CCN-CERT IA-09/16

CIBERAMENAZAS 2015/TENDENCIAS 2016

RESUMEN EJECUTIVO



cn-cert

centro criptológico nacional

CONTENIDOS

1	PRÓLOGO	3
2	FACTORES DE LAS AMENAZAS	4
3	LAS CIBERAMENAZAS Y SUS AGENTES	6
4	HERRAMIENTAS UTILIZADAS POR LOS ATACANTES	14
5	RESILIENCIA	22
6	ACTIVIDAD DEL CCN	26
7	TENDENCIAS	28
	ANEXO B: DISPOSITIVOS Y COMUNICACIONES MÓVILES	32

1. PRÓLOGO

Al igual que en años anteriores, 2015 ha visto incrementar el número, tipología y gravedad de los ataques contra los sistemas de información de las Administraciones Públicas y Gobiernos, de las empresas e instituciones de interés estratégico o aquellas poseedoras de importantes activos de propiedad intelectual e industrial y, en general, contra todo tipo de entidades y ciudadanos.

La generalización del uso de los medios electrónicos incrementa la superficie de ataque y, en consecuencia, los beneficios potenciales derivados, lo que constituye sin duda uno de los mayores estímulos para los atacantes.

Así lo ha constatado, un año más, el **Centro Criptológico Nacional** al elaborar su ya tradicional *Informe de Ciberamenazas y Tendencias*[1] y cuyo extracto y principales conclusiones presentamos en este documento. En él se examina el impacto, en España y fuera de sus fronteras, de las **amenazas y los ciberincidentes** más significativos ocurridos en 2015: **ciberespionaje** (por estados y empresas), **ciberdelincuencia, hacktivismo**[2] y, como singularidad, el que hemos denominado **ciberyihadismo** (acciones atribuibles a grupos de tendencia violenta y radical dentro del islam político), los actores internos o los ciberinvestigadores.

El documento matriz, y este Resumen Ejecutivo, abordan además las **herramientas** empleadas por los atacantes (con especial relevancia de los exploits[3] , exploit-kits y código dañino) y la **resiliencia** (la forma en que los sistemas de información han sabido afrontar los ciberataques y sus **vulnerabilidades** y las **medidas** adoptadas para fortalecerlos).

Además el Informe completo recoge las principales **tendencias para este 2016** en materia de ciberseguridad y tres grandes anexos que completan esta visión general: (Anexo A) **Actividad** más destacada del **Centro Criptológico Nacional**; (Anexo B) **Dispositivos y comunicaciones móviles** y (Anexo C) **Hacktimismo en 2015**.

La mayor parte de la información de este informe es el resultado de la experiencia del CCN-CERT durante 2015 en el desarrollo de sus competencias. Asimismo, se han tenido en cuenta otras fuentes documentales, nacionales e internacionales, públicas y privadas, y se ha contado con la colaboración de entidades externas, profesionales y miembros del mundo académico.

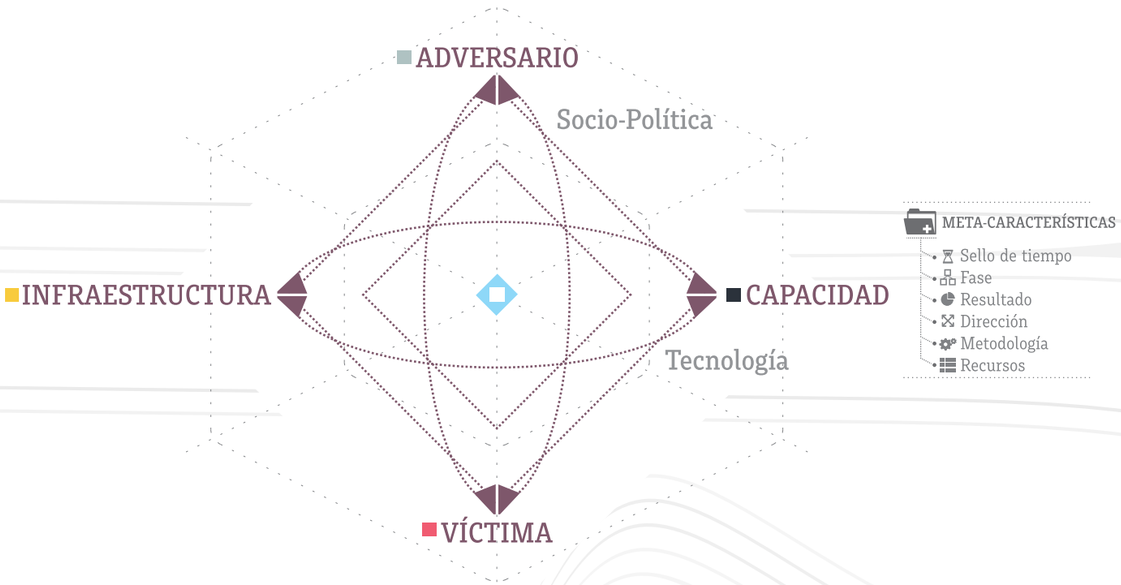
CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2016.09.27 18:37:15 +02'00'

[1] El Informe completo (CCN-CERT IA-09/16 Ciberamenazas 2015/Tendencias 2016) está disponible en el portal https://www.ccn-cert.cni.es
[2] Activismo digital antisocial. Sus practicantes persiguen el control de ordenadores o sitios web para promover su causa, defender su posicionamiento político, o interrumpir servicios, impidiendo o dificultando el uso legítimo de los mismos.
[3] Un exploit es un programa que explota o aprovecha una vulnerabilidad de un sistema informático en beneficio propio. Exploit día cero: Aprovechamiento de una vulnerabilidad inmediatamente después de haber sido descubierta. Se beneficia del lapso de tiempo requerido por los fabricantes para reparar las vulnerabilidades reportadas.

2. FACTORES DE LAS AMENAZAS

1. Inadecuada **gestión de actualizaciones de seguridad (parches)** y el uso de **software desactualizado** en ordenadores, dispositivos móviles o servidores centrales.
2. Desconocimiento de los métodos seguidos por los **ataques de Ingeniería Social**.
3. El período, en ocasiones largo, en el que fabricantes y proveedores de servicios solucionan las **vulnerabilidades detectadas**.
4. Los ataques a través de **Amenazas Persistentes Avanzadas (APT[4])** representan actualmente la amenaza más significativa para las empresas y los organismos públicos de todo el mundo y continuarán siéndolo en el futuro.
5. La **interconexión de los sistemas de entornos industriales**, particularmente en el área de Infraestructuras Críticas[5], dificulta las medidas a adoptar, máxime cuando el período de distribución de malware (tanto fijo como móvil) cada vez es menor.
6. Profesionalización de los atacantes, lo que provoca la **sofisticación de las amenazas**
7. Disponibilidad de **herramientas de ataque** que posibilita la aparición de nuevos actores.
8. **Modelo de negocio** de los atacantes, con dificultad para la atribución del delito.

Un modelo de análisis de seguridad es el recogido en la Guía CCN-STIC 425 Ciclo de Inteligencia y Análisis de Intrusiones, en el que se incluyen dos nuevas meta-características: la **Socio-Política**, que vincula al Adversario con su Víctima y la **Tecnológica**, que vincula la Infraestructura con la Capacidad, tal y como se representa en la figura siguiente:



2.1 EVOLUCIÓN TECNOLÓGICA Y CIBERSEGURIDAD

Se destacan los elementos más significativos del año 2015:

- Penetración del software (conflicto entre funcionalidad y seguridad)
- Dispositivos móviles versus protección de la información
- Compatibilidad versus seguridad de la información
- Pérdida de confianza en los servicios electrónicos
- Nuevas áreas de aplicación del IoT (Internet de las Cosas[6])
- Exigencia de redes separadas
- Seguridad en equipamientos médicos
- Inexistencia de alternativas analógicas
- Dependencia tecnológica en las infraestructuras críticas (cibersabotaje, sector financiero, medios de comunicación, otros estados, redes que gestionan infraestructuras críticas y otras)



[4] Advanced Persistent Threat
[5] Véase el IA-04/16 Amenazas y análisis de riesgos en Sistemas de Control Industrial (ICS) del CCN-CERT (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1381-ccn-cert-ia-04-16-amenazas-y-analisis-de-riesgos-en-sistemas-de-control-industrial-ics/file.html)
[6] Internet of Things (IoT)

3. *LAS CIBERAMENAZAS Y SUS AGENTES*

3.1 CIBERESPIONAJE / ACTORES ESTATALES / ORGANIZACIONES PRIVADAS

Como en años anteriores, durante 2015 el **ciberespionaje** (político o industrial) ha constituido la mayor amenaza para los países, estando especialmente dirigida a los sistemas de información de las corporaciones industriales, empresas de Defensa, alta tecnología, automoción, transportes, instituciones de investigación y Administraciones Públicas.
La complejidad, volumen e impacto de estos ataques, habitualmente conducidos a través de APTs han sido similares a lo sucedido en 2014. Las evidencias de 2015 permiten afirmar que, en significativas ocasiones, tales acciones han sido llevadas a cabo por **Servicios de Inteligencia o Departamentos de Defensa extranjeros**, que siguen invirtiendo importantes recursos en dotarse de capacidades de defensa y, también, de ataque. Asimismo, los Estados, en mayor o menor medida, son objeto de ciberataques con origen en otros Estados, interesados en obtener información de relevancia económica, geoestratégica o militar.
Además, los países continúan aprovechando los conflictos internacionales para llevar a cabo ataques (pudo observarse en la crisis de Ucrania).
En el caso del ciberespionaje industrial, son las organizaciones privadas las que actúan de atacantes (en ocaciones también los Estados). El lucro derivado de una obtención ilícita de información y, el deterioro intencionado de los sistemas de la competencia son buenos motivos para que las organizaciones del sector privado desarrollen ciberataques.

- **ATAQUES MÁS DESTACADOS DE 2015:**

- En **España**, durante 2015, los actores principales en el robo de información han sido los grupos: APT28, Snake, APT29 y Emissary Panda.
-Ataque al Bundestag alemán: los sistemas centrales de la red interna del Parlamento Federal fueron comprometidos.

ESTE TIPO DE ATAQUES CONTINUARÁ EN ASCENSO EN LOS PRÓXIMOS AÑOS, AL TIEMPO QUE LO HACE SU SOFISTICACIÓN Y PELIGROSIDAD.



3.2 CIBERDELITO / CIBERDELINCUENTES

El **ciberdelito**, su profesionalización y el crecimiento de la organización interna de sus actores han acaparado en 2015 el siguiente nivel de atención. La sofisticación de las técnicas usadas, la disponibilidad de nuevas o renovadas herramientas (incluyendo la prestación de servicios delincuenciales bajo demanda - on demand-) y la pulcritud en la perpetración de tales acciones constituyen una preocupación en franco crecimiento.
El año 2015, de manera análoga a lo ocurrido en 2014, evidenció que las organizaciones cibercriminales están dispuestas a invertir grandes cantidades de dinero en la preparación de sus acciones. Del mismo modo, el denominado Cibercrimen como Servicio "CaaS *Cybercrime*-As-A-Service" ha incrementado su penetración y profesionalización, habiéndose percibido una cierta "competencia" entre los propios ciberdelincuentes, lo que obliga a sus autores a prestar a sus "clientes" un "servicio" cada vez más fiable.

- **ATAQUES MÁS DESTACADOS DE 2015:**

-**Campaña Carbanak** dirigida contra entidades financieras de Europa del Este, en donde lograron infectar a varios bancos a través de spearphishing. Se estima que los autores fueron capaces de sustraer entre 250 y 1.000 millones de dólares.
-**Corcow**: un ataque dirigido usando técnicas de inteligencia, a entidades financieras (y sus clientes), que tuvo especial incidencia en Rusia y Ucrania.
-Ataque a **Hacking Team**: exfiltración y publicación de informes de esta empresa italiana especializada en la venta de herramientas y tecnologías de ataque y monitorización.
-**Home Depot** sufrió el robo de 56 millones de números de tarjetas de crédito y débito, además de 53 millones de direcciones de correo electrónico de sus clientes.
- Las sustracciones de datos personales de **Community Health Systems** (4,5 millones de pacientes), Anthem (80 millones de asegurados) y Premera (11 millones de aseguradas en Estados Unidos).

LOS BENEFICIOS OBTENIDOS Y EL ACCESO CADA VEZ MÁS FÁCIL A LAS HERRAMIENTAS DE PERPETRACIÓN DE ESTE TIPO DE ATAQUES PROPICIARÁ EL INCREMENTO DEL NÚMERO DE CIBERDELINCUENTES Y, EN CONSECUENCIA, EL DE SUS ACCIONES.



Categoría	Objetivo	Tipo de la organización	Impacto económico
Hackers[7] -no- profesionales	Brechas de seguridad	Individuos / No-profesional	Bajo
Crackers	Software de seguridad, piratería del copyright	Individuos / No-profesional	Bajo
Piratas	Seguridad, piratería del copyright	Individuos / Organizados	Bajo
Atacantes	Robo IP, extorsión	Criminal / No-profesional	Alto
Exploradores de vulnerabilidades “Black hat”	Vulnerabilidades TIC	Individuos / No-profesional	Bajo en ejecución; alto en consecuencias si se venden o ceden a terceros las vulnerabilidades
Desarrolladores profesionales de código dañino y script kiddies[8]	Vulnerabilidades TIC y formas para explotarlas	Individuos / No-profesional	Bajo en ejecución; alto en consecuencias si se venden o ceden a terceros las vulnerabilidades
Carders[9] y muleros	Robo de datos	Organizada	Alto
Extorsionadores	Botnets y código dañino como herramientas para la extorsión	Individuos / No-profesionales / Organizados	Medio
Phishing[10] e ingeniería social	Spam	Organizados	Alto
Defraudadores “Black hat”	Ataques script	Organizados	Alto
Tramposos	Juego online	Individuos / Organizados	Medio
Defraudadores “Click fraud”	Trampas y acceso	Individuos / Organizados	Alto
Hacktivistas	Ataques políticos	Individuos / Organizados	Bajo

[7] Hacker es alguien que descubre las debilidades de un ordenador o una red informativa o también alguien con un conocimiento avanzado. El término es reclamado por los programadores, quienes argumentan que los que irrumpen en los ordenadores se denomina “craker”, sin diferenciar entre los delincuentes informáticos “sombreros negros Black hat” y los expertos en seguridad informática “sombreros blancos o White hat”, por último “sombrero gris o Grey hat” se referiría a un hacker talentoso que a veces actúa ilegalmente, pero con buenas intenciones. Sin embargo todavía existe controversia en estos términos. https://wikipedia.org/wiki/Hacker_seguridad_informatica

[8] Son aquellos que, con conocimientos limitados y haciendo uso de herramientas de terceros, perpetran sus acciones a modo de desafío, sin ser, en ocasiones, plenamente conscientes de sus consecuencias.

[9] Carders. Tipo de hacker que trafican con tarjetas de crédito

[10] Phishing. Suplantación de identidad. Consiste en el envío de correos electrónicos que aparentan ser fiables y que suelen derivar a páginas web falsas recabando datos confidenciales de las víctimas.

3.3 CIBERTERRORISMO / GRUPOS TERRORISTAS

Aunque la peligrosidad potencial de las acciones atribuibles al ciberterrorismo sigue creciendo, no puede afirmarse que, en la actualidad, represente una grave amenaza, especialmente por las limitadas capacidades técnicas que se han observado en sus despliegues.

3.4 HACKTIVISMO / HACKTIVISTAS[11]



Personas o grupos, más o menos organizados, que desarrollan sus acciones en el ciberespacio movidos generalmente por motivos ideológicos. En los últimos años sus ciberataques (desfiguración de páginas web, ataques DDoS[12] o sustracción de datos confidenciales de sus objetivos) pretendieron ser la respuesta a determinadas medidas adoptadas por gobiernos y que consideraban perjudiciales para la libertad de Internet. En general, el año se ha caracterizado por un número reducido de operaciones hacktivistas comparado con años anteriores.

- **ATAQUES MÁS DESTACADOS DE 2015:**

  -Confrontación entre grupos en la órbita de ‘**Anonymous**’, por un lado, contra identidades hacktivistas que apoyan o muestran simpatía por el grupo yihadista ‘**Daesh**’[13].

  -Tras el ataque al semanario francés, **Charlie Hebdo**, se produjeron múltiples desfiguraciones a sitios web franceses. La operación de Anonymous #OpCharlieHebdo Anonymous dio lugar a la reacción #OpFrance, en la que decenas de sitios web franceses mostraron textos islámicos.

  -En **Iberoamérica** se mantuvo una ofensiva contra el Gobierno de Nicolás Maduro (Venezuela) y varias operaciones antigubernamentales en México.

[11] El Anexo C del Informe completo de Amenazas CCN-CERT IA-09/16 recoge un monográfico sobre Hacktivismo en 2015

[12] Distributed Denial of Service (DDoS) (Denegación de Servicio Distribuida). Ataque de denegación de servicio que se realiza utilizando múltiples puntos de ataque simultáneamente

*[13] Dulat Aslamiyah Eraq wa Sham (**Daesh**) Islamic State of Iraq and Sham (ISIS).Sham es una zona que comprende todo Siria y parte del Líbano*

-En España se caracteriza por una baja densidad con la excepción de 'La 9ª Compañía de Anonymous'.

3.5 CIBERYIHADISMO / GRUPOS YIHADISTAS

En 2015 ha aparecido una nueva amenaza: el **ciberyihadismo**, que usando métodos, procedimientos y herramientas del terrorismo, el hacktivismo y la ciberguerra constituye una realidad incipiente y supone una de las mayores amenazas con las que se enfrentarán las sociedades occidentales en los próximos años.
Las importantes vías de financiación de estos grupos (al socaire de Daesh) hacen posible que puedan llegar a adquirir los conocimientos y las herramientas precisas para el desarrollo de ciberataques o la contratación de los mismos.
Hasta el momento, sus ataques se han limitado a la desfiguración de páginas web, ataques DDoS a pequeña escala o, más comúnmente, al uso de Internet y de las redes sociales para la diseminación de propaganda o el reclutamiento y la radicalización, actividades que no exigen grandes conocimientos o infraestructura.

- **ATAQUES MÁS DESTACADOS DE 2015:**

-Uso de código dañino (por ejemplo, en Siria se detectaron ciberataques para obtener datos sobre posiciones de los objetivos locales).
-Ataque a sitios web
-Instrucciones para el uso de una herramienta de acceso remoto (RAT[14]) para el control de equipos.
-Ataques a redes sociales para la obtención de información
-Ataques de phishing para obtener datos de tarjetas de crédito y obtener información.
-El grupo **CyberCaliphate** afiliado a Daesh atacó y tomó el control de las cuentas de Twitter y Youtube del US Central Command.

LAS CAPACIDADES DEL CIBERYIHADISMO NO HAN HECHO SINO EMPEZAR A MOSTRARSE. ES DE ESPERAR CIBERATAQUES MÁS NUMEROSOS, MÁS SOFISTICADOS Y MÁS DESTRUCTIVOS EN LOS PRÓXIMOS AÑOS, EN TANTO PERSISTA LA ACTUAL SITUACIÓN EN TORNO A DAESH.

3.6 CIBERVANDALISMO/VÁNDALOS Y SCRIPT KIDDIES

Se denomina cibervándalos a aquellos individuos que, poseyendo significativos conocimientos técnicos, llevan a cabo sus acciones con el único motivo de demostrar públicamente que son capaces de hacerlo.
Por su parte, los denominados script kiddies son aquellos que, con conocimientos limitados y haciendo uso de herramientas construidas por terceros, perpetran sus acciones a modo de desafío, sin ser, en muchas ocasiones, plenamente conscientes de sus consecuencias.
Pese a la difusión mediática que durante 2015 han recibido las acciones de los cibervándalos, no constituyen una amenaza seria a los intereses de las organizaciones.

- **ATAQUES MÁS DESTACADOS DE 2015**

-Desfiguración de la página web de Malaysian Airlines

DE CARA A LOS PRÓXIMOS AÑOS NO SE PREVÉN ALTERACIONES SUSTANCIALES DEL COMPORTAMIENTO DE ESTOS ACTORES

[14] **RAT.** *Remote Access Tools*

3.7 ACTORES INTERNOS

Los también denominados Insiders son personas que están o han estado trabajando para una organización (empleados o exempleados, colaboradores y proveedores) y que provocan brechas de seguridad importantes. En algunos casos se detecta exfiltración de información por motivos económicos o políticos, en otros casos se da por negligencia o despecho de determinadas personas.
En varios de los ciberincidentes ocurridos en 2015 se pudo observar cómo algunos empleados manejaron información sensible en servidores privados sin adoptar las adecuadas medidas de seguridad.

- **ATAQUES MÁS DESTACADOS DE 2015**

-Un empleado de una **compañía de seguros** depositó datos de las reclamaciones de 27.000 asegurados en un servidor privado para probar un determinado software.
-Caso de **AMS-IX** (compañía holandesa de intercambio de Internet): un error durante los trabajos de mantenimiento hicieron caer la plataforma y los servicios web no estuvieron disponibles durante diez minutos, lo que, pese a lo limitado del tiempo, tuvo repercusión internacional, dada la importancia del sistema afectado.

LOS ACTORES INTERNOS SÓLO HAN VENIDO REPRESENTANDO UN PEQUEÑO PORCENTAJE DE LOS AGENTES DE LAS AMENAZAS (MENOS DEL 15%).

3.8 CIBERINVESTIGADORES

Buscan vulnerabilidades en entornos TIC al objeto de verificar la protección de los sistemas objeto de sus investigaciones. Con frecuencia, además de informar a las empresas, se publica en los medios de comunicación el resultado de sus investigaciones con un doble efecto: positivo y negativo.
En el plano negativo es evidente que la publicidad de cualquier vulnerabilidad conlleva que los sistemas identificados sean más vulnerables a ataques externos, facilitando la acción de los atacantes, que pueden llegar a beneficiarse de los resultados de las investigaciones. Incluso, se han dado casos de ciberinvestigadores acusados de realizar extorsiones a las entidades investigadas.

AGENTES DE LA AMENAZA

	ORIGEN DE LA AMENAZA	MOTIVACIÓN	NIVEL DE CONOCIMIENTO
1	Estados	Mejora de su posición geopolítica o estratégica. Ciberterrorismo como falsa bandera Contraterrorismo o protección de la seguridad nacional.	ALTO
2	Ciberdelincuentes	Beneficio económico (directo o indirecto)	ALTO > MEDIO
3	Hacktivistas	Acercarse a sus objetivos ideológicos.	MEDIO
4	Grupos Yihadistas	Lograr la penetración de su ideología.	BAJO>MEDIO
5	Grupos terroristas	Lograr cambios en la sociedad, mediante el uso del terror, o influir en la toma de decisiones políticas. Objetivos de alto impacto.	MEDIO > BAJO
6	Cibervándalos	Picardía. Búsqueda de desafíos.	BAJO
7	Actores internos	Venganza o beneficios económicos o ideológicos (en ocasiones, dirigida desde el exterior).	ALTO > BAJO
8	Ciberinvestigadores	Revelación de debilidades (y su propio perfil)	MEDIO
9	Organizaciones privadas	Obtener o vender información valiosa.	ALTO > BAJO



OBJETIVOS

SECTOR PÚBLICO	SECTOR PRIVADO	CIUDADANOS
Ciberespionaje político	Ciberespionaje económico	Ciberespionaje instrumental
Cibercapacidades ofensivas	Cibercapacidades ofensivas	
Sustracción, publicación o venta de información	Sustracción, publicación o venta de información	Sustracción, publicación o venta de información
Manipulación de información	Manipulación de información	Manipulación de información
Interrupción de sistemas	Interrupción de sistemas	Interrupción de sistemas
Toma de control de sistemas	Toma de control de sistemas	Toma de control de sistemas
Sustracción y publicación de la información sustraída	Sustracción y publicación de la información sustraída	
Desfiguraciones	Desfiguraciones	
Interrupción de sistemas	Interrupción de sistemas	
Toma de control de sistemas	Toma de control de sistemas	
Interrupción de Sistemas / Toma de control	Interrupción de Sistemas / Toma de control	Propaganda y reclutamiento
Desfiguraciones	Desfiguraciones	
Interrupción de Sistemas / Toma de control	Interrupción de Sistemas / Toma de control	
Sustracción de información	Sustracción de información	Sustracción de información
Interrupción de sistemas	Interrupción de sistemas	
Sustracción, publicación o venta de información	Sustracción, publicación o venta de información	
Interrupción de sistemas	Interrupción de sistemas	
Recepción y publicación de información	Recepción y publicación de información	
	Sustracción de información (espionaje industrial)	Uso/abuso o reventa de información de clientes o público en general

BAJO

- No se han observado nuevas amenazas o tendencias, o
- Se dispone de medidas suficientes para neutralizar la amenaza, o
- No ha habido incidentes especialmente significativos en el periodo analizado.

MEDIO

- Se han observado nuevas amenazas o tendencias, o
- Se dispone de medidas (parciales) para neutralizar la amenaza, o
- Los incidentes detectados no han sido especialmente significativos.

ALTO

- Las amenazas o su tendencia se ha incrementado significativamente.
- Las medidas adoptadas tienen un efecto muy limitado, por lo que la amenaza permanece.
- Los incidentes detectados han sido especialmente significativos.

4. HERRAMIENTAS UTILIZADAS POR LOS ATACANTES

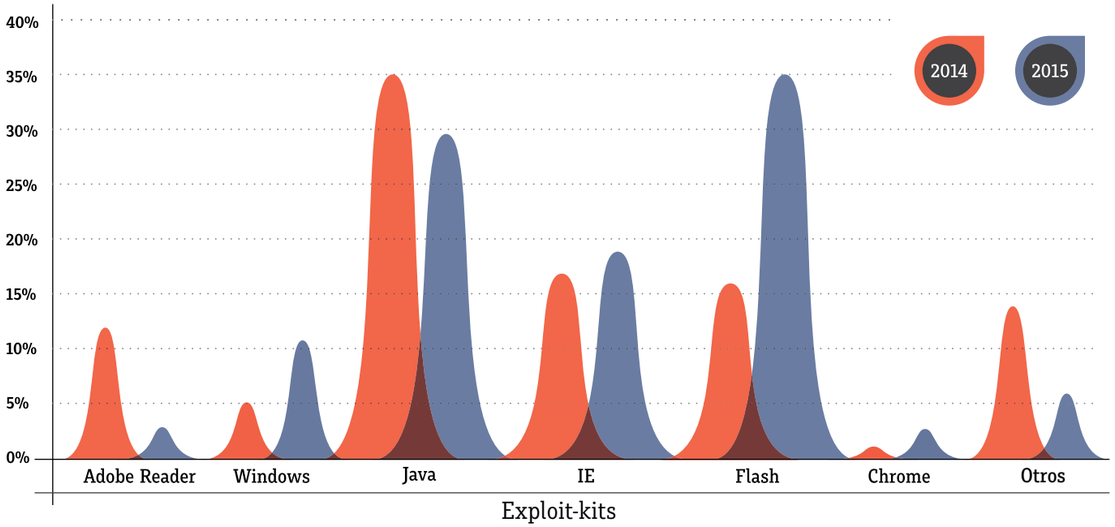
4.1 HERRAMIENTAS CONSTRUIDAS PARA OTROS FINES

Los atacantes están haciendo un uso masivo de herramientas desarrolladas para otros fines, tales como la monitorización de sistemas o la realización de pruebas de penetración. Algunos ejemplos de ello son los servicios SaaS (Software as a Service o booter services), que permiten a los atacantes perpetrar ataques de Denegación de Servicios Distribuidos (DDoS) a través de un sitio web.

Otro ejemplo: los responsables de las campañas de ataque denominadas Cleaver, Hurricane Panda y Anunak/Carbanak utilizaron la herramienta MimiKatz (diseñada originariamente para recuperar contraseñas, tickets Kerberos y funciones resumen (hashes15) de memoria de un sistema Windows) para obtener datos de registro (log) a una red Windows y lograr acceder a los sistemas de la red.

4.2 EXPLOITS, EXPLOIT-KITS Y EXPLOIT DRIVE-BY

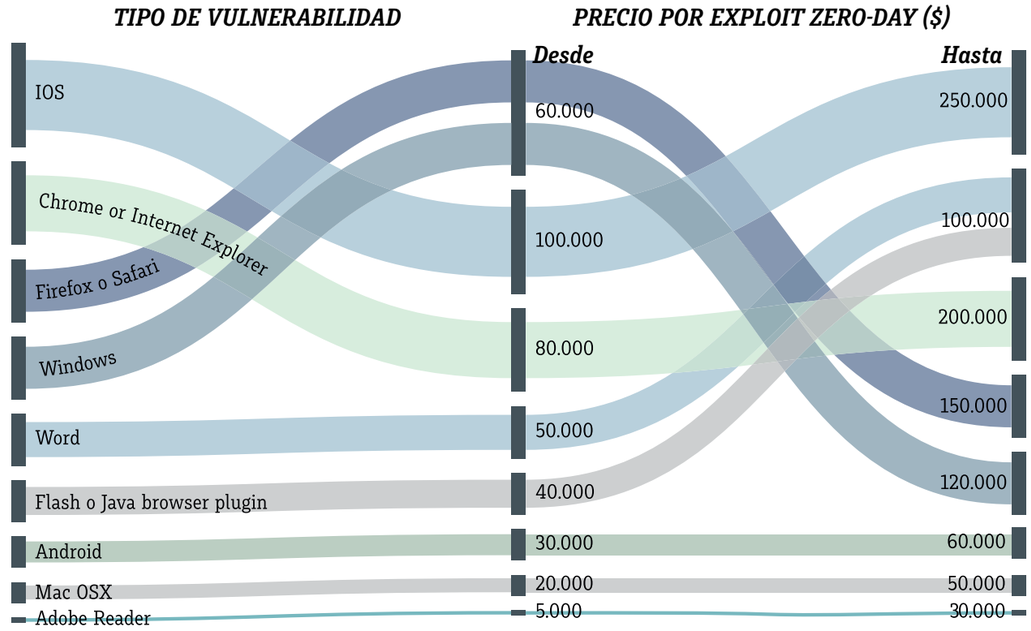
Las herramientas más utilizadas para realizar los ataques (al igual que en los últimos años), son exploits, exploit-kits y exploit Drive-By (permiten infectar el sistema de la víctima con código dañino cuando accede a una determinada página web, distribuyéndose habitualmente mediante banners de publicidad). Windows y las aplicaciones PHP[16] (plug-ins[17] para Wordpress[18] y Joomla, sobre todo) siguen constituyendo el foco de los exploits, aunque es cierto que en 2015 se redujo sustancialmente su publicación. Sin embargo, los exploit-kits más habituales se centran en Adobe Flash, como puede observarse en el gráfico inferior[19]. En el primer semestre de 2015, ocho nuevos exploits (empaquetados en forma de exploit-kits) se dirigieron a explotar vulnerabilidades de este programa. Cinco eran de día-cero.



Estas herramientas no sólo se utilizan en páginas web dudosas, sino también en aquellas otras absolutamente legítimas y fuera de sospecha.

También son muy comunes los ataques por Watering Hole[20] que constituyen un mecanismo habitual para iniciar ataques dirigidos especialmente cuando las páginas web infectadas son de visita frecuente por parte de personas de la organización-víctima.

La figura siguiente nos recuerda el precio de diferentes tipos de exploits-kit, atendiendo a las vulnerabilidades atacadas[21].



EN COMPARACIÓN CON 2014 Y DEBIDO AL USO MASIVO DE EXPLOITS DRIVE-BY Y EXPLOIT-KITS, EL NIVEL DE AMENAZAS SE HA AGRAVADO CONSIDERABLEMENTE.
LAS INVESTIGACIONES MÁS RECIENTES SEÑALAN QUE LOS CIBERATACANTES ESTÁN INVIRTIENDO EN EL DESARROLLO DE NUEVOS EXPLOITS Y EN LA BÚSQUEDA DE NUEVAS VULNERABILIDADES.

[15] La función de hashing criptográfico es una función (matemática) en la cual un algoritmo conocido toma un mensaje de longitud arbitraria como entrada y produce un resultado de longitud fija (generalmente denominado "código hash" o "resumen de mensaje"). CCN-STIC 401 Glosario de Términos

[16] PHP Hypertext Preporcessor es un lenguaje de código abierto muy adecuado para el desarrollo web de contenidos

[17] Un plugin o complemento es una aplicación que se relaciona con otra para aportarle una función nueva y generalmente muy específica. Esta aplicación adicional es ejecutada por la aplicación principal e interactúan por medio de la API (Application Programming Interface. Interfaz de programación de aplicaciones). http://es.wikipedia.org/wiki/Complemento_(informática)

[18] Wordpress y Joomla son sistemas de creación de contenidos para páginas web o Content Management System (CMS)

[19] http://exploit-db.com/

[20] Abrevadero. Estrategia en la que se ataca a un grupo en particular (organización, sector o región) en tres fases: 1. Adivinar/observar los sitios web que el grupo utiliza a menudo. 2. Infectar uno o más de ellos con malware. 3. Infección de alguno de los miembros. Su eficacia se basa en la confianza depositada en las páginas web que se visitan con asiduidad. Es eficaz incluso con grupos concienciados que son resistentes a spear phishing y otras formas de phishing. CCN-STIC 401 Glosario de Términos

[21] McAfee Labs: Threats Report (Aug., 2015)

4.3 CÓDIGO DAÑINO[22] / RANSOMWARE[23] / CRYPTOWARE

Representa una de las herramientas más utilizadas para realizar las infecciones que preceden a los ataques. El número total de versiones de código dañino para PC se estima actualmente en más de **439 millones** (siendo **Windows el sistema más afectado**), al tiempo que el número de malware en plataformas móviles sigue aumentando de manera incesante (**un 96% de este código dañino afecta al sistema operativo Android**).

La variedad de muestras de Ransomware o Cryptoware (Critroni, CryptoFortress, CTB-Locker, Cryptolocker y Cryptowall) no ha dejado de crecer y sus métodos de distribución van variando: exploits drive-by[24] , correos electrónicos con enlaces a programas dañinos, alojamiento en macros de los productos de Microsoft Office, etc. Durante 2015 se han podido constatar infecciones por Cryptoware en multitud de organizaciones, públicas y privadas, de todos los tamaños, incluyendo instituciones sanitarias y pymes. De hecho, la empresa Dell SecureWorks ha informado de que, solamente la variante Cryptowall, infectó a más de 625.000 sistemas informáticos de todo el mundo en tan sólo cinco meses A modo de ejemplo, podemos citar el caso Coinvault, una infección investigada conjuntamente por la Policía Holandesa y Kaspersky Lab, en la que pudo determinarse que, aproximadamente, el 1,5% de las victimas hicieron efectivo el pago del rescate.

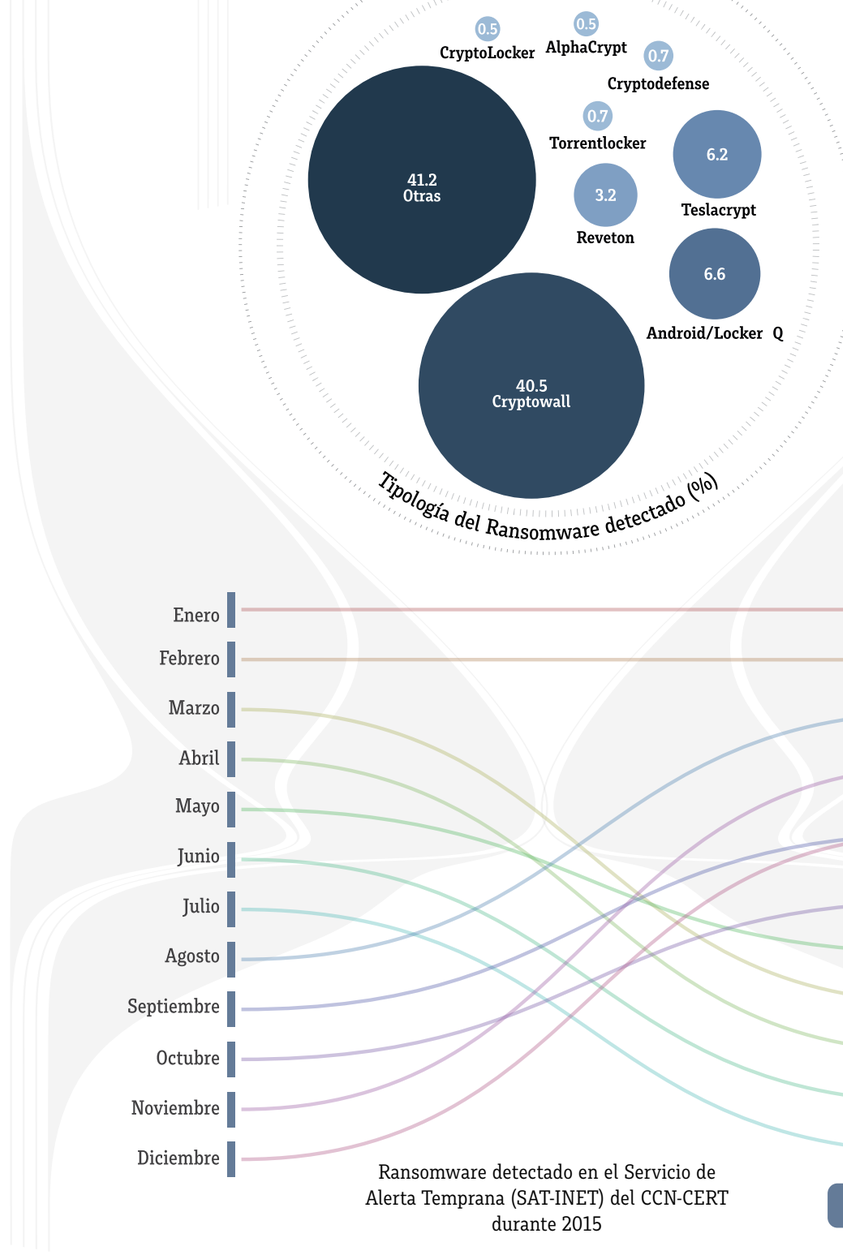
Es lógico que aparezcan nuevas variantes, dado que se calcula que un tanto por ciento de las víctimas satisfizo el rescate, lo que estimula a los delincuentes para mejorar continuamente sus herramientas y sus objetivos: grandes empresas, pymes y consumidores finales; nuevos sistemas operativos y nuevos dispositivos (incluyendo los dispositivos móviles).

Código dañino	Nivel de amenaza	Función primaria	Vector de infección primario	Nominaciones/ Variantes	
Cryptolocker	Alto	Ransomware	Adjunto correo electrónico		▲
DarkComet	Alto	RAT	Exploit Kit	Fynlaski, Fynlos, Kradernok, DarkKornet	▲
Dridex	Alto	Robo de datos	Adjunto correo (macro Word)	Bugat, Feodo, Cridex	▲
Zeus	Alto	Robo de datos	Exploit Kit	Zbot, Garneover (GOZ)	◆
Blackshades	Alto	RAT	Exploit Kit		▲
Citadel	Alto	Robo de datos	Exploit Kit		▲
SpyEye	Alto	Robo de datos	Droper		▲
CTB-Locker	Medio	Ransomware	Adjunto a correo (.zip)	Critroni	▲
Dyre	Medio	Robo de datos	Dropper (Upatre)	Dyreza	▲
Tinba	Medio	Robo de datos	Exploit Kit	Tyrrybanker, Zusy	▲
Carberp	Medio	Robo de datos	Exploit Kit		◆
Shylock	Medio	Robo de datos	Exploit Kit	Caphaw	◆
Ice IX	Medio	Robo de datos	Exploit Kit		▼
Torpig	Medio	Robo de datos	Exploit Kit	Sinowal, Anserin	▼

Tendencia del código dañino en cuanto a peligrosidad (según Europol)

[22] Software que realiza funciones no deseadas, no solicitadas o perjudiciales en un sistema infectado.

[23] Consiste en el secuestro del ordenador (imposibilidad de usarlo) o el cifrado de sus archivos (Cryptoware) y la promesa de liberarlo tras el pago de una cantidad de dinero por el rescate.

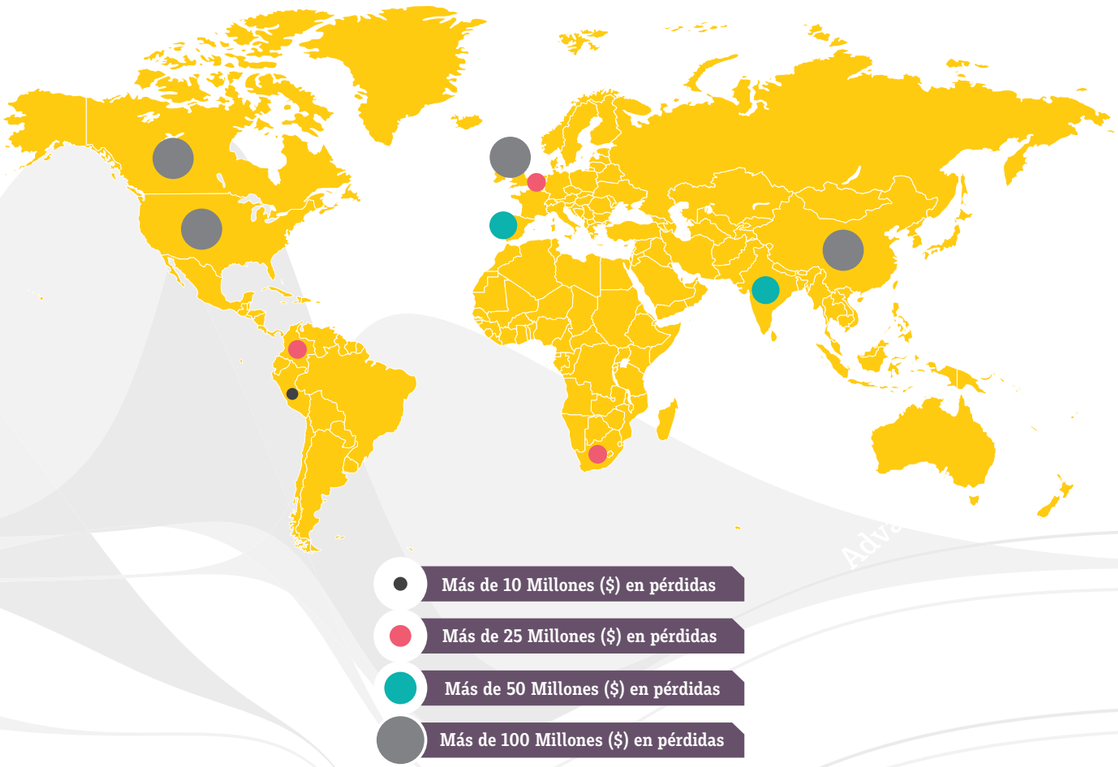


[24] Mecanismos de ataque que permiten infectar el sistema de la víctima con código dañino cuando accede a una determinada página web previamente infectada. El código explota las vulnerabilidades de los navegadores web, sus complementos o el propio sistema operativo

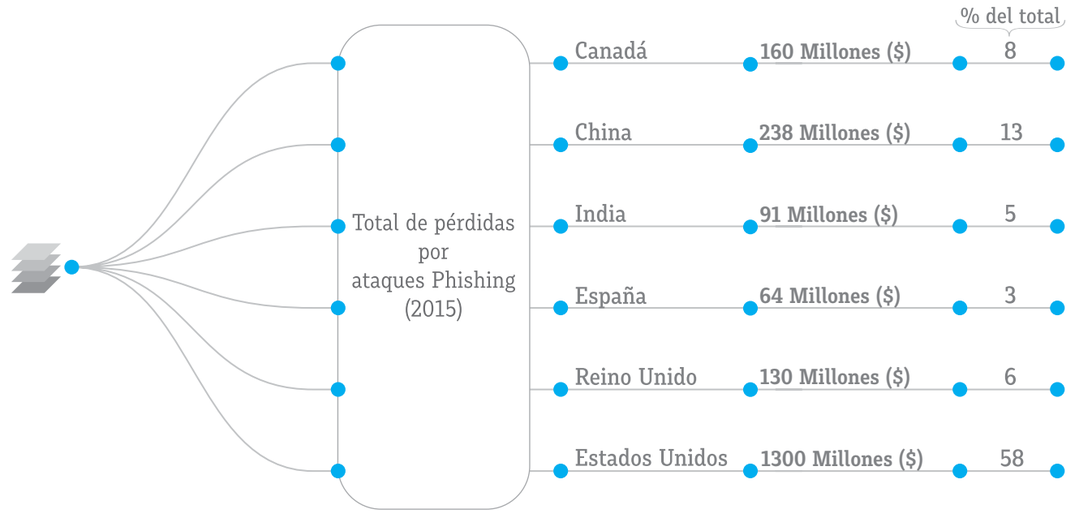
4.4 SPAM (CORREO BASURA) Y PHISHING / SPEARPHISHING

Este término se puede subdividir en varios tipos: spam tradicional, spam de código dañino y mensajes de phishing. Tras un aumento en 2014, el spam tradicional disminuyó en 2015, aproximadamente el 30% del volumen del año anterior. Sin embargo, el que lleva malware, utilizando direcciones de correo electrónico obtenidas en otros sistemas infectados, aumentó significativamente y constituyó la principal la principal fuente de infecciones.
Se encontraron muchas muestras de código dañino de la **familia Geodo.**
Se ha observado, además, **que se distribuyen cada vez más profesionalmente**. La utilización de técnicas de engaño y suplantación, el uso de versiones individuales del código dañino y el control horario de la descarga, son herramientas dirigidas a provocar la infección del sistema del usuario sin que el software anti-virus sea capaz de detectarlo.
En cuanto al phishing y spearphishing (correo dirigido de alguien conocido) son las herramientas más utilizadas para iniciar ataques personalizados (y también los más temidos) y realizar ciberespionaje.

La figura siguiente muestra los países dónde se han producido las mayores pérdidas por efecto del phishing[25].



[25] *Fuente: EMC-RSA http://spain.emc.com/microsites/rsa/phishing/index.htm*



4.5 BOTNETS[26]

Las botnets son utilizadas por los ciberdelincuentes de forma masiva, al objeto de sustraer información, cometer fraude de banca online, atacar a la disponibilidad de los sistemas informáticos o enviar spam. Debido a la profesionalización de los ciberdelitos, operar una botnet es relativamente fácil y poco costoso para los no especialistas. Por ello, el nivel de peligrosidad actual continúa siendo crítico y la tendencia va en aumento.

- En febrero de 2015 se desactivó una botnet especialmente significativa: Ramnit, que había causado aproximadamente 3,2 millones de infecciones en todo el mundo.

- Gracias a su cuota de mercado, **los sistemas principalmente comprometidos por botnets son Windows**, aunque los atacantes están redoblando sus esfuerzos para dirigirse contra sistemas Mac OS X y Android.

- Persiste la tendencia del uso dañino de **servidores web comprometidos** para operar **servidores C&C[27] (Mando y Control)**.

4.6 ATAQUES DDOS

Aunque siguen produciéndose ataques DDoS, los perjuicios que han podido causar han sido cuantitativamente menores que los ocurridos en 2014 y su duración también (la mayoría tienen una duración de entre 30 minutos a una hora). No obstante, el volumen máximo de los ataques está aumentando y acercándose a 400 Gbps, estando el ancho de banda promedio de un ataque DDoS entre 8 y 12 Gbps. Así, por ejemplo, un proveedor de la red india fue alcanzado por un ataque de este tipo con un pico de 334 Gbps. En 2015, algunos sectores que han denunciado novedosos ataques de este tipo han sido las instituciones educativas o los servicios de transportes públicos. No obstante, los preferidos son la industria del juego (35,3% de los ataques) y la industria del software/ tecnología (25,2% de los ataques).
También se tiene evidencia de que se están utilizando servicios **Booter** que permiten perpetrar un ataque sin grandes conocimientos técnicos (DDoS-as-a-Service) y los denominados **ataques por reflexión** donde se utilizan servidores de acceso público para reforzarlo. Esto hace que los operadores de este tipo de servidores se conviertan en coautores (involuntarios) de las acciones dañinas.

[26] *Robot Network"(red de robot o zombies): Red de equipos infectados por un atacante remoto. Los equipos quedan a su merced cuando desee lanzar un ataque masivo, tal como envío de spam o denegación [distribuida] de servicio. CCN-STIC 401 Glosario de Términos*
[27] *Command and Control*

4.7 OFUSCACIÓN

Se denomina ofuscación cualquier actividad llevada a cabo por los atacantes para dejar el menor número posible de trazas de sus acciones, con el objeto de dificultar su identificación, la metodología seguida, etc. Un ejemplo de ello es el uso de servicios legítimos para la distribución de código dañino (hay ejemplos en Dropbox, Pinterest, Reddit, Google Docs. Gmail, etc.).

4.8 INGENIERÍA SOCIAL

Constituye uno de los vectores de ataque preferidos por los agentes de las amenazas, que engañan a sus víctimas, para que permitan la instalación de programas dañinos, y todo ello al objeto de acceder a la información del sistema atacado.

En este caso, los atacantes tienen la posibilidad de obtener de forma rápida y anónima datos personales de sus víctimas a través de las redes sociales y suele constituir la primera fase de los ataques dirigidos (tratando de adivinar la contraseña de la víctima, generando confianza, correos electrónicos personalizados o spearphishing).

El ataque del "falso Presidente" ha sido muy lucrativo en el entorno comercial en 2015 (el atacante se hace pasar por un directivo de la organización, encargando a un empleado la transferencia urgente destinada a un proyecto secreto).

4.9 WATERING HOLE

Suele ser la segunda opción para los atacantes cuando no tiene éxito un ataque mediante spearphishing. Los atacantes, aprovechando una vulnerabilidad conocida e infectan previamente con código dañino una página web que las víctimas visitan frecuentemente.

También se ha incrementado el uso de mensajes publicitarios dañinos (lo que se ha denominado **malvertising**).

4.10 LIBRERÍAS JAVASCRIPT

La inclusión de Javascript y otras librerías en una página web han propiciado en 2015 una importante serie de incidentes. Con frecuencia, los desarrolladores de sitios web invocan directamente una librería en lugar de copiarla a su propio sitio web. Si un atacante logra manipular una librería está en condiciones de atacar a todos los sitios web que contengan una llamada dinámica a la misma.

4.11 LAS MACROS COMO VECTOR DE ATAQUE

Varias familias recientes de software dañino, tales como **Dridex, Vawtrak y Cryptodefense** son claros ejemplos de código dañino que se instala en los sistemas de los usuarios finales a través de macros.

4.12 ROUTERS INALÁMBRICOS

Los routers de particulares y pymes comprometidos permiten, por ejemplo, ajustar la configuración del DNS (Domain Name System) para redirigir el tráfico a páginas web infectadas, formar parte de una botnet, propagar código dañino y penetrar en la red o manipular el tráfico sin ser detectado.

4.13 ROBO DE IDENTIDAD

Habitualmente, el robo de identidad (usuario, contraseña u otros datos) se lleva a cabo mediante mecanismos de ingeniería social, instalación de código dañino en los sistemas de la víctima (incluso existen programas cuya función es precisamente este robo) o a través de ataques previos a sitios web.

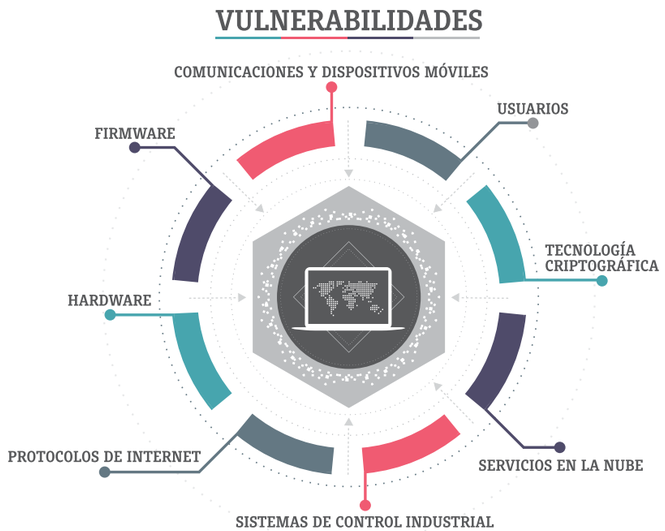
Así pues los atacantes pueden obtener un beneficio económico directo con la venta de identidades robadas y con un margen muy amplio, por lo que, esta actividad se mantendrá como una amenaza permanente en los próximos años.

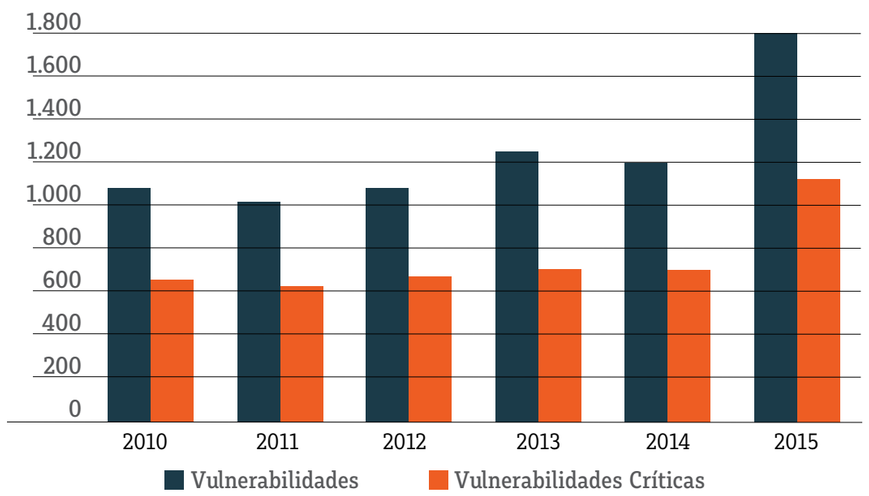


5. RESILIENCIA[28]

5.1 VULNERABILIDADES

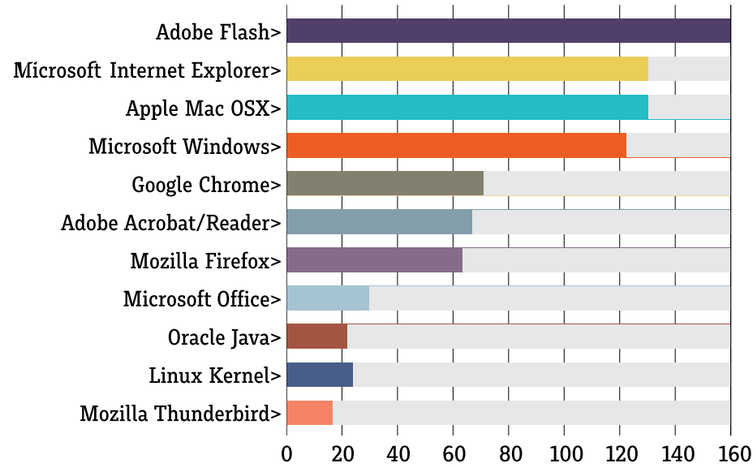
Aunque los usuarios son fuente de vulnerabilidades (el caso del phishing es un buen ejemplo), las de **software** siguen constituyendo el elemento más problemático. Así, **el número de vulnerabilidades críticas** en 2015 en productos TIC estándar **se ha incrementado notablemente** en comparación con las cifras del año anterior.





[28]Capacidad de los sistemas para seguir operando pese a estar sometidos a un ciberataque, aunque sea en un estado degradado o debilitado. Así mismo, incluye la capacidad de restaurar con presteza sus funciones esenciales después de un ataque. CCN-STIC 401 Glosario de Términos

A finales de septiembre de 2015, estaban identificadas **847 vulnerabilidades críticas de los 11 productos de software** de la figura siguiente:



Por su parte, **en 2015, en el portal del CCN-CERT, se publicaron un total de 5.099 vulnerabilidades correspondientes a 10 fabricantes** (Microsoft, Red Hat, Cisco, Oracle, Adobe, Suse Linux, Debian, IBM, Apple y Symantec), frente a las 3.346 de 2014.

Otros tipos de vulnerabilidades detectadas fueron:

- **Firmware**[29]: tras la infección, es casi imposible de detectar el ataque en el propio dispositivo (memorias USB, discos duros, ordenadores, etc.).
- **Hardware**: se requiere acceso físico al equipo para este tipo de ataque. Son muy difíciles de detectar (si no imposible), por ejemplo la manipulación del chip, teclado, USB, etc. La mejor protección sólo puede lograrse mediante la producción de componentes en entornos seguros y su distribución por medio de una cadena de suministro segura.
- **Usuario**: más de la mitad de todos los ciberataques exitosos están relacionados con el usuario (estudio de IBM), siendo el acceso no autorizado el principal.
- **Servicios en la nube:** la conciencia de los propietarios en materia de seguridad TIC sigue siendo deficitaria. Los proveedores no han hecho grandes inversiones en este sentido.
- **Tecnología criptográfica**: Los algoritmos criptográficos actuales pueden considerarse como seguros (aparte de RC4 cuyo uso no se aconseja en TLS[30]). El requisito previo para esto son unas longitudes razonables de parámetros y claves.
- **Protocolos de Internet**: en muchas ocasiones, las vulnerabilidades estructurales de la arquitectura de Internet se basan en decisiones de diseño del pasado con difícil vuelta atrás. El uso de HTTPS[31] ofrece ventajas para todos los tipos de servicios web, evitando la monitorización no deseada del comportamiento de navegación del usuario.
- **Comunicaciones y dispositivos móviles**: representan ciertos riesgos por el rápido desarrollo del software (sin garantías de una correcta actualización de vulnerabilidades), el almacenamiento de la información en la nube, la conexión a accesos públicos sin cifrar (**hotspots**), la geolocalización y la posibilidad de interceptación.

29 Firmware funciona como el nexo de unión entre las instrucciones (software) que llegan al dispositivo desde el exterior y las diversas partes electrónicas (hardware)
30 TLS. Transport Layer Security. Protocolo de cifra que permite el intercambio seguro de información entre dos extremos
31 Secure Hyper Text Transfer Protocol. Protocolo seguro de transferencia de hipertexto, utilizado habitualmente en navegación web.

Del mismo modo, existe un riesgo importante en las **aplicaciones (Apps)** y en el uso profesional del dispositivo privado (BYOD[32]).

- **Sistemas de Control Industrial**: La creciente utilización de componentes TIC estándar hace que estén expuestos a los mismos riesgos que cualquier otra organización. En 2015 se han dado casos, de fallos generalizados en sistemas de producción completos, de ransomware, spyware o spearphishing. Incluso, investigadores norteamericanos utilizaron Internet para penetrar de forma inalámbrica en el sistema de información y entretenimiento de un vehículo todo terreno, a través de una vulnerabilidad.

5.2 MEDIDAS

Este epígrafe examina las medidas que, durante 2015, han contribuido de manera más significativa a aumentar la resiliencia de los sistemas de información sobre los que se aplican y, en su consecuencia, de las organizaciones afectadas.



PERSONALES

- Concienciación y la mejora de la competencia de los usuarios
- Cualificación del profesional de la ciberseguridad
- Divulgación responsable de vulnerabilidades
- Cooperación entre los diferentes actores

TÉCNOLÓGICAS

- Autenticación de dos factores
- Uso de la criptografía: protocolos TLS y DNSSEC[33]
- Incremento de la capacidad de detección
- Adecuación a las medidas de seguridad establecidas en el Esquema Nacional de Seguridad (ENS)[34] especialmente para las Administraciones Públicas.
- Despliegue eficiente de las capacidades, incluyendo herramientas de intercambio de ciberamenazas como REYES desarrollada por el CCN-CERT.
- Ejercicios de ciberseguridad

REGULATORIAS

- Armonización de la legislación europea
- Instrumentos jurídicos que permitan el uso en remoto de métodos de investigación
- Aplicación de la Directiva Europea sobre ataques contra los sistemas de información

[32] BYOD. Bring your own device
[33] DNSSEC.Domain Name System (DNS) Security Extensions. Constituye una forma de seguridad criptográfica para el protocolo DNS
[34] RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

- DECÁLOGO DE CIBERSEGURIDAD -

01 **Aumentar la capacidad de vigilancia de las redes y los sistemas.**
Es indispensable contar con el adecuado equipo de ciberseguridad.

02 **Monitorización y correlación de eventos.**
Uso de herramientas capaces de monitorizar el tráfico de red, usuarios remotos, contraseñas de administración, etc.

03 **Política de Seguridad Corporativa restrictiva.**
Adecuación progresiva de los permisos de usuario, servicios en la "nube" y la utilización de dispositivos y equipos propiedad del usuario (BYOD).

04 **Configuraciones de seguridad en todos los componentes de la red corporativa.**
Se incluirán los equipos móviles y portátiles.

05 **Uso de productos, equipos y servicios confiables y certificados.**
Redes y sistemas acreditados para información sensible o clasificada

06 **Automatizar e incrementar el intercambio de información.**
Reciprocidad con otras organizaciones y Equipos de Respuesta a Incidentes de Seguridad de la Información (CERTs).

07 **Compromiso de la Dirección con la ciberseguridad.**
Los cargos directivos deben ser los primeros en aceptar que existen riesgos y promover las políticas de seguridad.

08 **Formación y la Sensibilización de usuarios (eslabón más débil de la cadena).**
Todos y cada uno de los niveles de la organización (dirección, gestión e implantación) deben ser conscientes de los riesgos y actuar en consecuencia

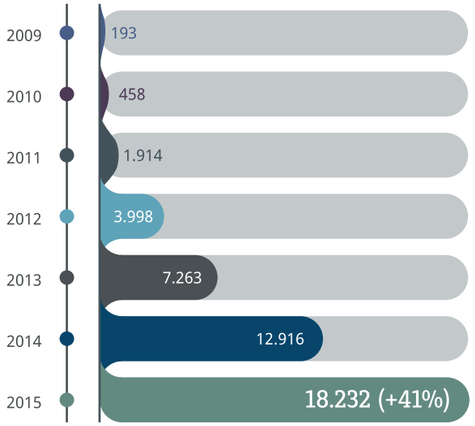
09 **Atenerse a la legislación y buenas prácticas.**
Adecuación a los distintos estándares (en el caso de las Administraciones Públicas al Esquema Nacional de Seguridad –ENS-).

10 **Trabajar como si se estuviese comprometido.**
Suponer que los sistemas están ya comprometidos o lo estarán pronto y proteger los activos fundamentales.

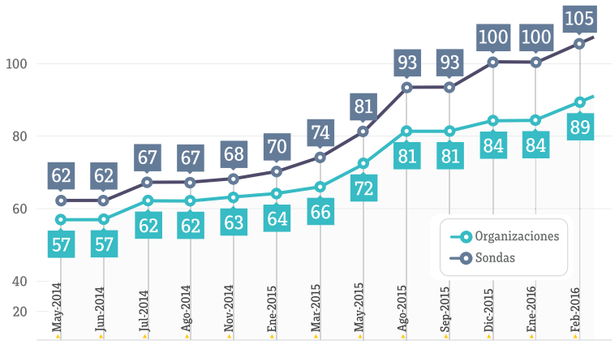
6. ACTIVIDAD DEL CCN

6.1 GESTIÓN DE INCIDENTES EN 2015

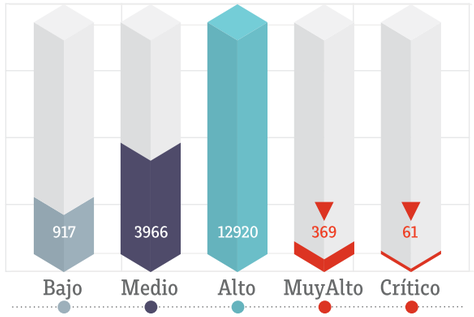
El CCN-CERT gestionó durante 2015 un total de **18.232 incidentes** detectados en las Administraciones Públicas y en empresas de interés estratégico. Esta cifra representa **un incremento del 41,45%** con respecto al año 2014.



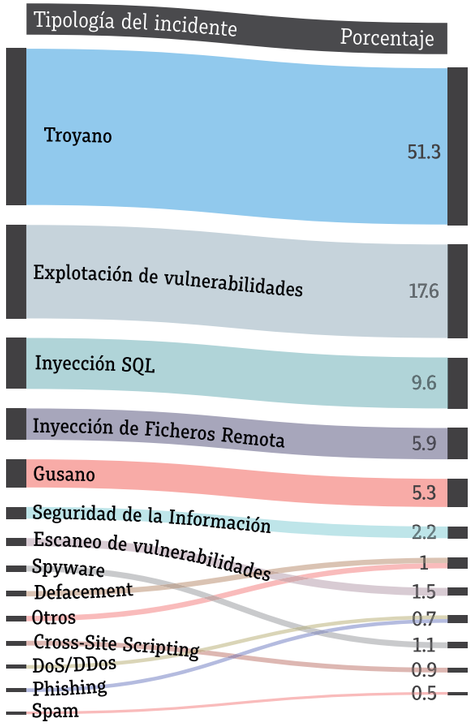
Evolución de los Incidentes gestionados por el CCN-CERT



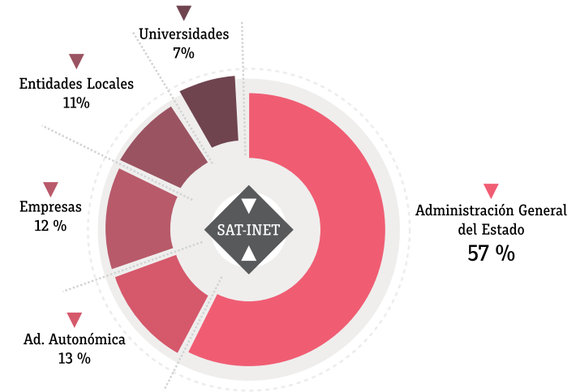
Organizaciones adscritas al Sistema de Alerta Temprana en Internet del CCN-CERT (y las sondas instaladas)

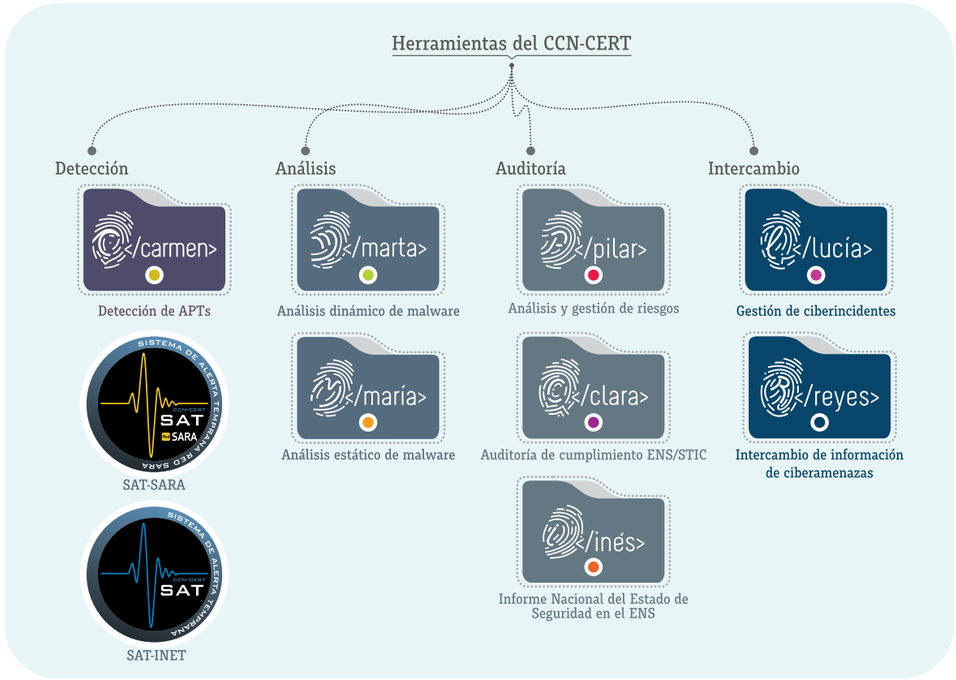


Del total de incidentes, **430** fueron catalogados por el equipo de expertos del CERT Gubernamental Nacional con un nivel de riesgo **muy alto o crítico**; es decir, se tuvo constancia de que los ataques afectaron a los sistemas de la organización y a su información sensible. La figura siguiente muestra la distribución de los ataques gestionados, en función de su peligrosidad.



Distribución de las 89 organizaciones adscritas al Sistema de Alerta Temprana de Internet (SAT-INET)





ESQUEMA DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN

CERTIFICACIÓN CRIPTOLÓGICA

Productos capaces de proteger la información

13 Expedientes abiertos de producto de cifra.

CERTIFICACIÓN FUNCIONAL

En base a criterios establecidos y reconocidos como estándar internacional

27 Expedientes abiertos de producto de TIC

3 Expedientes de acreditación de laboratorios

CERTIFICACIÓN TEMPEST

Equipos protegidos frente a las emanaciones

146 Expedientes abiertos para la certificación TEMPEST de locales, equipos y plataformas móviles

Proyectos de certificación en los que ha trabajado el Organismo de Certificación en 2015

7. TENDENCIAS

A continuación se resumen las tendencias que presumiblemente se esperan en 2016 y en años venideros.

Respecto de...	es de esperar que...	
El número de atacantes (estados o delincuentes profesionales) con capacidad para desarrollar ciberataques...	... aumente.	↑↑
Debido al número limitado de desarrolladores de software de calidad...	... el denominado "Cybercrime-As-A-Service" se incremente, reduciendo las barreras de entrada para los ciberdelincuentes.	↑
La sofisticación de los adversarios...	... se desarrolle, por lo que la detección y la respuesta serán más difíciles.	↑
El spear-phishing...	... siga siendo muy utilizado por los atacantes, así como el aumento de las infecciones por Watering Hole	↔
El Ransomware/Cryptoware...	... continúe siendo una amenaza de las de mayor importancia.	↑
Los adversarios con altas capacidades técnicas...	... suban en número, así como el volumen de incidentes. No se prevé incremento sustancial en las capacidades técnicas	↔
Las desfiguraciones de páginas web y secuestro de medios de comunicación social...	... se incremente.	↑

7.1 CIBERESPIONAJE

7.1.1 ATAQUES DE LOS ESTADOS Y LA CIBERGUERRA

Los estados seguirán reforzando sus cibercapacidades (defensivas y ofensivas) buscando una mayor seguridad en sus operaciones, lo que dificultará la detección de las campañas. Al tiempo mejorarán la capacidad de obtención de información (ciberespionaje), perfeccionando sus métodos de tratamiento y ampliando día a día el concepto de ciberguerra y las reglas de la participación en la misma.
De hecho, las competencias en ciberguerra forman ya parte del arsenal político internacional, compuesto por los sistemas ofensivos y defensivos.

7.1.2 DIFICULTAD EN LA DETECCIÓN

La capacidad de los atacantes para sortear los sistemas de seguridad y evitar ser detectados irá en aumento. Experimentarán con infecciones que no requieren del uso de un archivo. Gracias a las vulnerabilidades en la BIOS[35], los controladores y otro firmware, evadirán las defensas inyectando comandos en la memoria o manipulando funciones para introducir una infección o filtrar datos.
También se producirá el secuestro de protocolos de control remoto o shell remoto, como VNC[36] RDP(Remote Desktop Protocol), WMI (Windows Mangement Instrumentation) y PowerShell[37] , con el que los agresores tendrán el control directo sobre los sistemas y la instalación de código dañino de forma transparente a las herramientas de seguridad.

7.1.3 ATAQUES MÁS PACIENTES

Seguirán registrándose ataques capaces de permanecer inactivos durante varios meses antes de conseguir sortear los entornos aislados o las infecciones que recopilan datos sigilosamente sin interferir con el usuario. También, mecanismos de infiltración ocultos en protocolos normalmente cifrados, como HTTPS. Otra técnica que seguirá presente es la del señuelo: un código dañino o una botnet que atrae la atención del equipo de seguridad, mientras que el verdadero ataque se infiltra sigilosamente por otro lugar, sin ser observado.

7.1.4 ¿GHOSTWARE? ¿CÓDIGO DAÑINO FANTASMA?

A medida que los atacantes se convierten en el foco de atención de los investigadores, fuerzas policiales y de la justicia, desarrollarán una nueva variante de código dañino diseñado para cumplir con su misión y borrar todas las huellas, antes de que las medidas de seguridad pueden detectarles.
Es presumible que 2016 dé las primeras evidencias de este **Ghostware**, desarrollado para robar datos... y desaparecer sin dejar rastro.

7.1.5 MALWARE DE DOS CARAS

Como quiera que las medidas de seguridad han evolucionado (entre ellas, las sandbox o zona de prueba), no es descartable que, en los próximos años veamos el surgimiento de un nuevo código dañino que, tras ejecutar una tarea inocente, y pasar el filtro de las pruebas, ejecuta seguidamente el proceso dañino, una vez que ha despejado los protocolos de seguridad.

7.1.6 MAYOR INTERVENCIÓN DE LOS GOBIERNOS

Por otro lado existe una corriente en todo el mundo para involucrarse más en la legislación de Internet, lo que tendrá un gran impacto sobre la seguridad de las organizaciones, así como de la red en su totalidad.

7.2 CIBERDELINCUENCIA

7.2.1 EVOLUCIÓN

La mayoría de las acciones de los ciberdelincuentes tienen por objeto obtener dinero, persiguiendo aquello que tiene valor. Por ese motivo, el incremento en el valor de los datos personales será determinante, y seguirá creciendo.
Además, los ciberataques serán más accesibles a usuarios sin grandes conocimientos técnicos, lo que permitirá o favorecerá la aparición de objetivos más personales, como el descrédito o el falso testimonio, los ataques contra la integridad, el acoso o el vandalismo.

7.2.2 LA EXTORSIÓN DDOS SERÁ CADA VEZ MÁS COMÚN

Grupos como **DD4BC o Armada Collective**, especializados en enviar correos pidiendo el pago de un rescate y amenazando con colapsar un sitio web, han confirmado el éxito de esta técnica. Esta amenaza continuará (y empeorará) en 2016, toda vez que cada vez más criminales ven los beneficios potenciales de la extorsión DDoS.

7.3 OTRAS TENDENCIAS TÉCNICAS

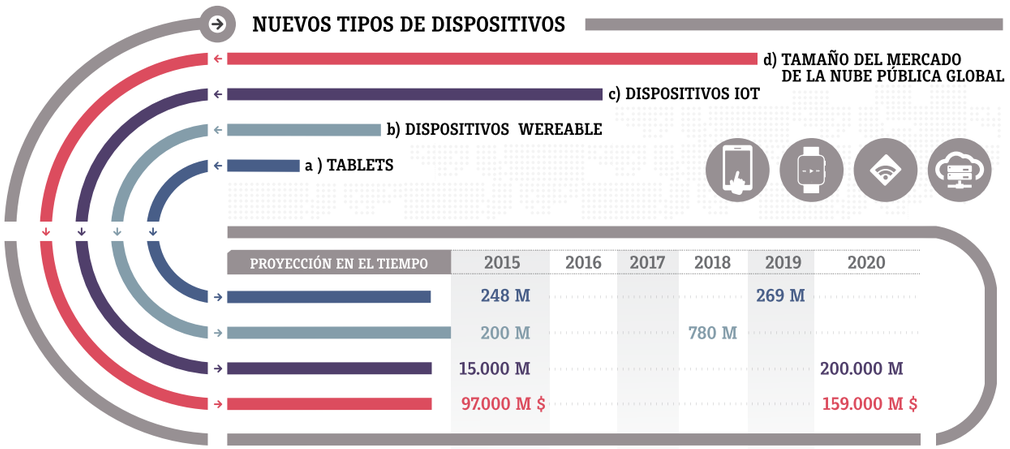
7.3.1 SEGURIDAD DEL HARDWARE

Se prevé la aparición de muchos grupos que, empleando nuevas técnicas, desarrollarán ataques singularmente efectivos contra las vulnerabilidades del hardware o firmware. En paralelo surgirán mecanismos de protección como el arranque seguro, los entornos de ejecución de confianza, la protección contra manipulaciones, la aceleración de la criptografía, la protección de memoria activa y la identidad de dispositivos, pondrán las cosas más dificiles a los atacantes.

[35] Basic Input and Output System
[36] VNC. (Virtual Network Computer) Computación Virtual en Red es un programa de código libre basado en estructura cliente-servidor que permite tomar el control del ordenador servidor remotamente a través de un ordenador cliente https://wikipedia.org/wiki/VNC
[37] Powershell. Es un interfaz de consola con posibilidad de escritura y unión de comandos por medio de instrucciones (scripts en inglés) https://wikipedia.org/wiki/Powershell

7.3.2 ATAQUES AL INTERNET DE LAS COSAS

El incremento del denominado Internet de las Cosas (IoT) y de sus usuarios seguirá atrayendo el interés de los ciberdelincuentes. No sólo de los dispositivos (teléfonos, tabletas, TV, wearables[38] , luces, coches, electrodomésticos) de los que se puede extraer una cantidad ingente de información, sino también de los servicios que están detrás conectados a una central en la nube.



Evolución del volúmen nuevos dispositivos[39]

7.3.3 LA VIRTUALIZACIÓN Y EL ACCESO A LA NUBE

La virtualización presenta ventajas e inconvenientes: aísla y protege los servidores virtuales y las aplicaciones pero dificulta la detección de los desplazamientos laterales. En los próximos años se generalizará **la tecnología SDN** (Software Defined Networking) o **redes definidas por software**, y no solo en entornos de centros de datos y de la nube. Se utilizará junto con la tecnología NFV[40] para crear variedades de servicios bajo demanda, en formatos adaptables y automatizados. El riesgo será una mayor superficie de ataque y puntos únicos de fallo.

7.3.4 SEGURIDAD Y PRIVACIDAD

En los próximos años, el volumen y los datos personales que se recopilarán abarcará todo tipo de información personal: nombre, dirección, número de teléfono, correo electrónico, historial de compras, sitios más visitados, comportamientos cotidianos (lo que comemos, vemos y escuchamos), nuestro peso, presión sanguínea, medicación, hábitos de sueño o el ejercicio que hacemos. Los sensores proporcionarán esta información a organizaciones, que a su vez nos enviarán publicidad, recomendaciones y ofertas adecuadas a nuestros intereses. Esta "huella digital" tendrá un enorme valor económico, por lo que se impondrá la necesidad de protegerla, controlarla y, lógicamente, habrá quien intente hacerse con estos datos de manera "legítima" (acuerdos consentidos) o por medios ilícitos. Mediante técnicas analíticas que se utilizan en el mundo Big Data, estos delincuentes buscarán vínculos y correlaciones en las identidades personales y venderán la información al mejor postor.

[38] Wearables (ponible o usable o complementos inteligentes). Es un dispositivo que se lleva sobre, debajo o incluido en la ropa y que está siempre encendido permitiendo la multitarea. https://wikipedia.org/wiki/Wearable

[39] Fuente: McAfee Labs, 2015.

[40] NFV Network Functions Virtualization. Virtualización de las Funciones de Red, consiste en virtualizar componentes esenciales de red, como cortafuegos, enrutadores, conmutadores, almacenamiento, balanceadores de carga etc. de manera que no es necesario tener los equipos físicos, y se puedan realizar las mismas funciones, desplegando los servicios de red basados en software que pueden alojarse en servidores de forma centralizada o distribuida. NFV básicamente es la tecnología "cloud" (nube) del mundo de las IIC aplicada al mundo de los operadores de telecomunicaciones y proveedores de servicios. https://wikipedia.org/wiki/NFV

ANEXO B:

DISPOSITIVOS Y COMUNICACIONES MÓVILES

El Informe CCN-CERT IA-09-16 incluye tres grandes anexos que completan el panorama general de la Ciberseguridad en 2015. En el primero (Anexo A) se recoge la actividad más destacada del Centro Criptológico Nacional (véase páginas centrales); en el segundo (Anexo B), Dispositivos y comunicaciones móviles y, en el tercero (Anexo C), el Hacktimismo en 2015.

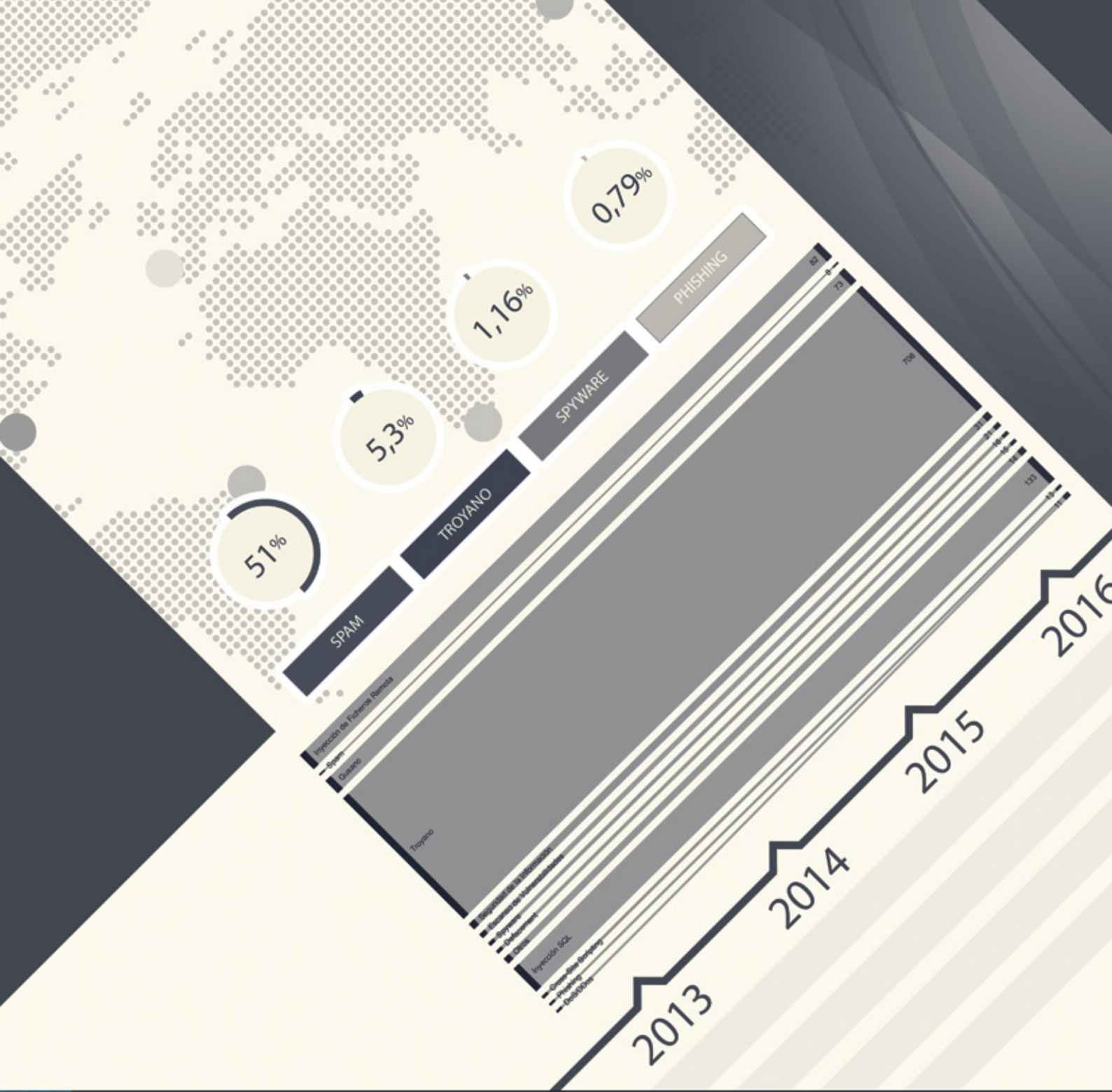
En el caso de los dispositivos y comunicaciones móviles, se hace un balance de la situación actual, las ciberamenazas que se ciernen sobre ellos, el malware para iOS, el modelo de permisos en Android y las vulnerabilidades más importantes destacadas.

Así, las tecnologías móviles se sitúan como una de las áreas principales en el panorama emergente de amenazas de seguridad, y en concreto, debido a su estrecha relación con el Internet de la Cosas y por los riesgos asociados a la pérdida o robo de los dispositivos. De igual modo, se calcula que existen más de **9 millones de muestras** de código dañino para móvil, con un **aumento del 50% con respecto al año anterior** (el 95% dirigido a Android) y el ransomware se constituyó como el malware más prevalente para Android. De entre ellos, destacan: **Locker** (engaña al usuario para hacerle creer que está instalando una actualización de software no dañina), Porn Droid, o **Lockerpin**, distribuido a través de sitios web para adultos, modifica el código de acceso del dispositivo para forzar al usuario a pagar el rescate.

El incidente de **Hacking Team** (una compañía que comercia con vulnerabilidades y exploits no públicos y que trabaja con agencias gubernamentales) confirmó las capacidades de sus desarrollos, tanto para dispositivos móviles Android como iOS. De hecho, se usaron once apps (WhatsApp, Twitter, Facebook, Facebook Messenger, WeChat, Google Chrome, Viber, Blackberry Messenger, Skype, Telegram y VK) para distribuir malware.

Se espera un incremento de los denominados **Potentially Unwanted Software** o **PUS**, es decir, apps que espían las actividades y datos del usuario, o el ataque a sistemas de pago, cada vez más utilizados a través del móvil, y el malware bancario, que seguirá profesionalizándose y cuyo principal objetivo es obtener las credenciales del usuario al acceder a la banca online a través del móvil, como por ejemplo **SlemBunk**.





CCN-CERT
centro criptológico nacional

WWW.CCN-CERT.CNI.ES
WWW.CCN.CNI.ES
WWW.OC.CCN.CNI.ES