestre de 2018. Fuente: Securylist

5.3.Amenazas Híbridas

Las denominadas "amenazas híbridas" son acciones coordinadas y sincronizadas con origen habitualmente en los Estados o en agentes patrocinados por ellos, que atacan deliberadamente vulnerabilidades sistémicas de los Estados y sus instituciones, a través de una amplia gama de medios y en distintos sectores-objetivo: políticos, económicos, militares, sociales, informativos, infraestructuras y legales, utilizando el ciberespacio como la herramienta más versátil y adecuada para sus propósitos. Constituye, por tanto, el fenómeno resultante de la convergencia e interconexión de diferentes elementos que, en conjunto, constituyen una amenaza más compleja y multidimensional.

5.4.Ataques a Sistemas de Control Industrial (ICS)

Los Sistemas de Control Industrial han sido víctimas frecuentes de ataques no dirigidos, infectando con ransomware estaciones de trabajo de operadores u otros componentes de control. Los vectores de entrada fueron, principalmente, correos de phishing y soportes extraíbles, aunque también se evidenciaron casos en los que la infección se produjo como resultado de la utilización de sistemas de mantenimiento remoto configurados incorrectamente. En todos los casos, el código dañino explotó vulnerabilidades conocidas de software obsoleto y una inadecuada segmentación entre las redes de oficina y las redes de producción. Todo parece apuntar que este tipo de incidentes continuará representando una amenaza significativa para los ICS en los próximos años.

La progresiva introducción de la "Industria 4.0"[10] también ofrece nuevos puntos de partida para las actividades delictivas.

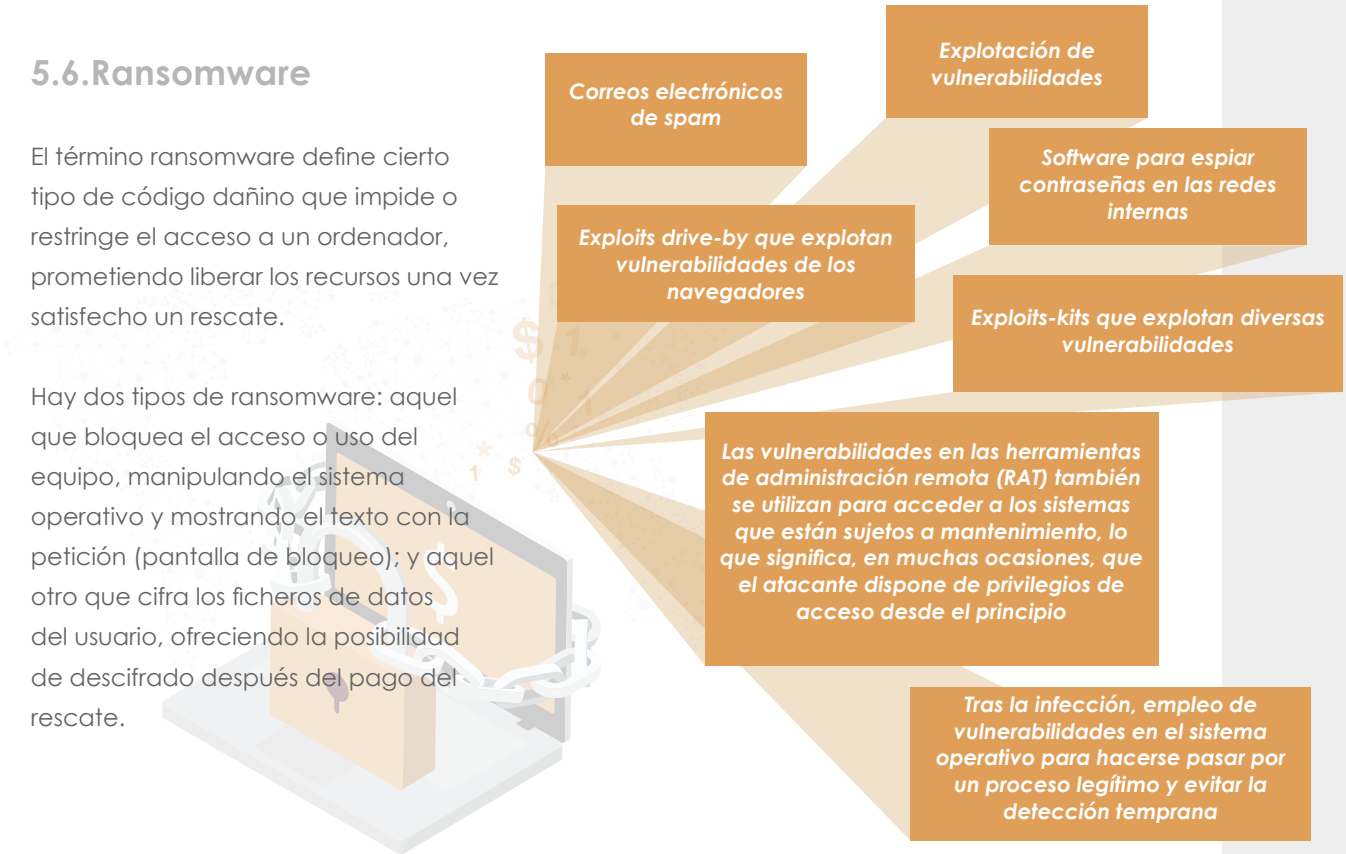
5.5.Correo electrónico

Durante 2018, las principales manifestaciones de ciberataques de este tipo fueron los casos de phishing o spear-phishing perpetrados por delincuentes, Estados o actores patrocinados por ellos con el objetivo de desarrollar acciones de espionaje o sabotaje. Según la empresa Verizon, los Estados utilizaron técnicas de phishing en el 70% de sus ciberataques[11].

5.6.Ransomware

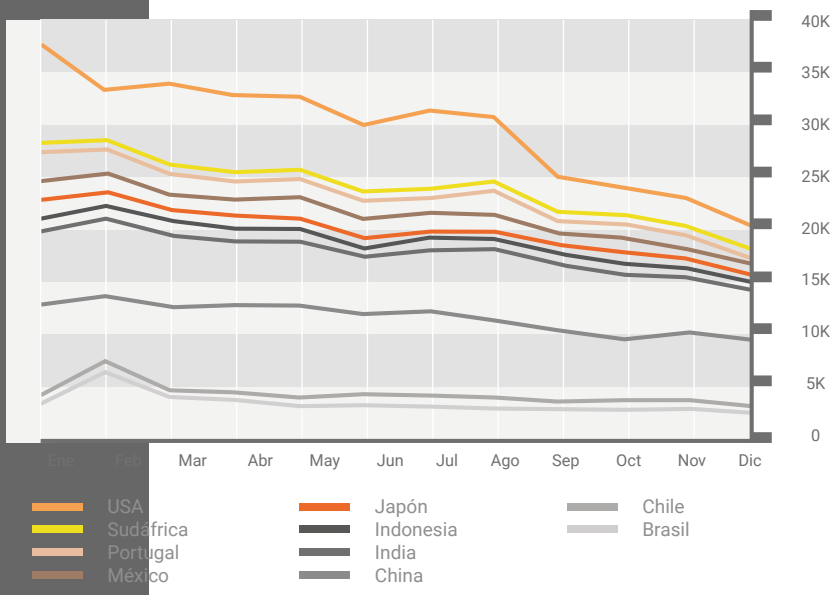
El término ransomware define cierto tipo de código dañino que impide o restringe el acceso a un ordenador, prometiendo liberar los recursos una vez satisfecho un rescate.

Hay dos tipos de ransomware: aquel que bloquea el acceso o uso del equipo, manipulando el sistema operativo y mostrando el texto con la petición (pantalla de bloqueo); y aquel otro que cifra los ficheros de datos del usuario, ofreciendo la posibilidad de descifrado después del pago del rescate.

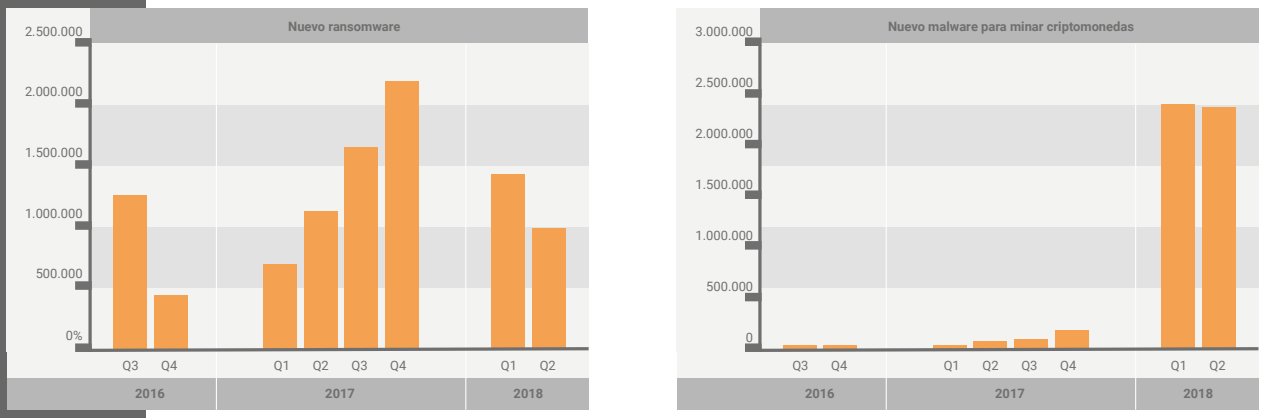


[10]Industria 4.0 y su sinónimo, Cuarta Revolución Industrial, iniciada recientemente, donde la inteligencia artificial sería el elemento central, relacionada con la acumulación creciente de grandes cantidades de datos (big data), el uso de algoritmos para procesarlos y la interconexión masiva de sistemas y dispositivos digitales. (Fuente: Wikipedia)
[11]Verizon op. cit.

De forma similar a los servicios de botnet disponibles para ataques DDoS, en la actualidad también hay ofertas de *Ransomware-as-a-Service*. No obstante, el ransomware parece disminuir en la medida en la que otros modelos, como la minería de criptomonedas, son más rentables o prometen beneficios más constantes.



Penetración de ransomware por país/mes, durante 2018 (Fuente: Symantec).



Correlación entre el volumen de detección de ransomware y de cryptojacking (Fuente: McAffee)

5.7.Spam y Phishing

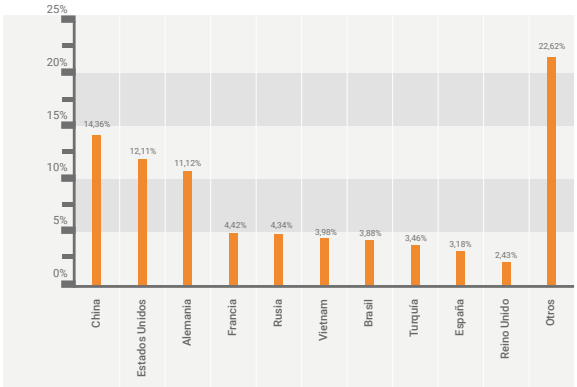
Suele denominarse spam a los correos electrónicos no solicitados, dividiéndose en tres categorías:

Spam convencional
A menudo se utiliza para anunciar productos o servicios, así como en intentos de fraude.

Malware spam ("malspam")
Utilizado por los agentes de las amenazas para infectar los sistemas de los destinatarios con código dañino. El malware puede estar en un adjunto a un correo electrónico o introducirse indirectamente a través de un enlace en el cuerpo del correo o en los archivos adjuntos. Este enlace conduce al malware o a un sitio web que contiene exploits drive-by.

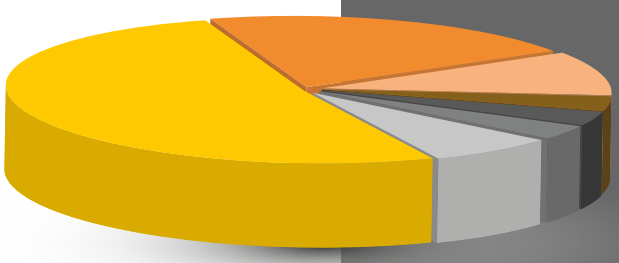
Suplantación de identidad (Phishing)
Alientan a los usuarios a entregar información, tal como el inicio de sesión en sitios web controlados por los agentes de las amenazas.

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



Distribución del origen de las acciones de spam (Fuente: Securlist)

Citas	52,20%
Desconocido	20,80%
Software	10,00%
Almacenamiento	3,30%
Productos farmacéuticos	3,30%
Tiendas	3,20%
Otros	7,20%



Distribución de spam por áreas (Fuente: BSI)

Frecuentemente, los sistemas que distribuyen spam se ensamblan en una botnet, lo que facilita a los atacantes la comercialización de sus actividades como servicio.

La botnet **Necurs** ha seguido siendo el mayor remitente de mensajes de spam. No obstante, se han seguido observando campañas más pequeñas de malspam fuera de esta botnet. De particular interés son las que han perseguido la difusión de **Emotet**. Este código dañino utiliza los datos de Outlook obtenidos durante una infección para enviar un correo electrónico que pretende ser de una persona con la que la víctima potencial ya se ha comunicado.

Se ha demostrado que el phishing es la forma preferida de comprometer a las organizaciones[12]: el 75% de los Estados miembros de la UE revelaron casos de phishing[13]. Un último dato: más del 90% de las infecciones de código dañino y el 72% de las violaciones de datos en organizaciones se originaron a partir de ataques de phishing[14].

*El **75%** de los Estados miembros de la UE revelaron casos de phishing.*

ESTAS SON LAS EVIDENCIAS

más significativas de 2018 en torno al phishing

- Los ataques de phishing se han hecho más **específicos**.
- Cambio de objetivo: del consumidor a la **organización**.
- Crecimiento de los ataques de phishing a **dispositivos móviles**: han aumentado en torno al 85% anual desde 2011. Actores avanzados utilizan técnicas de phishing móvil, por ejemplo, Dark Caracal y Pegasus.
- Crecimiento de los sitios de phishing que utilizan **HTTPS**: Durante 2017, un tercio de los sitios web de phishing han sido accedidos a través de mecanismos HTTPS.
- Permanece el problema de **Business Email Compromise (BEC)**: este tipo de ataque de phishing dirigido a ejecutivos y empleados de los departamentos económicos o de recursos humanos con el objetivo de sustraer dinero de sus organizaciones. Desde octubre de 2013 hasta mayo de 2018, se han reportado 78.000 ataques de BEC en todo el mundo, con unas pérdidas estimadas de 12 mil millones de dólares.
- El **spearphishing** es el método de entrega de facto para grupos APT: El 71% de los grupos de APT han usado spearphishing como vector de infección. Durante 2018, los grupos del crimen organizado de más alto perfil fueron FIN7 y Cobalt Group. Además, los actores estatales siguen usándolo como principal vector de infección para sus operaciones de ciberespionaje e interrupción de servicios.
- Tendencias en **archivos adjuntos maliciosos**, los más comunes son documentos de Microsoft Office, archivos de datos, archivos JavaScript, scripts de Visual Basic y documentos PDF.

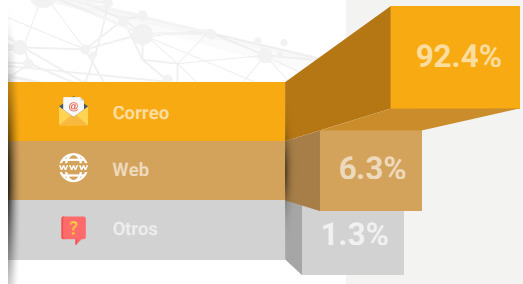
[12]Véase: https://www.fireeye.com/company/press-releases/2018/new-fireeye-email-threat-report-underlines-the-rise-in-malware-l.html
[13]Véase: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018
[14]Véase: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

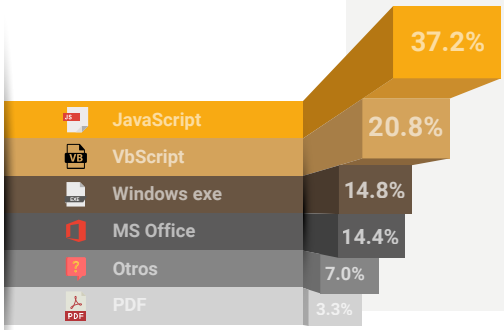
5.8.Código dañino

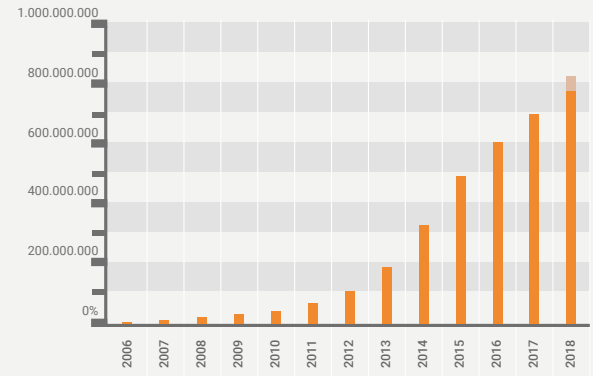
El código dañino o malware es una parte integral de la mayoría de los escenarios de ataque. Al igual que en años anteriores, continúa siendo una de las mayores amenazas para los consumidores, las empresas y el sector público.

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

- Aunque el adware es una de las formas más fáciles de distribuir código dañino, ha habido pocos desarrollos de esta amenaza.
- El 94% de todos los ejecutables dañinos ha sido malware polimórfico.
- El 79% del código dañino detectado en las organizaciones estaba dirigido a Windows, el 18% a Linux y el 3% a los sistemas Mac.
- Se ha descubierto el primer malware para la Unified Extensible Firmware Interface (UEFI).
- La mayoría del código dañino móvil se alojó en tiendas de aplicaciones de tercera parte y las categorías de aplicaciones en las que se encontró la mayoría del tal malware móvil fueron: Estilo de Vida Lifestyle (27%) y Music&Audio (20%).
- Se ha mantenido la tendencia de malware preinstalado.
- Los troyanos de acceso remoto siguen aumentando. FlawedAmmyy es el primer RAT que aparece en la lista de los diez programas maliciosos más importantes[15].
- Los endpoints aumentan como objetivos de las amenazas, probablemente debido a lo difuso del perímetro de las organizaciones y el uso de dispositivos móviles[16].







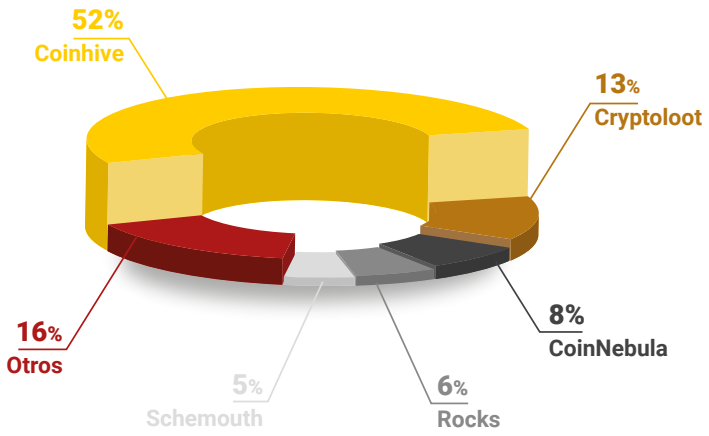
Evolución del código dañino en los últimos años (Fuente AV-Test)

Aunque el código dañino sigue siendo la ciberamenaza más común[17], se ha observado que los Estados han incrementado el uso de software legítimo y de proveedores de buena fe para acceder a víctimas concretas, lo que dificulta la prevención y detección de tales ataques.

[15]Véase: https://www.zdnet.com/article/this-remote-access-trojan-just-popped-up-on-malwares-most-wanted-list/
[16]Véase: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf
[17]Véase: ENISA: Threat Landscape Report 2017 (en https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017)

5.9.Criptojacking

Cada vez más frecuentemente, los ciberdelincuentes intentan obtener beneficios a través del criptojacking, es decir: utilizar la potencia de cálculo de los sistemas informáticos de terceros para el minado de criptomonedas (cryptomining). La razón de este comportamiento persigue la monetización directa en base a la generación de criptomonedas. La tendencia de los cryptominers sigue de cerca el flujo de dinero y la valoración de los precios del mercado de criptomonedas[18].

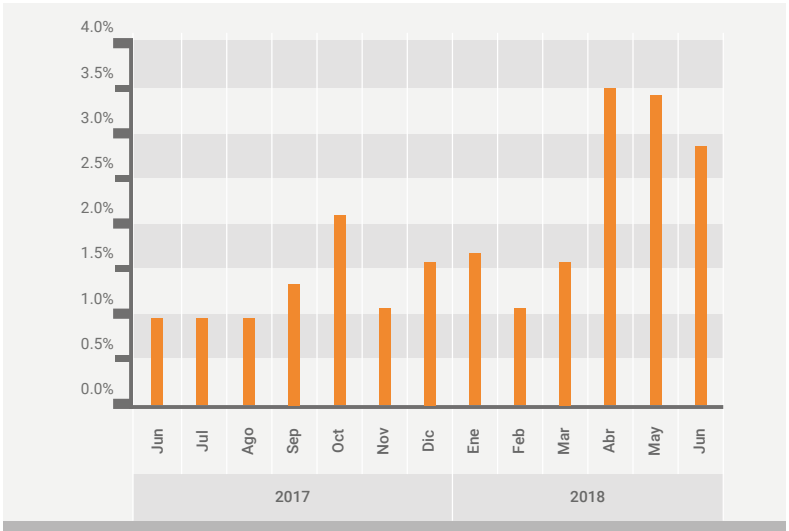


Top global de malware Criptomonedas

Además de los sistemas informáticos tradicionales, los dispositivos de IoT y los dispositivos móviles también se utilizan para extraer criptomonedas.

Además de los sistemas informáticos tradicionales, los dispositivos de IoT y los dispositivos móviles también se utilizan para extraer criptomonedas[19].

Aunque es pronto para decirlo, es posible que estemos asistiendo a una transición del ransomware tradicional al software dañino criptográfico. Asimismo, se ha observado una preocupante tendencia general para la infraestructura crítica, porque podría tener un impacto en la estabilidad y la capacidad de respuesta de las operaciones de tales sistemas. Porcentaje de sistemas ICS atacados por cryptomining[20].

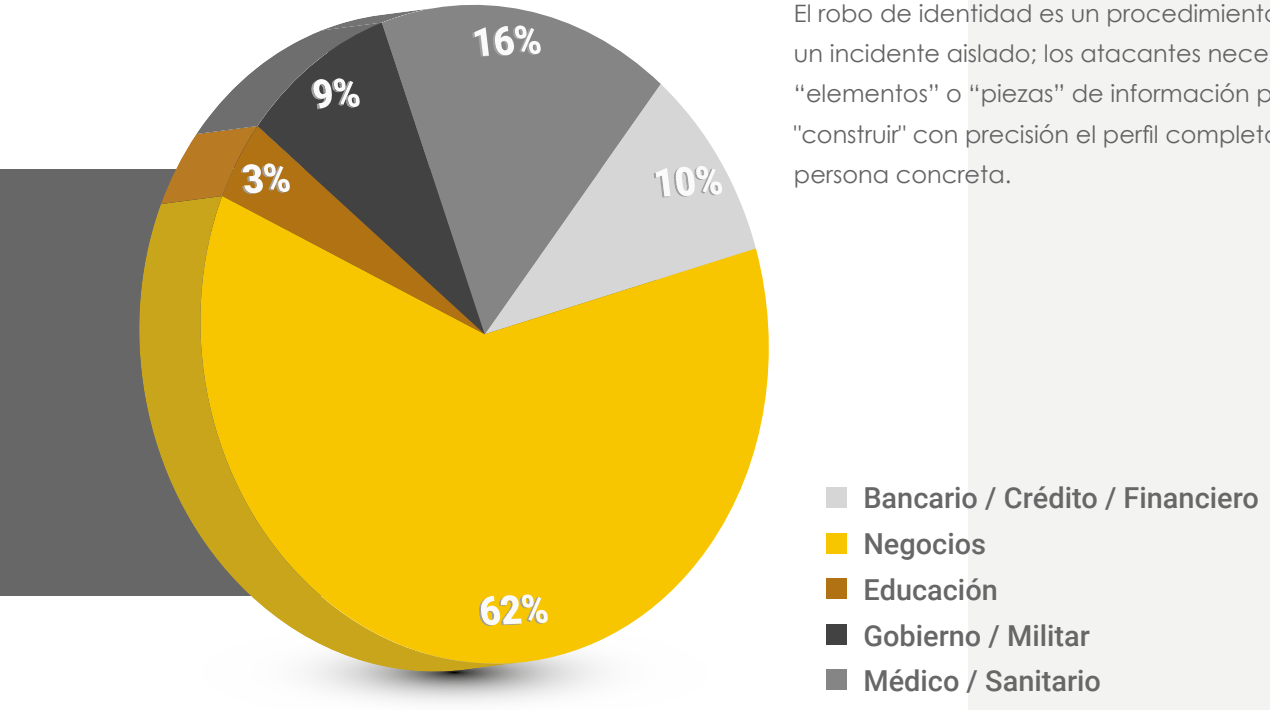


Porcentaje de sistemas ICS atacados por cryptomining

[18]Ver: https://resources.malwarebytes.com/files/2018/07/Malwarebytes_Cybercrime-Tactics-and-Techniques-Q2-2018.pdf
[19]Véase: Avast: Cybercriminals could build cryptomining armies using vulnerable IoT devices at Mobile World Congress 2018 (en https://press.avast.com/cybercriminals-could-build-cryptomining-armies-using-vulnerable-iot-devices-at-mobile-world-congress-2018)
[20]Ver: https://securelist.com/threat-landscape-for-industrial-automation-systems-in-h1-2018/87913/

5.10.Robo de identidad

El robo de identidad es un procedimiento más que un incidente aislado; los atacantes necesitan varios "elementos" o "piezas" de información personal para "construir" con precisión el perfil completo de una persona concreta.



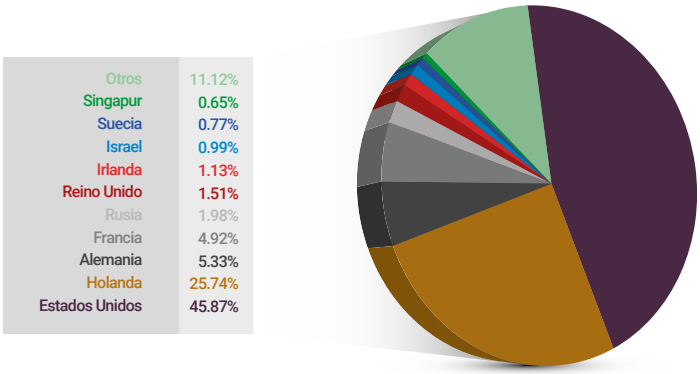
Número de registros comprometidos durante 2018 en diferentes sectores (Fuente: Idtheftcenter)

5.11.Ataques Web

Este tipo de ataques se centran en los sistemas y servicios web para comprometer a la víctima, lo que comprende la explotación de los navegadores, los sitios web, la explotación del sistema de gestión de contenido (CMS) y los propios servicios web. Los ataques drive-by, waterhole, redirection y man-in-the-browser son algunas de las categorías más conocidas de tales acciones. Durante 2018, los ataques basados en la web siguieron siendo una de las amenazas más importantes, por su amplia difusión. Estas son algunas de las evidencias más significativas de 2018:

- APT, campañas de código dañino y ataques basados en watering hole.
- Extensiones para navegadores.
- Incremento de los compromisos relacionados con los sistemas de gestión de contenido (CMS): A principios de 2018, se observaron varios ataques contra Drupal que entregaban mineros de criptomonedas y herramientas de ingeniería social[21]. Más tarde, en septiembre de 2018, se evidenció una ola de ataques dirigidos a sitios de Wordpress vulnerables[22].
- Continúa la tendencia de los exploits kits basados en el navegador web (drive-by).

[21]Véase: https://blog.malwarebytes.com/threat-analysis/2018/09/mass-wordpress-compromises-tech-support-scams/
[22]Véase: https://labs.sucuri.net/?note=2018-09-18



Distribución por países de ataques basados en web en el segundo trimestre de 2018. Fuente: (Securelist)

Ataques a aplicaciones web

La frecuencia de ataques ha disminuido ligeramente. No obstante, permanecen como vectores muy peligrosos los denominados "ataques automatizados", que muestran capacidades de explotación más eficientes.

Las cuestiones más significativas de este tipo de ataques son:

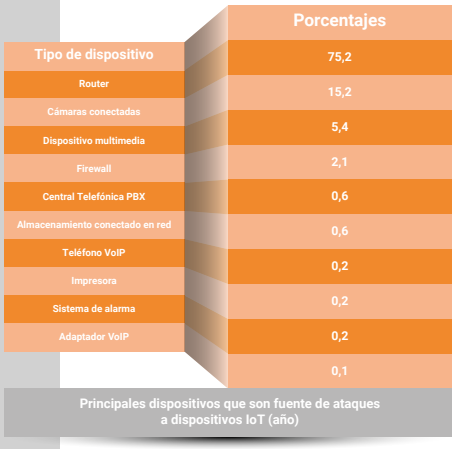
- ***SQL injection*** sigue liderando este tipo de ataques: continúan siendo los mayoritarios en este tipo de acciones (51%) pese a ser la variante más conocida, tanto para los atacantes como para las víctimas.
- La inclusión de archivos locales y el ***cross-site-scripting*** el segundo y tercer ataque más frecuentes, con un 34% y un 8%, respectivamente, de las acciones.
- ***Códigos muertos***, también conocidos como rutas/API huérfanas, son porciones obsoletas o abandonadas de aplicaciones web, que aumentan injustificadamente la superficie de ataque en sistemas interconectados[23].
- No se ha apreciado un significativo incremento de las vulnerabilidades en el sector financiero, comercio minorista y atención sanitaria[24].
- Los ataques a **aplicaciones legacy** siguen estando en los puestos más altos.

5.12.Botnets, IoT, IoT botnets y Android

La amenaza derivada de las botnets sigue siendo alta y, si bien en un principio los atacantes se centraban en sistemas informáticos tradicionales, se ha ampliado la superficie de ataque reorientándose hacia dispositivos móviles y dispositivos IoT. Durante 2018, las botnets se utilizaron principalmente para el robo de información, ataques de denegación de servicio (DDoS) y para el envío de correo no deseado con código dañino. Lo más significativo ha sido el aumento en la aparición de botnets que comprometen dispositivos electrónicos del hogar conectados a internet, utilizándolos como bots. Asimismo, cabe destacar que aproximadamente el 25% de las botnets apuntan a sistemas Android, mientras que las infecciones restantes son, predominantemente, en sistemas Windows.

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

[23]Véase: https://info.tcell.io/hubfs/DemandGen_Content/Research%20Papers/tCell_wp-stateofsecurity-2018-web.pdf
[24]Véase: https://info.whitehatsec.com/rs/675-YBI-674/images/WhiteHatStatsReport2018.pdf

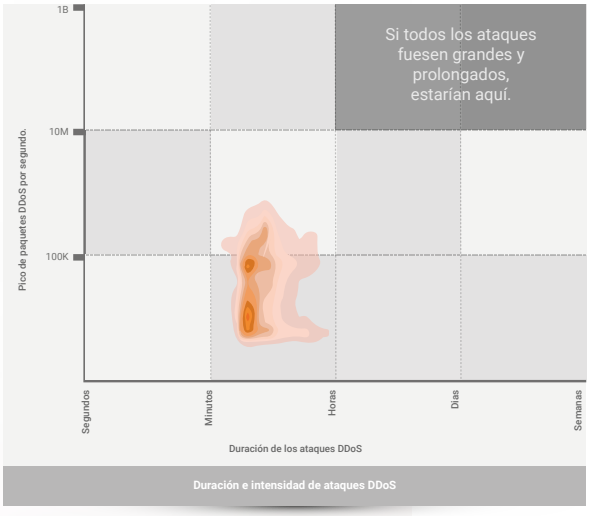


Los routers y las cámaras conectadas son la principal fuente de los ataques, con un 90% de la actividad dañina.

5.13.Ataques DDoS

El número de acciones DDoS sigue en aumento, en concreto, en torno al 16%.

- **Internet de servicios conectados:** Varias investigaciones señalan que las API se están convirtiendo en una superficie de ataque muy popular entre los agentes de las amenazas. Una acción hostil contra tales tecnologías posibilitaría la interrupción de los servicios en diferentes organizaciones, incluso en sectores específicos, como el sanitario.
- **Ataques DDoS y geopolítica:** se han advertido ataques DDoS dirigidos contra autoridades o candidatos políticos de distintos países.
- Los **ataques DDoS como servicio:** El precio de estos proveedores para ejecutar ataques DDoS sencillos ronda los cinco dólares, variando su coste en función de las diferentes capacidades ofrecidas: ataques paralelos, límites por día y múltiples vectores de ataque. En 2018, la National Crime Agency de Reino Unido, junto con la unidad de delitos holandesa (Dutch National High Tech Crime Unit) desmanteló una importante plataforma DDoS conocida como "webstresser.org" que se había utilizado para iniciar entre cuatro y seis millones de ataques en todo el mundo[25].
- **Ataques DDoS multivectoriales:** Akamai informó sobre una serie de ataques específicos dirigidos a los servidores DNS durante casi 2 días, de manera intermitente, que también incluía otro vector (basado en PSH / ACK - TCP) con un pico de 120 Gbps (18.6Mpps). Además, un actor malicioso introdujo un conjunto de generadores de tráfico en un tutorial de YouTube que podía alcanzar un máximo de 170 Gbps (65Mpps). Otros ataques multivectoriales que utilizan incorrectamente los protocolos IKE e IPMI sustentan las teorías de que el código *Mira*" sigue usándose[26].
- **IOT y ataques DDoS:** durante el primer trimestre de 2018 se observó un aumento en el número y la duración de los ataques DDoS detectados.



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

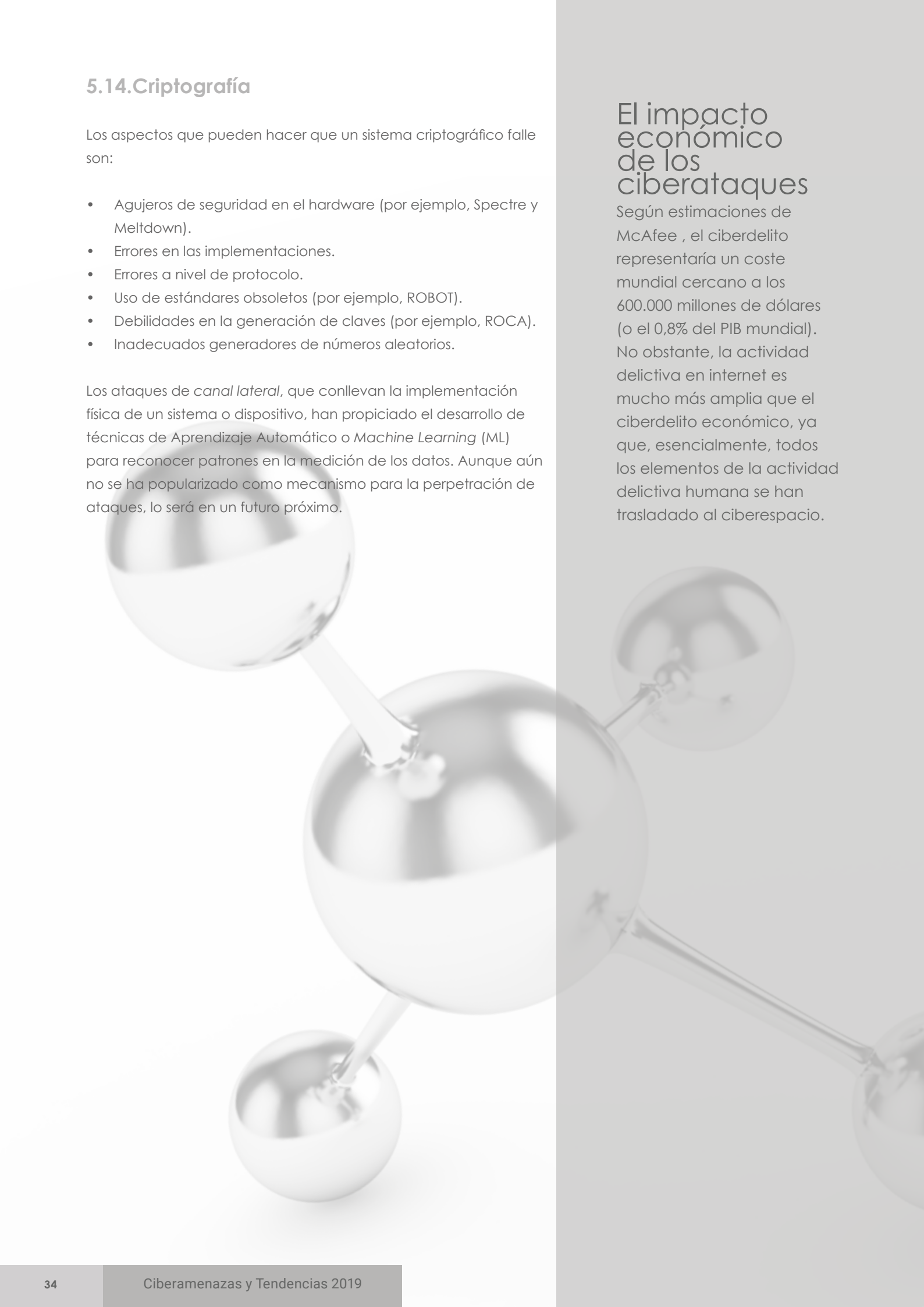
[26]Véase: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-summer-2018-web-attack-report.pdf

5.14.Criptografía

Los aspectos que pueden hacer que un sistema criptográfico falle son:

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

Los ataques de *canal lateral*, que conllevan la implementación física de un sistema o dispositivo, han propiciado el desarrollo de técnicas de Aprendizaje Automático o *Machine Learning* (ML) para reconocer patrones en la medición de los datos. Aunque aún no se ha popularizado como mecanismo para la perpetración de ataques, lo será en un futuro próximo.



El impacto económico de los ciberataques

Según estimaciones de McAfee , el ciberdelito representaría un coste mundial cercano a los 600.000 millones de dólares (o el 0,8% del PIB mundial). No obstante, la actividad delictiva en internet es mucho más amplia que el ciberdelito económico, ya que, esencialmente, todos los elementos de la actividad delictiva humana se han trasladado al ciberespacio.

6 Medidas

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

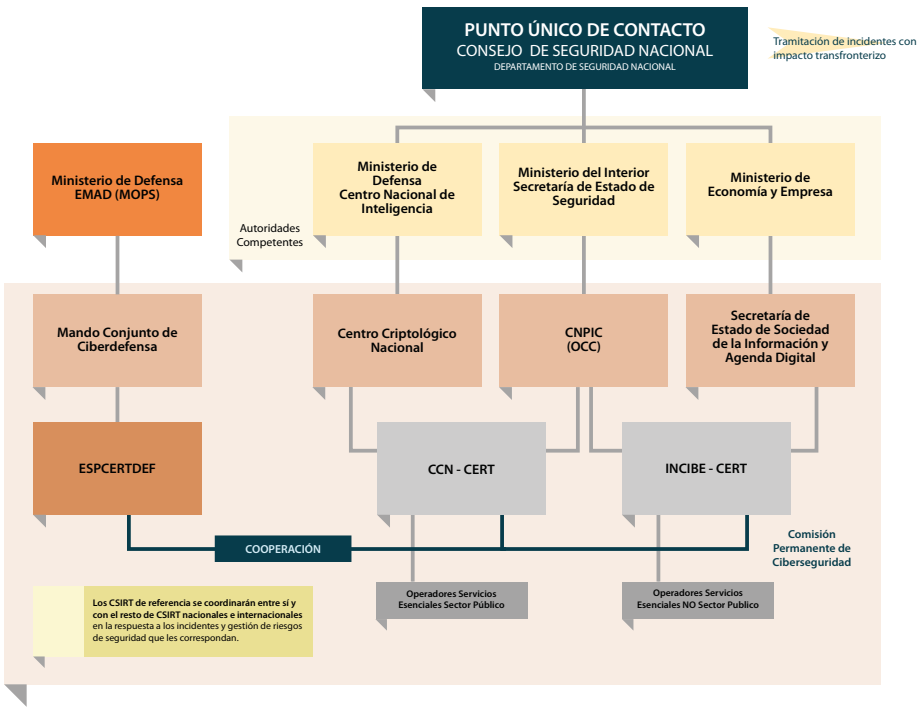
6.1.Marco estratégico y legal

2018 ha sido testigo del desarrollo y/o entrada en vigor de varias iniciativas legales, europeas y nacionales, en aspectos relacionados con la ciberseguridad,

- **Estrategia de Ciberseguridad Nacional**. En 2018 arrancaron los trabajos para la actualización de la Estrategia de Ciberseguridad Nacional de 2013 (finalmente fue publicada en el BOE el 30 de abril de 2019).

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

- **Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información**, en cumplimiento del mandato de transposición de la **Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016**, por el que se establece que el CCN-CERT actuará como el equipo de respuesta a incidentes de referencia para el sector público y como coordinador nacional de la respuesta técnica en los supuestos de especial gravedad y que requieran de un nivel de coordinación superior.



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

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**, que establece los criterios y procedimientos para la notificación por parte del Sector Público al Centro Criptológico Nacional (CCN) de aquellos incidentes que tengan un impacto significativo en la seguridad de la información que manejan y los servicios que prestan.

Cybersecurity Act

Propuesta en el año 2017, parte de un amplio conjunto de medidas para hacer frente a los ciberataques y construir una robusta ciberseguridad en la Unión Europea. Incluye un mandato permanente para la Agencia de Ciberseguridad de la UE, ENISA y una base más sólida en el nuevo marco de certificación de seguridad cibernética para ayudar a los Estados miembros a responder eficazmente a los ataques cibernéticos con un mayor papel en la cooperación y coordinación a nivel de la Unión.

Asimismo, crea también un marco para los certificados europeos de ciberseguridad para productos, procesos y servicios que serán válidos en toda la UE. Esta norma se encuentra actualmente en discusión por el Parlamento y el Consejo.

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

Refuerza la seguridad jurídica y transparencia a la vez que permite que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios.

Propuesta de Reglamento para poner en común recursos y conocimientos técnicos en tecnologías de ciberseguridad[27]

en la Comisión Europea que plantea crear una Red de Centros de Competencia en Ciberseguridad, con el fin de canalizar y coordinar mejor la financiación disponible para la cooperación, investigación e innovación en la materia.

Acceso a pruebas electrónicas

En abril de 2018, la CE propuso dos normas para facilitar a las autoridades policiales y judiciales la obtención de pruebas electrónicas necesarias para investigar y enjuiciar a delincuentes individualizados y a organizaciones terroristas. Tales normas son un reglamento para el acceso transfronterizo a pruebas electrónicas (e-evidence) y una directiva que lo complementa con el propósito de armonizar la designación de los representantes legales de las compañías en línea[28].

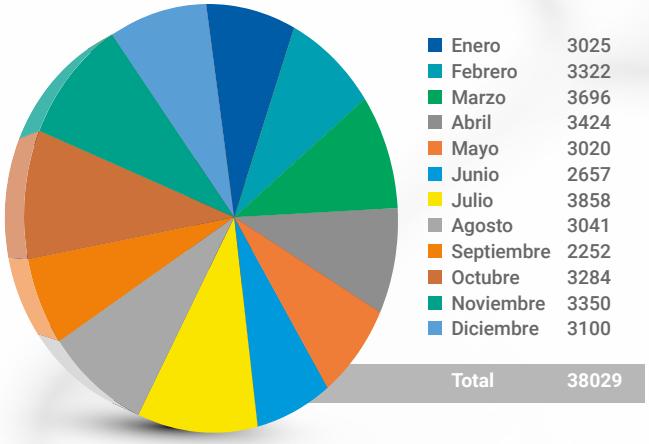
Consejo de Certificación del Esquema Nacional de Seguridad (CoCENS)

Se ha constituido el Consejo de Certificación del Esquema Nacional de Seguridad (CoCENS), compuesto por representantes de todas las partes involucradas: Entidad Nacional de Acreditación (ENAC), Ministerio de Hacienda y Función Pública, Agencia Española de Protección de Datos, Centro Criptológico Nacional y todas las Entidades de Certificación del ENS, públicas y privadas. Su objetivo es ayudar a la adecuada implantación del Esquema Nacional de Seguridad y, en consecuencia, a la más garante prestación de los servicios públicos.

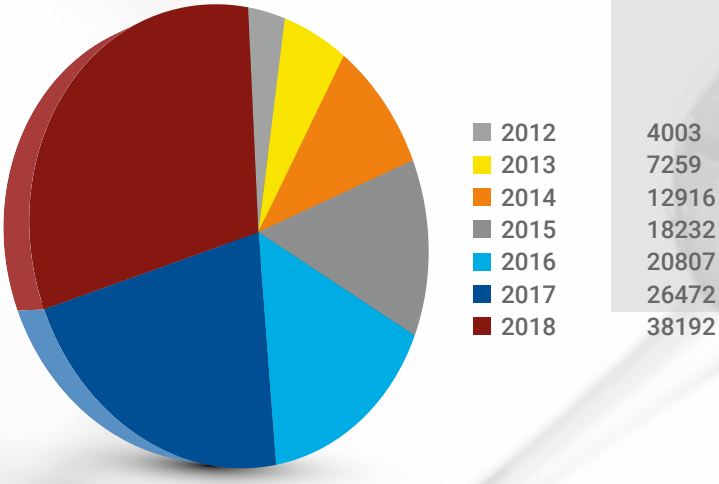
[27]Propuesta para una "Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres", COM (2018) 630, de 12 de septiembre.
[28]Propuesta para la "Regulation on European Production and Preservation Orders for electronic evidence in criminal matters", COM (2018) 225, de 17 de abril, y propuesta para una "Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM (2018) 226, de 17 de abril.

6.2.Actividad del Centro Criptológico Nacional (CCN)

En 2018, el CCN-CERT ha gestionado un total de 38.192 incidentes de seguridad, lo que ha supuesto un incremento del 43,65% con respecto a 2017.

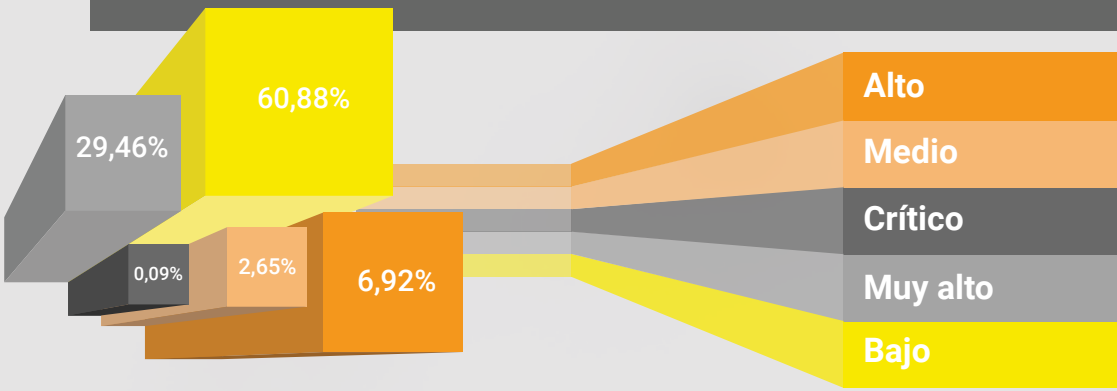


Número de incidentes gestionados por el CCN-CERT en 2018

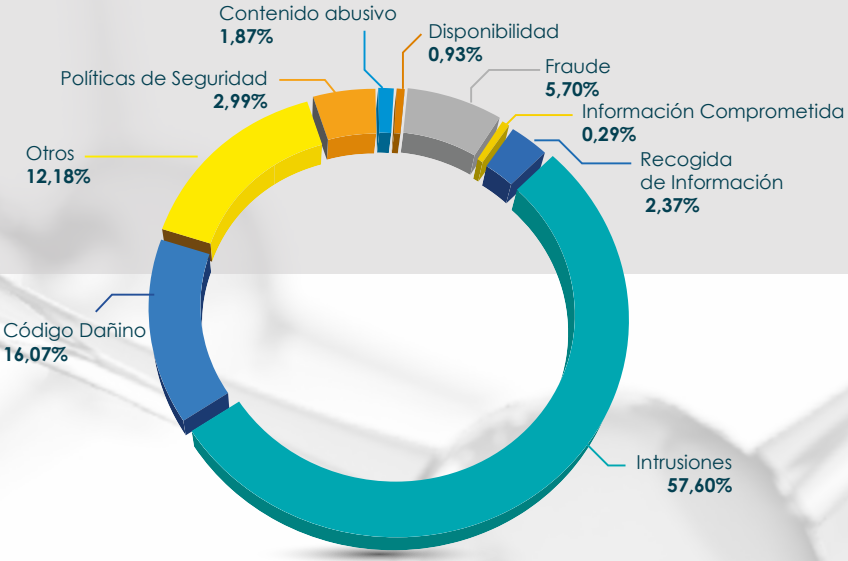


Total de incidentes gestionados por año

El 2,7% de los incidentes gestionados tenían una peligrosidad "Muy Alta" o "Crítica", es decir, el CCN-CERT ha tenido que hacer frente a una media de 2,8 incidentes diarios de este tipo.



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



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

Los ciberincidentes detectados en este período han afectado a múltiples sectores: Administración Pública y, en general, Sector Público, sector Aeronáutico, Entidades Financieras, sector Energético, Sistema Sanitario, Transporte Aéreo y Servicios e Infraestructuras TIC.

Ciberincidentes destacados en 2018

Merecen destacarse los ataques al sector financiero, con el objetivo de la sustracción económica de fondos, cuya actividad ha supuesto a los atacantes un beneficio estimado de más de 1.000 millones de dólares, desde 2014. En el **sector bancario**, en marzo de 2018, los ciberataques Carbanak-Cobalt fueron detectados gracias a la actividad conjunta de una empresa de seguridad y un CERT extranjero.

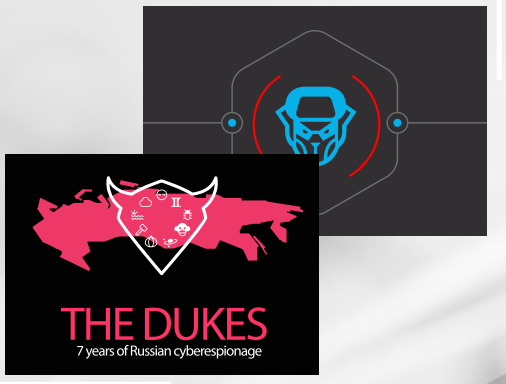
El **CCN-CERT**, por su parte, desplegó su actuación en los momentos previos al cash-out, lo que evitó, en gran medida, consecuencias aun más graves.

El vector de agresión fue spear-phishing, atacando vulnerabilidades no parcheadas. El progreso de los ataques en las redes de las víctimas fue menor de dos semanas hasta alcanzar el control total. Los más destacado es que se utilizaron herramientas disponibles al público (Powershell y Cobalt Strike Beacon), no herramientas construidas a propósito.

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

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

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

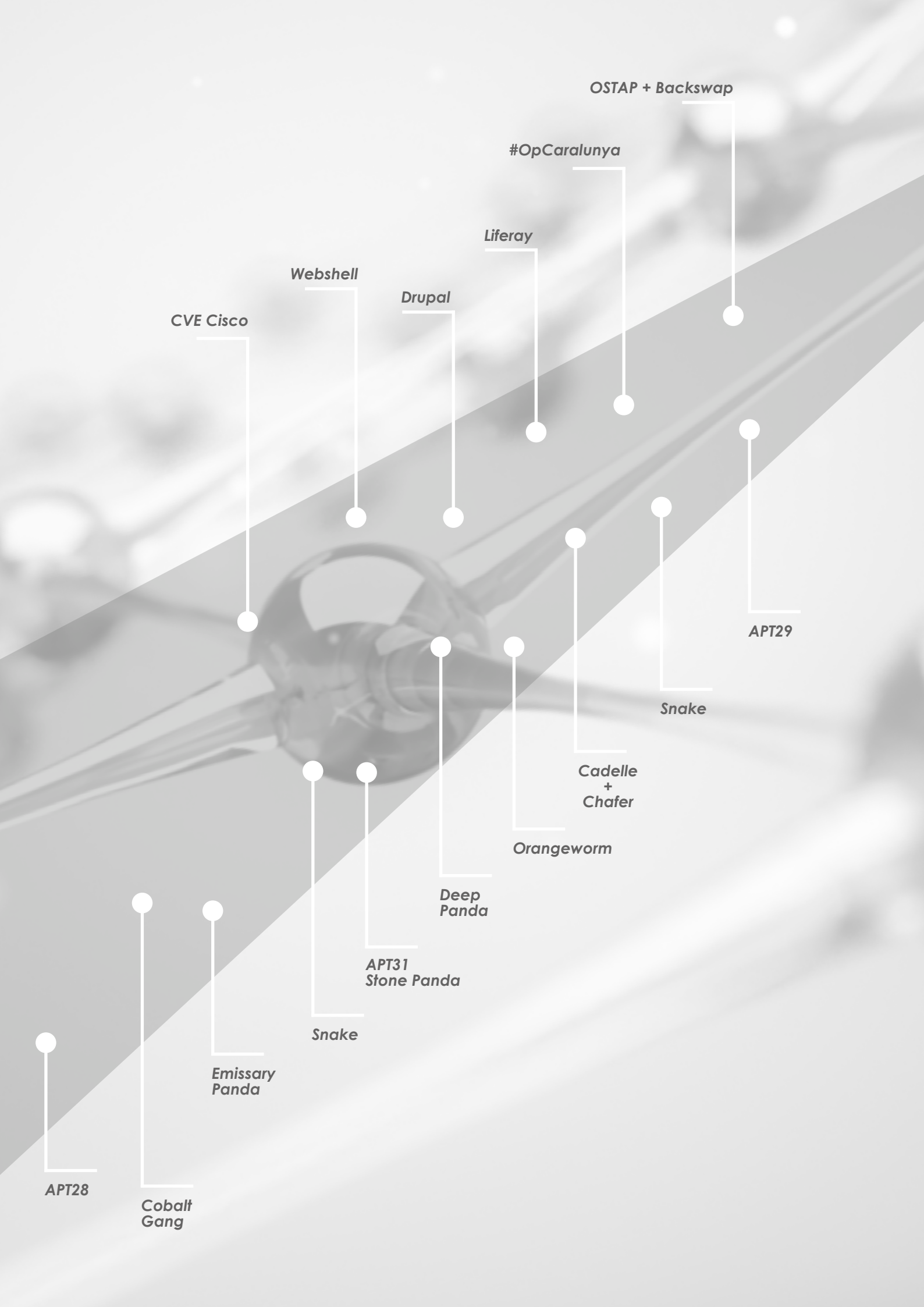


En el **sector de Gobierno** (Administraciones Públicas), el actor principal ha seguido siendo APT29 que, en noviembre de 2018, lanzó una campaña global que apuntaba a un total aproximado de 3.000 víctimas.

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

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

AAPP
Aeronáutico
Bancario
Energía
Salud
Transporte Aéreo
TIC


OSTAP + Backswap
#OpCaralunya
Liferay
Webshell
Drupal
CVE Cisco
APT29
Snake
Cadelle
+
Chafer
Orangeworm
Deep
Panda
APT31
Stone Panda
Snake
Emissary
Panda
APT28
Cobalt
Gang

Los recursos generados por el CCN-CERT

53 nuevas Guías CCN-STIC

72 informes técnicos, 30 informes de amenazas, 26 informes de código dañino y 4 informes de buenas prácticas.

Un total de 22 cursos presenciales

7 cursos on-line y 13 cursos a distancia a través de VANESA. Se han presentado una primera edición del Curso STIC de Seguridad en Infraestructuras de Red y del curso piloto STIC sobre Auditorías de Seguridad.

En materia de detección del talento, se ha proseguido en 2018

con la Plataforma **ATENEA** de desafíos de seguridad, que ha albergado la actividad de más de 5.000 usuarios y más de 70 retos de seguridad; a la que se ha unido ATENEA ESCUELA, que ha incorporado más de 60 retos de seguridad.

Nuevas soluciones y versiones

Nueva solución para la gestión y evolución de los niveles de exposición a los que se encuentra sometida una entidad.

Desarrollo de la versión 7.2, un nuevo conjunto de amenazas. En 2019 ha dado comienzo el proyecto PILAR-Cloud, cuyo objetivo es disponer de la última versión de esta herramienta en la nube, con un nuevo interfaz de usuario.

Desarrollo de la versión 2.0 de CLARA, facilitando su integración con ANA.

Agiliza la labor de análisis de incidentes a través del nuevo motor de inteligencia y su nueva interfaz.

Finalmente

el cuadro siguiente muestra los resultados de la ejecución de las herramientas de análisis **MARTA, MARIA** y **CARMEN** (detección de compromisos por APT).

</marta>

314
Total de binarios subidos

1796
Total de análisis realizados

</maría>

267
Total de usuarios

343
Total de análisis
Pos. 167 / Neg. 182

70,81%
Mejor ratio de detección

1,86%
Peor ratio de detección

carmen
Ciberinteligencia Avanzada

54 Implantaciones operativas en todo el mundo

28 Implantaciones en organismos y empresas

Integración con Reyes, Marta, Claudia y Panda

Cabeceras completas HTTP y subida de ficheros PCAP

vSOC

El CCN está trabajando en la implementación y promoción de los Centros de Operaciones de Seguridad virtuales (vSOC) en su comunidad de referencia, con el objetivo de mejorar las capacidades de vigilancia, detección y respuesta ante cualquier ataque posible, así como optimizar sus recursos en función de la información que manejan y los servicios que prestan.

Convenio de colaboración con el Mº de Justicia

Durante 2018, el Ministerio de Justicia ha suscrito un Convenio de colaboración con el CNI-CCN para el desarrollo del Centro de Operaciones de Seguridad de la Subdirección General de Nuevas Tecnologías de la Justicia.

7 Tendencias

En 2019, los agentes estatales continuarán realizando campañas de intrusión como parte de sus estrategias nacionales y es seguro que para ello utilizarán sus cibercapacidades.

Las entidades de los sectores del gobierno, la defensa, los think tanks y las ONG continuarán siendo los objetivos prioritarios de sus operaciones. Estas intrusiones, probablemente, serán respaldadas por proveedores de los sectores de telecomunicaciones y tecnología, y pueden incluir compromisos en la cadena de suministro, como se ha observado en los años precedentes.
Es de esperar que los futuros ciberataques incrementen su volumen y su sofisticación. Los siguientes párrafos esbozan lo que cabe esperar del inmediato futuro.

1. Aumentarán los ciberataques patrocinados por Estados

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

2. Ataques a la cadena de suministro

En 2019, los ataques a la cadena de suministro aumentarán a medida que las grandes corporaciones se abran a un mayor riesgo según aumenten la confianza en sus partners.

Debido a estos peligros, muchas empresas que dependen de terceros han creado procesos de gestión de riesgos de proveedores dentro de sus organizaciones. Los equipos de gestión de estos riesgos dentro de las organizaciones serán más habituales a medida que aumenten los ataques a la cadena de suministro.

3. La nube como objetivo

Durante 2018 se han producido muchos incidentes relacionados con la computación en la nube y se espera que continúen y evolucionen en los próximos años, debido a que una gran cantidad de datos se mueve allí y los atacantes siguen los mismos pasos.

4. Sofisticación del código dañino

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

5. Los ciberataques dirigidos a personas

Los seres humanos siguen siendo el eslabón débil en todos los sistemas de seguridad, por lo que, a medida que aumente la eficacia de las protecciones contra código dañino, los agentes de las amenazas modificarán su objetivo, atacando a las personas. Es de esperar que los próximos años sean testigo de un mayor volumen de correos electrónicos de suplantación de identidad (phishing) y sitios web falsos diseñados para engañar al usuario y facilitar el acceso a datos confidenciales, tales como contraseñas o números de tarjetas de crédito.

6. Utilización de dispositivos inteligentes en ciberataques

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

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

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

Es de esperar más dispositivos IoT mal protegidos destinados a otros fines perjudiciales. Entre los más problemáticos se encuentran los ataques contra dispositivos de IoT que conectan los mundos digital y físico. Es de esperar un número creciente de ataques contra estos dispositivos que controlan la infraestructura crítica, como la distribución de energía y las redes de comunicaciones, y a medida que los del hogar se hagan más omnipresentes, es probable que haya futuros intentos de utilizarlos como arma por los Estados.

8. Incremento del Criptojacking

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

9. El código dañino será más engañoso

Durante los próximos años se verán nuevas variantes de malware más difíciles de detectar y que podrían residir en los sistemas infectados durante un período de tiempo muy largo.

10. Aprendizaje automático para bloquear nuevas amenazas

El desarrollo de nuevos tipos de código dañino sigue a un ritmo incesante. Las herramientas de *Machine Learning*, que monitorizan la actividad del ordenador para detectar y bloquear automáticamente los procesos sospechosos incluso antes de que un malware haya sido identificado oficialmente, constituirán herramientas primordiales. Esta protección proactiva será vital para vencer a los ciberdelincuentes, especialmente a aquellos que usan malware con técnicas de ocultación.

11. IA como herramienta en los ciberataques

La fragilidad de algunas tecnologías de inteligencia artificial se convertirá en una preocupación creciente en 2019. De alguna manera, el surgimiento de sistemas críticos de IA como objetivos de ataque comenzará a reflejar la secuencia que se vio hace 20 años en internet, lo que atrajo rápidamente la atención de los delincuentes cibernéticos.

Recíprocamente, los defensores dependerán cada vez más de la IA para contrarrestar los ataques, identificar las vulnerabilidades y fortalecer sus sistemas ante posibles ataques. Con el tiempo, esta inteligencia artificial dirigida a la seguridad también podría ayudar a las personas a comprender mejor las concesiones de entregar información personal a cambio del uso de una aplicación u otro beneficio adicional.

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

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

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

13. Incremento de la actividad legislativa y regulatoria

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

La atribución y la responsabilidad son dos de los aspectos más importantes cuando se trata de derrotar a los ciberatacantes. Sin riesgos y sin repercusiones por la actividad dañina llevada a cabo en el ciberespacio, los agentes de las amenazas seguirán atacando.

www.ccn.cni.es
www.ccn-cert.cni.es
oc.ccn.cni.es

centro criptológico nacional

IA-13/19