# CIBERSEGURIDAD:
# **TENDENCIAS 2017**

Investigación VIU

viu | Universidad Internacional de Valencia

**Autores**

Prof. Manel Medina
(catedrático esCERT-UPC, director máster en gestión de la ciberseguridad)

Mercè Molist
(periodista de divulgación de ciberseguridad)

**Fecha**

Febrero 2017

# 1. RESUMEN EJECUTIVO

En 2016 hemos vivido un crecimiento extraordinario de cinco tipos de ataques:

1. Ataques de denegación de servicio distribuidos (DDoS) usando dispositivos domésticos conectados a internet (IoT), aprovechando que los usuarios los conectan sin actualizar las contraseñas de fábrica.

2. Ataques de secuestro de ficheros en discos duros y dispositivos móviles, pidiendo un rescate por recuperarlos crecieron un 800% en 2016. Normalmente se infecta el ordenador mediante un email contaminado con malware. Han generado ataques con un ancho de banda de más de 1Tbps (1.000Gbps).

3. Fraude del CEO (Director ejecutivo), en el que se suplanta su identidad en correos electrónicos para engañar a alguna persona de la empresa para que haga una transferencia a una cuenta del atacante con engaños de ingeniería social. Ha provocado estafas/robos de 600.000€ por término medio en los ataques publicados, que son solo del orden del 15% de los que se producen. En 2015 provocaron pérdidas de 2 o 3 miles de millones de dólares en todo el mundo (según las fuentes).

4. Las webs desde las que se hace Phishing crecieron un 25% durante 2016, con puntas de crecimiento del 100% en primavera. Un 30% de los usuarios abren los mensajes de phishing y un 12% clica en la URL "sin pensar".

5. El robo de datos personales (denunciados) ha batido cifras récord de número de usuarios afectados: Voter Database 191M, Friend Finder Network, 412M, MySpace 164M, Dailymotion 85M, Anthem 80M, Weebly 43M. Con un coste medio de unos 4M€ por incidente o unos 150 €/registro robado, que puede ser mayor si impacta en el valor de las acciones en bolsa.

Estos hechos nos enseñan que debemos invertir y esforzarnos en conseguir que TODOS:

a) Actualicemos las credenciales de los dispositivos IoT y que los fabricantes lo faciliten.

b) Comprobar muy bien los remitentes de los emails, y preguntar antes de abrirlos en caso de la más mínima sospecha.

c) Desconfiar de comunicaciones de nuestros compañeros o amigos que nos llegan por conductos nuevos y pedir confirmación siempre por otro canal.

d) Proteger el acceso a nuestros perfiles de redes sociales y email con autenticación de doble factor.

e) Proteger la privacidad de usuarios y clientes con sistemas de autenticación en la sombra, identificando comportamientos anormales o sospechosos.

f) Aprender a identificar los ataques y comportamientos sospechosos, a proteger nuestros equipos y las personas que nos rodean de estos ciberataques. En definitiva, formarnos en ciberseguridad para sobrevivir en el ciberespacio.

# 2. INTRODUCCIÓN

## 2.1. PANORAMA DE LA CIBERSEGURIDAD DURANTE 2016 EN LATINO-AMÉRICA

El informe del Banco Interamericano de Desarrollo (BID) y la Organización de Estados Americanos (OEA), que lleva por título: "Ciberseguridad 2016, ¿Estamos preparados en América Latina y el Caribe?"[1], asegura que sólo 6 países en Latinoamérica y el Caribe tienen planes de seguridad cibernética, un dato muy preocupante.

Brasil, Jamaica, Uruguay, Panamá, Trinidad y Tobago, Colombia y Panamá tienen medidas contra amenazas de ciberseguridad, mientras que, en el caso de México, Perú, Bahamas, Argentina, Antigua y Barbuda, Costa Rica, Bahamas, El Salvador, Haití, Surinam y República Dominicana, están todavía en proceso de adoptar medidas más potentes en materia de ciberseguridad. Los países en el mundo más avanzados en materia de ciberseguridad son, en la actualidad, Estados Unidos, Estonia, Israel y Corea.

El informe sobre Ciberseguridad[2] constata que cuatro de cada cinco países de la zona no presentan estrategias en materia de ciberseguridad, como planes de seguridad online y de protección de las infraestructuras críticas, dos de cada tres países no tienen ningún centro de comando y control de seguridad cibernética y la gran mayoría de ministerios carece actualmente de capacidad para hacer frente a los delitos cibernéticos, entre otras vulnerabilidades.

Los datos recogidos[3] fueron analizados mediante el uso de los 49 indicadores del modelo de madurez de la capacidad de seguridad cibernética desarrollado por el GCSCC (Global Cyber Security Capacity Centre de Oxford), que se divide en cinco dimensiones: 1) Política; 2) Sociedad; 3) Educación; 4) Legislación; y 5) Tecnología. Hay cinco niveles de madurez para cada indicador: 1) Inicial; 2) Formativo; 3) Establecido; 4) Estratégico; y 5) Dinámico.

Finalmente, es interesante citar el informe de la Unión de Telecomunicación Internacional: ITU Global[4], en el que se analizan las políticas de ciberseguridad aplicadas en la mayoría de países del mundo.

## 2.2 RETOS MÁS IMPORTANTES EN LA CIBERSEGURIDAD DURANTE 2016

La mayoría de informes publicados sobre los incidentes más destacables[5] y las tendencias de ciber-ataques ocurridos durante 2016 coinciden en apuntar hacia 3 familias de ataques como los más destacables, por su volumen, crecimiento o impacto económico:

- Malware en general, pero especialmente aquél que afecta a la seguridad de Internet de las cosas (IoT)

- Los ataques de Phishing en varias formas, especialmente aquellos que atentan a la Identidad digital

- Los ataques a la Accesibilidad a los datos y la información, en dos manifestaciones importantes: ataques de denegación de servicio distribuidos (DDoS) y secuestro de discos y bases de datos pidiendo rescate para recuperarlos (ransomware).

1 https://publications.iadb.org/handle/11319/7449?locale-attribute=es&

2 http://www.iadb.org/es/noticias/anuncios/2016-03-11/informe-ciberseguridad-en-america-latina-y-el-caribe,11422.htmlhttp://www.ciberseguridadparaempresas.com/ciberseguridad-en-latinoamerica-asignatura-pendiente/

http://acis.org.co/portal/content/level-3-presenta-informe-de-amenazas-y-ataques-en-toda-am%C3%A9rica-latina

3 https://mydata.iadb.org/Reform-Modernization-of-the-State/2016-Cybersecurity-Report-Data-Set/cd6z-sjjchttp://ceiuc.cl/Recomendados/informe-ciberseguridad-iestamos-preparados-en-america-latina-y-el-caribe

4 http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdfhttps://www.itu.int/en/ITU-D/Cybersecurity/Documents/Index_of_Indices_GCI.pdfhttp://www.itu.int/pub/D-STR-SECU-2015

http://www.itu.int/pub/D-STR-SECU-2015

http://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf

5 http://gestion.pe/tecnologia/tres-ciberdelitos-que-amenazan-seguridad-empresas-2168337http://www.efe.com/efe/america/tecnologia/el-secuestro-de-datos-crece-en-america-latina-con-brasil-mexico-y-peru-a-la-cabeza/20000036-2931752

# 3. PROTECCIÓN DE DISPOSITIVOS CONECTADOS A INTERNET

## 3.1. MALWARE

El malware sigue sin ser desbancado como rey de las amenazas en ciberseguridad. En 2016 se detectaron casi 760 millones de ataques de malware y el 31,9% de ordenadores personales conectados a Internet sufrieron al menos un intento de infección vía web el año pasado. China, Turquía, Taiwan, Ecuador y Guatemala son los países con mayores ratios de infección del mundo[6]. La situación no va camino de mejorar sino todo lo contrario: de expandirse hacia nuevos territorios, como la Internet de las Cosas (IoT).

| Ranking | Country | Infection Rate |
|---|---|---|
| 1 | China | 47.23% |
| 2 | Taiwan | 43.38% |
| 3 | Turkey | 39.01% |
| 4 | Russia | 37.86% |
| 5 | Ecuador | 37.21% |
| 6 | Guatemala | 36.55% |
| 7 | Peru | 36.01% |
| 8 | Mexico | 35.79% |
| 9 | Brazil | 33.88% |
| 10 | Venezuela | 32.31% |

Cada trimestre de 2016 hemos visto nacer 600 millones de nuevas muestras de malware[7]. Las más importantes novedades de este año ha sido:

a) el ransomware, con un crecimiento del 162%,
b) el código malicioso dirigido al robo de información y
c) el malware móvil, con un crecimiento del 150% respecto a 2015 y altos ratios de infección en Brasil, Indonesia, Filipinas y México.[8]

6 http://docs.apwg.org/reports/apwg_trends_report_q3_2016.pdf

7 http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-sep-2016.pdf

8 https://blog.malwarebytes.com/malwarebytes-news/2017/02/2016-state-of-malware-report

El ámbito móvil ha visto la aparición de entre 9 y 10 millones de nuevos especímenes durante 2016. Las infecciones en iOS han aumentado, pero en general tener un teléfono Android sigue siendo más arriesgado, concretamente tres veces más arriesgado a la hora de sufrir una infección, dado que el malware para este tipo de teléfonos se ha cuadruplicado.[9]

Las principales amenazas en telefonía en 2016 han sido los troyanos capaces de conseguir derechos de superusuario, de forma que podían hacer todo lo que quisieran en el dispositivo Android infectado. Esto incluye esconderse en la carpeta de sistema, hacerse prácticamente imposibles de borrar e instalar y activar diferentes aplicaciones que mostraban anuncios de forma agresiva. Incluso podían comprar nuevas apps en Google Play.[10]

La mayoría de estos troyanos se distribuían a través de la Google Play Store. Algunos tuvieron 100.000 descargas y uno en concreto, una Guía de Pokemon infectada, se instaló más de 500.000 veces. De todas formas, cabe aclarar que en las redes móviles la ratio de infección es 20 veces menor que en las redes residenciales. Los troyanos bancarios siguen siendo los reyes de los troyanos y 2016 ha visto cómo se trasladaban de la web a las aplicaciones móviles, siguiendo la estela de sus víctimas. A mediados de 2016 ya superaban los números de dispositivos atacados de 2014 y 2015 juntos. La banca móvil, básicamente operando Android, fue la responsable de este incremento, un 46% mayor que en 2015, que representa casi 3 millones de dispositivos.

El troyano bancario estrella de 2016 ha sido Svpeng, que ataca dispositivos Android. El acierto de este malware es su forma de difusión, a través de la red de anuncios de Google AdSense, muy usada en portales web, sitios de noticias y otros. El malware se instala en el dispositivo de la víctima cuando ésta ve el anuncio malicioso, sin necesidad de pinchar en él. Los países con más ataques de troyanos bancarios han sido Rusia, Brasil, Turquía, Sri Lanka y Paquistán.

El malware ha vivido también un incremento en su uso para el fraude de anuncios: ordenadores infectados visitan sitios web y pinchan en anuncios sin que su propietario se dé cuenta, provocando miles de millones en pérdidas para los anunciantes.

Las principales vías de infección de malware en 2016 han sido los documentos adjuntos y los enlaces maliciosos en el correo electrónico, así como los sitios web. Se detectaron más de 260 millones de URLs maliciosas que contenían exploits[11] y otros programas maliciosos, enlaces a otras páginas con exploits, centros de control de botnets[12], páginas extorsionadoras, etc.

Los programas maliciosos más abundantes en 2016 han sido los troyanos, los programas no solicitados (PUPs), "droppers" (programas que instalan malware), "ransomware", programas de Comando y Control, "keyloggers" (capturadores de pulsaciones de teclado), puertas traseras, divulgadores de información, malware para ataques de Denegación de Servicio Distribuida (DDoS) y troyanos de acceso remoto, más conocidos por las siglas RAT.

Desde el punto de vista del malware en circulación, el 60% han sido troyanos, el 16%, virus; el 11%, gusanos; el 4%, programas no solicitados y el 2% adware (programa malicioso para introducir publicidad) y spyware. Las cifras varían un poco si lo que tenemos en cuenta es la causa de la infección: 66% han sido causadas por troyanos, 2% por virus, 3% gusanos, 4% adware y spyware y 25% programas no deseados.

Una de las causas más importantes del crecimiento contínuo del malware es la proliferación en el mercado negro de las ofertas del llamado "malware-como-servicio". Estas infraestructuras consisten en diversos módulos masivos, como botnets, kits de exploits, configuradores de malware, código malicioso, etc. Los clientes pueden alquilarlos por unas decenas de euros al día, para montar ataques de, por ejemplo, ransomware, en los que pueden conseguir beneficios mensuales de 100.000 euros.

9 https://www.skycure.com/wp-content/uploads/2016/06/Skycure-Q1-2016-MobileThreatIntelligenceReport.pdf

10 https://securelist.com/analysis/kaspersky-security-bulletin/76858/kaspersky-security-bulletin-2016-executive-summary

11 Programas o herramientas para explotar automáticamente vulnerabilidades de programas legales u ordenadores

12 Redes de ordenadores "zombies", contaminados con un malware, que reciben órdenes remotamente desde un centro de control para realizar ataques coordinados entre muchos o todos los ordenadores de la red.

**Vectores de mitigación**

• Usar anti-virus y cortafuegos y tenerlos actualizados y bien configurados, tanto en el ordenador como en el teléfono móvil y tableta.

• Descargar aplicaciones sólo de sitios de confianza mejor si son los pre-configurados por el fabricante del dispositivo móvil.

• Evitar abrir mensajes de desconocidos, aunque parezcan de una persona conocida con una dirección nueva.

• No pinchar enlaces en mensajes sino teclearlos a mano en el navegador.

• Evitar visitar páginas web desconocidas.

## 3.2. DISPOSITIVOS DOMÉSTICOS CONECTADOS: INTERNET DE LAS COSAS (IOT)

La Internet de las Cosas, junto con el ransomware, ha copado los principales titulares periodísticos de 2016 referidos a la ciberseguridad de las personas y empresas. La impresión general es que estamos aún en el inicio de una explosión. Como aperitivo, en 2016 hemos visto importantes ataques de denegación de servicio (DoS) orquestados desde botnets creadas con dispositivos de la Internet de las Cosas (IoT, por "Internet of Things")

Según la Wikipedia, Internet de las cosas es "un concepto que se refiere a la interconexión digital de objetos cotidianos con Internet"[13]. Algunos objetos serían routers (equipos de acceso a Internet, ADSL o Fibra Óptica), cámaras web, puntos de acceso wifi, grabadores de vídeo, impresoras, televisores inteligentes e incluso bombillas. Son esencialmente micro-ordenadores, con su CPU, memoria e interfaces de red, conectados a Internet las 24 horas del día, realizando una tarea muy concreta.

La Internet de las Cosas está en pleno crecimiento exponencial. En 2008 estos objetos ya superaron a los humanos conectados a la red. Los analistas barajan diversas estimaciones, pero en general se admite que 2016 acabó con una Internet de las Cosas formada por seis mil millones de dispositivos y en 2020 podrían ser veinte mil millones.[14]

El principal problema de la Internet de las Cosas es que su ciberseguridad es mínima o nula. El usuario no puede interactuar directamente con el sistema operativo, por lo que no puede actualizarlo y la mayoría de dispositivos no están preparados para actualizarse solos. También suele ser difícil o imposible cambiar las contraseñas, cuya versión de fábrica puede ser demasiado fácil de adivinar o aparecer en manuales de acceso público.

Todo esto convierte a la Internet de las Cosas en un montón de millones de objetos desactualizados y vulnerables a ataques, conectados a Internet las 24 horas, algo muy interesante a la hora de orquestar ataques de Denegación de Servicio (DDoS), cuando es clave que los dispositivos que actúan como armas estén conectados el mayor tiempo posible a la red.

En 2016 hemos podido ver lo que los expertos consideran sólo el principio de los múltiples problemas que puede conllevar esta IoT con miles de millones de dispositivos mal protegidos. En verano de 2016, en plenos Juegos Olímpicos de Río de Janeiro, se usó una botnet hecha con 10.000 dispositivos de la IoT para bombardear diversos sitios web relacionados con los Juegos. El punto máximo del bombardeo fue de 540 Gbps.[15]

En septiembre, una botnet con 14.000 dispositivos de IoT se lanzó contra la web del periodista Brian Krebs. El punto máximo del ataque llegó a los 620 Gbps[16]. En octubre, otro ataque de la Internet de las Cosas, básicamente routers y cámaras IP, puso de rodillas al proveedor de DNS Dyn y a la propia Internet, dado que algunos

13 https://es.wikipedia.org/wiki/Internet_de_las_cosas

14 ENISA Threat Landscape Report 2016

15 http://www.arbornetworks.com/blog/asert/lizard-brain-lizardstresser

16 http://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

servicios como Twitter, Spotify o Reddit se vieron ralentizados o caídos esporádicamente. La potencia máxima rozó la friolera de 1,2 Terabits por segundo.[17]

En noviembre, el conocido proveedor de hosting francés OVH sufrió brutales oleadas de ataques DDoS, coordinados desde diferentes botnets hechas con cámaras IP, routers y grabadoras digitales. La potencia máxima fue de 1,1 Terabits por segundo[18]. También en noviembre, 900.000 clientes de Deutsche Telekom en Alemania se quedaron sin Internet ni televisión[19] tras un ataque DDoS de una botnet, creada con dispositivos IoT, posiblemente la misma que habría llevado a cabo los ataques anteriores y a la que se bautizó como Mirai.

El autor de esta botnet, Anna-Senpai, hizo público el código de Mirai el 30 de septiembre de 2016, permitiendo que cualquiera pueda a partir de ahora crear su propio virus y botnet de la Internet de las Cosas. Esto provocó una explosión tanto en la creación de botnets de este tipo como en la "caza y captura" de dispositivos de IoT por parte de los ciber-delincuentes, para añadirlos a sus respectivas botnets y alquilarlas al mejor postor.

A mediados de noviembre, el investigador Robert Graham llevó a cabo un inquietante experimento: conectó una cámara IP JideTech a Internet y en 98 segundos un virus tipo Mirai ya la había detectado y tomado su control.[20]

El parque de aparatos conectados a la Internet de las Cosas, por el que compiten esos oscuros empresarios del "DDoS-como-servicio", aún es pequeño en comparación con lo que puede llegar a ser. Según el estudio "Rise of the Machines" de Gartner, los brutales ataques vistos hasta ahora, que según Akamai[21] han supuesto un aumento del 70% en los ataques DDoS respecto al año pasado, serían sólo "testeos de combinaciones de tipos de tráfico, desde pequeños números de bots. Los autores de estos bombardeos estarían sólo haciendo pruebas sobre las capacidades del malware, sin llegar a desplegar ataques a gran escala".[22]

Los dispositivos de la Internet de las Cosas son especialmente apetecibles para la ciberdelincuencia primero por su número: son miles de millones de dispositivos inseguros a los que cada día se añaden 5,5 millones de objetos más. Están siempre conectados, por lo que están siempre disponibles. Suelen estar conectados a conexiones de Internet de alta velocidad, lo que permite generar mucho tráfico de datos de ataque DDoS. Además, estos objetos son muy útiles como proxyes anónimos. Por último, la tecnología y manuales para asaltar estos dispositivos y usarlos en ataques se han puesto a disposición pública.[23]

La mitigación de esta amenaza es realmente difícil, dado que buena parte de estos objetos no tienen forma de ser actualizados, ni de mejorar su seguridad. Las organizaciones ven con preocupación las expectativas de que, con Internet de las Cosas, sus ecosistemas crecerán de forma significativa, así como el volumen del intercambio de datos. Esto hará cada vez más difícil la monitorización del perímetro de los ecosistemas.[24]

Las organizaciones no están aún concienciadas de la dimensión real del problema. La Internet de las Cosas es sólo el sexto tema de ciberseguridad que más preocupa a las empresas. Los protección de los datos generados por estos dispositivos (36%) y la identificación de datos sensibles generados por los mismos (30%) son los riesgos a los que están más atentas, por el momento, las compañías.[25]

17 http://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit

18 http://www.bbc.com/news/technology-37504719

19 http://www.theregister.co.uk/2016/11/28/router_flaw_exploited_in_massive_attack

20 http://www.theregister.co.uk/2016/11/18/surveillance_camera_compromised_in_98_seconds

21 https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-security-executive-summary.pdf

22 http://icitech.org/wp-content/uploads/2016/12/ICIT-Brief-Rise-of-the-Machines.pdf

23 https://pages.arbornetworks.com/rs/082-KNA-087/images/12th_Worldwide_Infrastructure_Security_Report.pdf

24 http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2016

25 http://dtr.thalesesecurity.com/

**Vectores de mitigación**

- Antes de comprar estos objetos, asegurarse de que el software y contraseñas pueden ser actualizados y actualizarlos periódicamente.

- Investigar si realmente, para su correcto funcionamiento, estos dispositivos necesitan estar conectados a Internet y, en caso de que no sea necesario, desconectarlos, o conectarlos sólo cuando sea necesario.

- En general, aislar los dispositivos IoT de otros servicios y de Internet, si no es necesario.

- Cerrar servicios innecesarios en estos dispositivos, como la redirección DNS, muy usada en ataques DDoS, para evitar que sean accesibles desde Internet. Mejor deshabilitarla.

- Comprar dispositivos de fabricantes que puedan probar que sus productos son seguros y pedirles pruebas de esta seguridad.

- Monitorizar nuestro tráfico saliente.

## 3.3. INFRAESTRUCTURAS CRÍTICAS: SCADA

2016 ha sido el año en que se ha tomado conciencia de la importancia de la ciberseguridad en entornos industriales y de infraestructuras críticas, y de lo poco protegidos que están actualmente estos entornos. Prácticamente cada mes hemos conocido al menos dos casos de ataques importantes a infraestructuras críticas de todo el mundo, desde Ucrania hasta Estados Unidos, desde Uruguay hasta Japón.

El año empezó con un importante ataque contra la red eléctrica de Ucrania que dejó a 80.000 personas sin luz durante 6 horas, en un frío 23 de diciembre de 2015. Después se supo que una de las piezas claves de la acción ciber-terrorista había sido un virus, bautizado como BlackEnergy, junto con un fuerte ataque de Denegación de Servicio (DDoS).[26] El gobierno de Ucrania culpó al ruso del ataque.

El 17 de diciembre de 2016 se reprodujo otro ataque contra la red eléctrica de Ucrania, esta vez acompañado de otros ataques contra altos funcionarios, entre ellos la Administración del Transporte Ferroviario. Según algunos observadores, Ucrania estaría sirviendo de banco de pruebas a la hora para realizar ataques de este tipo.[27]

El "Mapa de Ruta de la Ciberseguridad Industrial en España"[28] describe la situación actual: "Los propietarios y gestores de los sistemas de control industrial tienen gran experiencia en el establecimiento y desarrollo de medidas de seguridad física, medio ambiental, de prevención laboral, lo cual, indudablemente ha salvado muchas vidas y protegido a las instalaciones industriales de ataques físicos (que requieren presencia física). Sin embargo, desde un punto de vista lógico, la gran mayoría de los sistemas de control industriales son vulnerables (malware, botnets, DDoS)".

"Esto supone un cambio de tendencia importante, ya que, debido a la integración de las redes de control con las corporativas, hoy en día, los ataques ya no requieren presencia física en las instalaciones y pueden ser realizados de manera remota a través de redes públicas. Esta situación se ve agravada por el hecho de que las instalaciones ya no deben defenderse sólo de los ataques dirigidos a ellas, sino que también son vulnerables a ataques casuales o al azar que tan sólo buscan un objetivo vulnerable".

26 https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

27 https://motherboard.vice.com/en_us/article/ukrainian-power-station-hacking-december-2016-report

28 https://www.cci-es.org/mapa

La completa seguridad en la industria y las infraestructuras críticas, es hoy una entelequia de la que empiezan a aprovecharse los atacantes. La situación es mejor o peor según la situación geográfica, según informe publicado por el Centro de Ciberseguridad Industrial: "Europa está entre 5 y 10 años por detrás de EEUU en la implantación de controles de Ciberseguridad Industrial, y países como España se encuentran más de un lustro por detrás de otros países europeos como Holanda o el Reino Unido. En Latinoamérica existen también importantes carencias en este ámbito".[29]

Uno de los pocos países latinoamericanos de los que se conocen datos de ataques a infraestructuras es Uruguay: durante 2016, su Centro de Respuesta a Incidentes de Seguridad Informática habría contado 21 casos, seis de muy alta severidad y 15 de alta severidad, dirigidos a servicios considerados como infraestructuras críticas.[30]

En Brasil, los ataques a sistemas industriales de automatización explosionaron en 2015, pasando de 114 el año anterior a 778. Los principales responsables fueron los ataques de malware. Esta alta incidencia demuestra que la mayoría de las redes de automatización en Brasil, igual que en otros países, "no tienen los recursos mínimos de seguridad frente a software malicioso, cuentan con máquinas sin antivirus, y con parches obsoletos, cuando existen. Este frágil escenario se debe básicamente a dos factores: el retraso de los fabricantes en la publicación y prueba de parches ya liberados, y la falta de buenas prácticas y políticas de ciberseguridad en las redes de automatización".[31]

En España, según datos del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), en 2015 se registraron 134 ataques contra infraestructuras críticas españolas y para 2016 se esperaba que fuesen más del doble, alrededor de 300.[32] El sector energético es el más atacado. Los incidentes más relevantes contra estas infraestructuras en España son los accesos no autorizados, el fraude y el malware, siendo el malware el tipo de incidente con mayor repercusión. Su aumento está siendo de más del 100% anual.


**Figure 3:** Fuente: Centro de Ciberseguridad Industrial.

29 https://www.cci-es.org/mapa

30 http://www.elobservador.com.uy/uruguay-sufrio-15-ciberataques-alta-severidad-2016-n1022628

31 https://www.cci-es.org/documents/10694/296864/Informe+incidentes+de+ciberseguridad+en+Brasil+2016_ES.pdf/042d6a49-1f73-470e-adfa-484805262dff

32 http://www.cnpic.es/Biblioteca/Noticias/NOTA_DE_PRENSA_SES_PNPIC.pdf

El malware tipo ransomware ha sido en 2016 responsable de algunos sonados ataques contra infraestructuras críticas. En mayo, una empresa de agua y electricidad de Michigan necesitó una semana para recuperarse de un ataque de ransomware que, por suerte, sólo afectó a sus oficinas.[33] Más grave fue, en noviembre, el ataque de un ransomware contra la Agencia de Transporte Municipal de San Francisco.[34] Durante una semana sus usuarios pudieron viajar gratuitamente porque el ataque impactó sus sistemas de pago, más de 2.000 ordenadores.

En España, un ransomware inutilizó el 25 de abril el servidor de la Subdirección General de Gestión Económica y Patrimonial del Ministerio del Interior, que da servicio a nueve departamentos.[35]

Otro número importante de ataques contra infraestructuras críticas se consideran realizados por grupos sofisticados pagados por gobiernos. Un buen ejemplo sería la llamada Operación Dust Storm, dada a conocer en febrero de 2016 por la firma Cylance. La Operación estaría en marcha desde 2010 y atacaría intereses comerciales de diferentes países, con especial foco en Japón, donde habría asaltado diferentes infraestructuras críticas como compañías eléctricas, petrolíferas y de gas, fianzas, transporte y construcción.[36]

Semanas después se descubría otra operación gubernamental dirigida al ataque de las infraestructuras críticas de sus enemigos: OnionDog, en marcha desde 2013 y dirigido contra países de habla coreana que usarían el popular programa de oficina Hangul. El troyano OnionDog aprovechaba una vulnerabilidad en este programa para atacar redes aisladas a través de un gusano USB. Metro y otros sistemas de transporte público, redes eléctricas, empresas del agua y otras estarían entre sus víctimas.[37]

Verizon informaba de otro importante ataque, en marzo de 2016, en una compañía no desvelada: un grupo hacktivista próximo a Siria se habría infiltrado en el sistema de control de una compañía de agua gracias a que las credenciales se guardaban en su servidor web, accesible vía SQL injection. El sistema atacado era el encargado de los controladores lógicos programables que regulaban las válvulas y canales que a su vez controlaban el flujo del agua y los químicos usados para su tratamiento.[38]

Junto a este aumento de la actividad delictiva contra infraestructuras críticas, han avanzado también los esfuerzos dirigidos a la prevención y protección. En marzo de 2016, el Secretario de Estado de Seguridad del gobierno de España presentaba, en la sede de la compañía Gas Natural Fenosa, el "Plan Nacional de Protección de Infraestructuras Críticas" ante 200 operadores públicos y privados de los sectores de energía, industria nuclear, sistema financiero, transporte y agua.[39] Siguiendo este plan, en junio se constituía la "Mesa de Coordinación para la Protección de las Infraestructuras Críticas".[40]

**Vectores de mitigación**[41]

- Crear una política adecuada para la gestión de las aplicaciones que hacen uso de las redes de automatización, aumentando el control de las mismas y limitando su uso a los aplicativos estrictamente necesarios.

- Limitar el uso de aplicaciones P2P y/o de intercambio de archivos basado en el navegador en las redes de automatización.

- Limitar el uso de aplicaciones de anonimización, como proxies, accesos remotos y túneles cifrados.

- Realizar copias de seguridad

33 http://www.theregister.co.uk/2016/05/03/michigan_electricity_utility_downed_by_ransomware_attack

34 https://threatpost.com/hackers-make-new-claim-in-san-francisco-transit-ransomware-attack/122138

35 http://www.elconfidencial.com/espana/2016-05-03/un-virus-ransomware-inutiliza-nueve-areas-del-ministerio-del-interior-una-semana_1192757

36 https://www.helpnetsecurity.com/2016/02/24/japanese-critical-infrastructure-under-targeted-attack

37 https://www.helpnetsecurity.com/2016/03/09/oniondog-apt-targets-the-infrastructure-industry

38 http://www.theregister.co.uk/2016/03/24/water_utility_hacked

39 http://www.cnpic.es/Biblioteca/Noticias/NOTA_DE_PRENSA_SES_PNPIC.pdf

40 http://www.cnpic.es/Biblioteca/Noticias/mesa_coordinacion_pic.pdf

41 https://www.cci-es.org/documents/10694/296864/Informe+incidentes+de+ciberseguridad+en+Brasil+2016_ES.pdf/042d6a49-1f73-470e-adfa-484805262dff

- Proteger las consolas de operación y supervisión para que se dediquen, exclusivamente, a las funciones típicas de operación, ingeniería y mantenimiento. Los servicios y puertos que no sean necesarios deben ser desactivados.

- Establecer perímetros de seguridad en las redes de acceso para poder filtrar y restringir los puntos de acceso. Bajo ningún concepto debería permitirse acceso directo a Internet o disponer de una dirección IP pública que permita el acceso desde una red externa.

- Formar al personal de operación y mantenimiento.

- Establecer una gestión de cambios derivados de incidentes de ciberseguridad.

- Establecer un proceso contínuo de gestión de la ciberseguridad.


**Figure 4:** Recomendaciones para operadores de infraestructuras críticas. (Fuente Kaspersky)

# 3.4. VEHÍCULOS INTELIGENTES

La ciberseguridad en coches inteligentes es un concepto nuevo que apareció con fuerza en verano de 2015, después que dos hackers demostrasen que era posible atacar remotamente un Jeep y hacerlo frenar en medio de la autopista.[42] En 2016 se han sucedido nuevas demostraciones públicas de inseguridad en coches inteligentes. Éstos son considerados parte de la Internet de las Cosas y, como el resto de dispositivos que la forman, su talón de Aquiles es la falta de ciberseguridad, debido a su complejidad y la poca familiarización de los fabricantes con este contexto.

ENISA define "coches inteligentes" como "los sistemas que incluyen funciones conectadas de valor añadido para mejorar la experiencia de los usuarios o la seguridad de los vehículos. Esto incluye no sólo vehículos particulares sino también comerciales, como autobuses, camiones y otros".[43]

En el último año han aumentado las investigaciones y exposiciones públicas que denuncian fallos de seguridad en coches inteligentes. Algunas de estas demostraciones han sido además muy fáciles y baratas, como el adolescente que consiguió abrir y poner en marcha remotamente un coche inteligente con una inversión de sólo 15 dólares en material eléctrico.[44]

Uno de los descubrimientos más espectaculares del año, por el número de vehículos afectados (100 millones), lo llevó a cabo un grupo de investigadores liderado por Flavio Garcia, de la Universidad de Birmingham. Consiguieron extraer la clave de cifrado que permite abrir y cerrar a distancia todos los coches Volkswagen creados a partir de 1995.[45]

En septiembre, investigadores chinos del Keen Security Lab mostraron en un vídeo cómo manipulaban el sistema de frenos de un coche Tesla mientras estaba siendo conducido. La manipulación era remota, a 19 km del coche, usando un portátil. Los investigadores consiguieron también abrir una puerta del vehículo sin usar ninguna llave.[46]

La industria de automoción ha demostrado tener poco en cuenta la seguridad informática en el diseño de sus vehículos inteligentes. Han sido reportados graves problemas en la protección de las comunicaciones, en la autenticación y autorización y en el diagnóstico. Como ejemplo, no se han establecido estándares de evaluación de seguridad en vehículos inteligentes. Conceptos de ciberseguridad como "prueba de penetración" son desconocidos para la industria.

Los avisos de los investigadores respecto a los peligros detectados no han estimulado un diálogo transparente con la industria de la automoción, que más bien ha mostrado una reacción tardía y negativa.[47]

Los principales ataques que puede sufrir un vehículo inteligente son accesos no autorizados al sistema de información o la red, instalación no autorizada de software, ataques de hombre-interpuesto (Man-in-the-Middle), uso no autorizado de dispositivos y sistemas, y filtración de información. En ellos pueden verse comprometidos los sensores, la Unidad de Control Electrónico (ECU), la Red de la área de Control (CAN), redes, subredes, conexiones inalámbricas y una miríada de componentes que hacen casi titánica la protección total del vehículo.

Las consecuencias debidas a la manipulación de las ECU y las redes pueden ser muy peligrosas, llegando hasta la desconexión de los frenos, parar el motor o activar el airbag en plena conducción, también acelerar o aminorar la velocidad del coche, forzar el cierre de las puertas, desactivar los cinturones de seguridad, activar los intermitentes, cerrar o encender el aire acondicionado, mover los retrovisores, subir y bajar las ventanas, poner las luces cortas o largas, manipular la radio o el televisor, etc.

42 http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

43 https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

44 http://www.forbes.com/sites/leoking/2015/02/23/14-year-old-hacks-connected-cars-with-pocket-money

45 https://arstechnica.com/cars/2016/08/hackers-use-arduino-to-unlock-100-million-volkswagens

46 http://www.bbc.com/news/technology-37426442

47 https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars


**Figure 5:** El futuro de Internet de las cosas: vehículos vulnerables...

**Vectores de mitigación**

- Mejorar la comunicación entre la industria y la comunidad de ciberseguridad. Promover el intercambio de información en talleres, conferencias, etc.

- Clarificar los temas de responsabilidad legal de la industria.

- Crear un consenso en estándares técnicos de buenas prácticas.

- Definir un esquema de evaluación por terceras partes

- Crear herramientas para análisis de seguridad en vehículos inteligentes.

# 3.5. DERECHO A LA PRIVACIDAD: PROTECCIÓN DE DATOS

## 3.5.1. PHISHING

El phishing[48] es un mecanismo criminal que emplea Ingeniería social y subterfugio técnico para robar Datos de identidad personal y credenciales de cuentas bancarias a los consumidores. Los patrones de ingeniería social usan e-mails falsificados, que se propone pertenecen a empresas o Agencias legítimas, diseñadas para llevar a los consumidores a sitios web que inducen a los visitantes a revelar datos financieros, como nombres de usuario y contraseñas. Los patrones de subterfugios técnicos usan programas tipo "crimeware" en PC, para robar credenciales directamente, a menudo utilizando sistemas para interceptar nombres y contraseñas de usuario de los consumidores conectados, y corromper las herramientas de navegación locales para redirigir a los usuarios a sitios web falsificados (o auténticos, pero a través de PROXYes controlados por phishers para interceptar las pulsaciones de teclas de los consumidores).

El patrón habitual de este tipo de ataque consiste en que recibimos un mensaje de correo electrónico (spam[49], en algunos casos se usa SMS en vez de correo), con una oferta comercial, de nuestro banco o proveedor de servicios o de un amigo o conocido, en el que se nos invita a:

a) Visitar una página web, que simulará ser la del comercio, banco o proveedor y nos pedirá, o bien que nos acreditemos para acceder al servicio, o bien los datos de nuestra tarjeta de crédito; o

b) Responder directamente al mensaje con nuestros datos de acceso.

Si lo hacemos, habremos dado nuestras credenciales a la organización que ha lanzado la "campaña" de "phishing" (en inglés significa pescando), para "a ver qué pescamos hoy" (una campaña dura unas 32 h, por término medio).

Hay quien piensa que el "phishing" está pasado de moda. Pero según los informes de APWG[50] el número de ataques de "phishing" se ha mantenido estable, aunque con ciertos repuntes estacionales de hasta 100% (se detectan 1 "phishing" nuevo cada minuto, más de 100.000 al trimestre). Los sitios desde los que se realizan ataques (URL) han aumentado un 25% durante 2016, con puntas de hasta un 100% más que los registrados a principio de 2016.

El peligro real para la sociedad es que el "phishing" ha derivado a "spear-phishing" o ataques dirigidos a engañar a una persona o grupo dentro de una organización. Consisten en mensajes muy concretos, aparentemente provenientes de personas conocidas o compañeros de trabajo, con temas y contenidos "calcados" de mensajes habituales de esa persona. Con estas técnicas se consigue acceso a datos confidenciales de la organización o a los sistemas de control de la producción, suministros o distribución, sembrando el caos y la interrupción del servicio. Este tipo de

48 Wikipedia. Phishing (2015). <http://en.wikipedia.org/wiki/Phishing>.

49 Gudkova, Darya; Demidova, Nadezhda (2014). "Spam and phishing in Q2 2014". Secure List. <http://securelist.com/analysis/quarterly-spam-re- ports/65755/spam-and-phishing-in-q2-2014/>

50 https://docs.apwg.org/reports/apwg_trends_report_q2_2016.pdfhttp://docs.apwg.org/reports/apwg_trends_report_q3_2016.pdf

ataques suele empezar por personas no-técnicas, escalando progresivamente en el escalafón de la organización hasta llegar a las personas con los privilegios necesarios para perpetrar el ataque.

En cuanto a los ataques a personas, el phishing ha seguido abusando de la información disponible en los medios sociales. Durante 2016 el phishing tuvo una participación significativa en las campañas de secuestro de datos: "ransomware". Éstos habían aumentado del orden de un 800% en comparación con 2015. Esta tasa se puede explicar con el aumento de sitios de phishing únicos en un 61%, reportado por APWG para el segundo trimestre de 2016. Por otra parte, es notable que el phishing ha alcanzado exitosamente el nivel ejecutivo: fraude basado en phishing basado en CEO ha causado pérdidas significativas a las empresas.[51] Tales ataques se llevan a cabo ya sea tomando cuentas de correo del ejecutivo a través de phishing, o directamente phishing empleados con mensajes falsos de la CEO.[52]

Combinación de phishing con la inteligencia (espionaje) que se ha ganado a través de los medios de comunicación social. Además de difundir mensajes de phishing a un determinado grupo objetivo, los atacantes han recopilado información de las redes sociales sobre comportamientos, por ejemplo, sobre sus trabajos, hábitos y estructuras organizacionales. Se espera que los ataques a múltiples niveles de la vida de la víctima van a aumentar en el futuro, en particular, cuando la información robada de dispositivos IoT se está tomando en cuenta.

El comportamiento medido de los usuarios al hacer frente a los mensajes de phishing es indicativo de las tasas de éxito de esta amenaza. 30% de los mensajes han sido abiertos por los destinatarios en promedio. 12% de los destinatarios han hecho clic en el malware adjunto / enlace y por lo tanto han causado una infección en su sistema.[53] La explicación puede ser la mayor eficiencia lograda por los phishers dado los avances en engañar a la gente.

Se demuestra que cuando se tiene en cuenta la inteligencia sobre el perfil del grupo de víctimas, se puede lograr un impacto mucho mayor con notablemente menos volúmenes de ataque.[54] Por lo tanto, mientras que el phishing ha jugado un papel importante en algunas otras amenazas, ha disminuido en general. Como razones para esta disminución se puede reconocer la eficacia de las medidas anti-phishing y el aumento de la calidad de phishing (es decir, ataques de phishing más específicos).

Las organizaciones de venta minorista y servicios (incluyendo comercio-e) tienen la cuota de ataques de phishing más alta (alrededor del 43%), seguidos del sector financiero, con un 21%, que ha aumentado a un ritmo de un 25% por trimestre (Figure 6: Sectores más atacados por Phishing durante 2016 (Fuente APWG. org)). Por último, el phishing se ha centrado en las empresas cada vez más pequeñas (1-250 empleados), mientras que la cuota de las grandes y medianas empresas se ha reducido[55], [56]. Se cree que esta tendencia continuará en un futuro próximo. Las encuestas muestran que el phishing está en la tercera posición de las amenazas más perjudiciales.[57]

Los 5 principales países que hospedan el sitio web de phishing: Estados Unidos, Belice, Hong Kong, Bélgica y Reino Unido[58]. La geografía de las víctimas de phishing incluye China (alrededor del 20%), Brasil (alrededor del 18%), Argelia (alrededor del 14%), Reino Unido (alrededor del 13%) y Australia (aproximadamente 12,5%).

51 https://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/

52 https://lifars.com/2016/07/email-scammers-stealing-billions-from-american-companies/?utm_source=Subs&utm_campaign=851e26b20d-CyberNews_July_28&utm_medium=email&utm_term=0_a931d19921-851e26b20d-342302245

53 http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

54 https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2016

55 https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers strike-large-business-en.pdf

56 https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf?aid=elq_9562&om_sem_kw=elq_14669249&om_ext_cid=biz_email_elq

57 http://blogs.splunk.com/2016/06/29/detecting-and-responding-to-the-accidental-breach/.

58 https://www.forcepoint.com/resources/reports/forcepoint-2016-global-threat-report

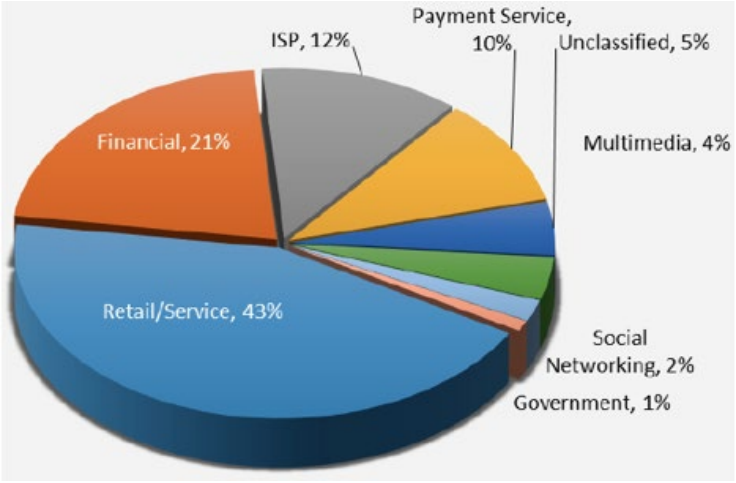


**Figure 6:** Sectores más atacados por Phishing durante 2016 (Fuente APWG.org)

**Vectores de mitigación:**

Las posibles contramedidas para evitar esta amenaza contienen los siguientes elementos:

- Realización de cursos de entrenamiento y concientización dirigido al phishing.

- Rendimiento del filtrado de correo electrónico seguro en las pasarelas.

- Verificación de la identidad del remitente y de las URL, así como control de los DNS usados.

- Detección y eliminación de archivos adjuntos maliciosos en las pasarelas de correo electrónico.

- Escanear URL recibidas y clicadas buscando características maliciosas en servicios PROXY.

- Implantación de detección de fraude y anomalías a nivel de red, tanto de entrada como de salida.[59]

- Implementación de múltiples controles (incluyendo autenticación de doble factor) para las transacciones financieras críticas.

59 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4701335/, https://eprint.iacr.org/2016/040.pdf,

## 3.5.2. PROTECCIÓN DE DATOS PERSONALES

Dato personal es cualquier información que se pueda usar para identificar, contactar o localizar a una persona, o puede ayudar a conseguirlo, con otros datos. En inglés se conoce con las siglas PII (Información de identificación personal). Pero hoy en día debemos considerar los datos personales desde dos perspectivas adicionales: a) los datos que permiten suplantar nuestra identidad, b) las que permiten atentar contra nuestra privacidad.

**1. Identidad digital**

En el mundo moderno todos los adultos y adolescentes (y muchos niños) tenemos una identidad digital, que nos permite ser reconocidos a las aplicaciones accesibles a través de la red Internet. De hecho, tenemos muchas de identidades digitales, tantas como redes sociales o cuentas de correo electrónico o portales web o aplicaciones a los que tenemos derecho de acceso.

La identidad digital es uno de los activos más codiciados por las mafias organizadas del cibercrimen, y una de las fuentes de ataque más comunes. Según un informe de Symantec[60] Se declaran más de 300 incidentes de robo de datos personales al año, pero sólo los operadores de telecomunicaciones están obligados a declararlos, y se estima que entre el 80% y el 90% no se declaran[61] (Figure 7). En cada incidente se exponen una media de más de 1 millón de identidades, aunque la mediana se está reduciendo a unas 5.000, porque la mayoría de ataques son a pequeños comercios o empresas (figure 8).


**Figure 7:** Brechas de datos personales comprometidos no declarados (fuente Symantec)

**2. Monetización de los datos personales**

Nuestros datos personales tienen un precio, que es función de nuestro perfil como personas (vida privada) y profesionales, y del tipo de información de que se trate: financiera, salud, sexo, religión, aficiones, etc.


**Figure 8:** Evolución de las brechas de datos personales (fuente Symantec)

60 https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf?aid=elq_9562&om_sem_kw=elq_14669249&om_ext_cid=biz_email_elq_

61 https://www.symantec.com/security-center/threat-report

En cuanto a las credenciales de identidad digital, el precio es función de la aplicación a la que de acceso: financieras, sanitarias, de operación de infraestructuras críticas, etc.

También depende del país o región donde habitamos y las plataformas en las que se comercialice.

Debemos ser conscientes de que las aplicaciones gratuitas en realidad cobran a través de la comercialización de nuestros datos personales.

Incluso hay productos comerciales (ordenadores y dispositivos móviles), que se comercializan a precios inferiores al de coste, contando con el beneficio que se obtendrá de los datos personales y posibilidad de perfilar a los clientes que los adquieran o los que se les regale.

Por lo tanto, se debe concienciar a la gente de la necesidad de evitar ceder estos datos de forma gratuita, para evitar sustos y problemas, además de financiar negocios ilegales.

### 3. Privacidad corporativa como persona jurídica

Las organizaciones también tienen una identidad digital, que va más allá del puro acceso a servicios en la red Internet, pues permite a los usuarios de la red identificar a la organización y diferenciarla de otras similares que puedan existir, es la "Imagen Corporativa".

Esta imagen digital corporativa puede verse deteriorada por varios motivos:

- La creación de identidades falsas en las redes sociales, dominios de Internet, o correos electrónicos, que pretenden ser la de la organización, con la intención de suplantarla en los mensajes transmitidos en el Mercado, la Sociedad o individuos concretos.

- El robo de datos corporativos, directamente de las bases de información corporativas (Data Leakage) o a través de perfiles de sus directivos en las redes sociales. Este es un peligro muy importante (recordemos los incidentes causados por WikiLeaks) y puede facilitar: a) la creación de identidades falsas "creíbles", b) daños económicos por la pérdida de concursos públicos o disminución del valor de las acciones en el mercado, c) daños difíciles de reparar en la imagen social de la organización en el mundo entero por la difusión de datos confidenciales.

El número de marcas únicas atacadas es de alrededor de 400, por lo que se han utilizado 350-400 URL por marca, según el informe de APWG[62], destacando: Microsoft (alrededor del 8%), Facebook (alrededor del 8%) y Yahoo (alrededor del 7%) son las tres principales organizaciones mencionadas en los mensajes de phishing[63]. Por sectores, el robo de datos ha afectado en un 44% al sector sanitario, un 31% a empresas[64], aunque en el informe de Symantec estas dos categorías se agrupan en "servicios" (Figure 9).


**Figure 9:** Incidentes y registros afectados informados por sectores (fuente Symantec)

62 http://docs.apwg.org/reports/apwg_trends_report_q3_2016.pdf

63 https://kasperskycontenthub.com/securelist/files/2016/08/Spam-report_Q2-2016_final_ENG.pdf

64 http://www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html

**4. Percepción del riesgo asociado al robo de datos personales**

A pesar de los datos alarmantes que hemos mencionado y el número de datos personales robados en brechas en los últimos meses (Figure 10), los ciudadanos y los directivos no tienen conciencia de los riesgos que representa la pérdida de identidad digital. Por ello debemos aumentar los esfuerzos para concienciar a los ciudadanos y profesionales de que hay dos peligros importantes a evitar:

- Robo de datos personales, que puede tener consecuencias económicas y funcionales importantes. Debemos distinguir entre el robo de:

o Nuestros datos personales, que puede causarnos inconvenientes derivados de su mal uso, como por ejemplo pérdida de privacidad, si alguien que no deseamos nos aborda y / o acosa, y nos provoca alteraciones psicológicas o pérdidas económicas directas (robo) o indirectos (incremento de medidas de seguridad personal o privacidad).

o Los datos personales que otras personas nos han cedido y que conservamos en nuestras agendas de contactos, listas de clientes, proveedores, ciudadanos, etc. En este caso, el daño lo pueden sufrir estas personas y por lo tanto nos debemos sentir responsables, y en el peor de los casos, la justicia nos puede pedir responsabilidad y castigarnos si no hemos tomado las medidas adecuadas de protección de estos datos.

- Alteración de datos personales, que puede conllevar problemas en nuestras relaciones sociales, también tenemos que hacer frente a dos escenarios:

o Modificación de nuestros datos personales (perfil, características personales, datos de contacto, etc.) a ficheros, agendas o bases de datos de una organización o persona determinada. Esto puede provocar que no puedan contactar con nosotros, que no nos puedan reconocer, o que perdemos derechos que nos corresponden. Todo esto puede tener un impacto negativo en nuestra relación con la entidad afectada.

o Modificación de los datos personales con las que nos identificamos ante una organización, puede igualmente alterar esta relación, hasta impedir que nos podemos relacionar con ella, o provocar su rechazo, por haber "perdido" los atributos que nos daban derecho.Modificación de los datos personales de otras personas que nosotros tenemos almacenadas, igualmente deterioraría nuestra relación con estas personas, limitando, debilitando o anulando nuestra capacidad de comunicarnos con ellas.

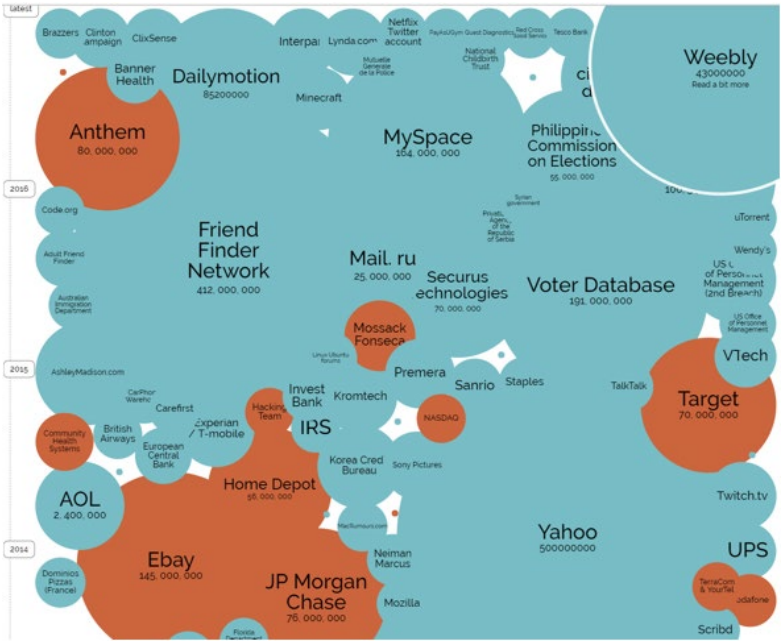


**Figure 10:** Últimos incidentes de robo de datos personales (fuente http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.)

El coste medio de una brecha de datos es de unos 4M USD, unos 150 USD/registro robado, aunque en los ataques más voluminosos el coste se dispara, por el impacto que puede tener en la valoración de la empresa en bolsa. Por ejemplo, el robo de credenciales de usuarios de PlayStation de Sony en 2011, provocó pérdidas en la compañía superiores a las que le causó el Tsunami de ese mismo año en Japón, que le obligó a interrumpir la producción en 5 plantas.

El robo de credenciales está relacionado con el acceso ilegal a: Documentos gubernamentales (declaraciones de beneficios o pago de impuestos) (aprox. 49%), fraudes de tarjetas de crédito (15%), fraude Telefónico o de otros suministros (10%), Fraude bancario (Ca 6%), Intento de robo de identidad (aprox. 3.7%), Fraude de préstamos (3.5%), relacionado con empleo (aprox. 3,3%), Otros (aprox. 19%). Curiosamente, las estadísticas son una verificación de la tendencia de monetización (precio en el mercado negro) de estas credenciales.

Hay iniciativas orientadas a aumentar la concienciación de usuarios y directivos, como eSAM[65] y Stop.Think.Connect[66] o la versión hispana: Cibervoluntarios[67]

**5. Percepción del riesgo de robo de identidad**

En general, los / las ciudadano / as son poco conscientes de la relevancia de su identidad digital, y las pesadillas que les podría provocar el robo de esta identidad, más allá del robo o modificación de los datos personales, que hemos visto en el apartado anterior, y que es una forma "blanda" o parcial de robo de identidad, pues no llega a permitir la suplantación de identidad. Una credencial de usuario se ofrece en el mercado negro por una media de 7USD, y el precio depende del tipo de cuenta o plataforma al que de acceso.

Debemos distinguir 2 formas de robo de identidad:

a) Robo de una identidad digital nuestra, que utilizamos habitualmente, normalmente en forma de robo de usuario / contraseña o algún dispositivo que nos permita identificarnos (tarjeta de claves, tarjeta chip, dispositivo electrónico, etc.). En este caso, quien nos ha robado la identidad, se puede mover por la Red Internet como si fuéramos nosotros mismos, y será difícil demostrar que lo que haga esta persona (o robot digital) no lo hemos hecho nosotros. Según a que nos dé derecho de acceso o porque utilizamos en esta identidad robada, los daños pueden ser de varios tipos:

a. En una entidad financiera: tendrá impacto económico.

b. En la Administración Pública (Gobierno-electrónico): tendrá impacto administrativo, económico e incluso podría ser multado.

c. En las redes sociales: podrá provocar desprestigio ante la familia, amistades o conocidos, si quien nos suplanta difunde imágenes o información falsa (o cierta) sobre nosotros o sobre otros, pero que queríamos mantener confidencial o secreta. O si ponen en palabras nuestras afirmaciones que no guste a nuestros contactos.

d. En el correo electrónico, puede tener las mismas consecuencias que en las redes sociales, pero si el correo es profesional o corporativo, el impacto puede tener consecuencias económicas y de prestigio profesional irreversibles. Recientemente se está utilizando correo electrónico corporativo para modificar los datos de pago de facturas, provocando la transferencia de fondos (el importe de la factura) a una cuenta corriente que no es el del

65 https://www.secureidentityalliance.org/index.php/e-security-awareness-model

66 https://stopthinkconnect.org/

67 https://www.cibervoluntarios.org/

proveedor, y en muchos casos, cuando se descubre la engaño, ya es demasiado tarde para retroceder la transferencia de fondos o divisas. Es el llamado "fraude al CEO" (Director ejecutivo), del que casi el 90% de las grandes corporaciones han sido objetivo, aunque no hay datos de en cuántas de ellas han tenido éxito esos ataques.

b) Creación de una identidad nueva con pretensión de que sea nuestra. Es equivalente a la suplantación de identidad física con un documento falso, en el que figuran nuestros datos personales y de identificación. Es una forma de suplantación de identidad más fácil de detectar que el anterior, pues quien nos conozca de verdad podría sospechar que algo no es correcta. Analicemos algunos casos:

a. En las redes sociales, es un ataque típico entre adolescentes o ex-parejas, para provocar acoso (ciber-bullying) o desprestigio. Requiere una labor continuada y persistente de captación de contactos del mundo real de la persona que se quiere suplantar, en el mundo virtual. Para ello se utilizan estrategias para engañar a los demás, diciendo que se ha cambiado de identidad porque se han perdido las credenciales, para no permitir a algunas personas acceder a las informaciones publicadas, etc. Una vez conseguida una masa crítica de contactos, se provocan los daños comentados con la identidad robada.

b. Con correos electrónicos falsos, igualmente tenemos los mismos tipos de ataques que si se ha robado el acceso a la cuenta de correo original, pero con una dirección que puede pertenecer a un proveedor (dominio) público, tipo Google, Yahoo, Microsoft live , etc. O creando un dominio que sea muy fácil de confundir con el original, por ejemplo BancSabadeil, en lugar de BancSabadell (sólo cambia 1 pixel). Este ataque es especialmente efectivo en transacciones comerciales con interlocutores extranjeros, que pueden tener dificultades para deletrear un nombre corporativo, sobre todo si la parte atacada normalmente usa un abecedario (o iconografía) diferente.

El 75% de los robos de datos son consecuencia de la mala protección de las credenciales de acceso. El 90% de los ataques se perpetran en cuestión de segundos/minutos del robo de las credenciales, mientras que solo el 25% de éstos son detectados en pocas horas. De hecho, se ha detectado un aumento de ataques detectados por policías o por organizaciones independientes, mientras que la detección interna ha disminuido. Aunque el 92% de las empresas Europeas han sufrido alguna brecha de datos en los últimos 5 años, solo un 42% de ellas lo considera un riesgo para su organización, con la consecuente falta de medidas de protección para evitarlas. Es de esperar que el nuevo reglamento general de protección de datos aprobado por el parlamento Europeo (GDPR), que prevé multas de hasta el 2% de la facturación mundial del grupo empresarial afectado por incidente, haga cambiar esta percepción.

Según informe del ITRC[68] (Identity Theft Resource Center[69] ) la distribución de robos de identidad reportados en 2016 por sectores muestra que las empresas (con alrededor del 43%) lideran las estadísticas, seguidos por el Sanitario/Médico (36%), Educación (9%), Gobierno/Militar (aproximadamente 7%) y Banca / Finanzas (Aproximadamente 4%). Es de destacar que, aunque ha aumentado el número de incidentes de brechas de datos el número de identidades robadas ha disminuido respecto a 2015.

68 http://hosted.verticalresponse.com/358216/ac0a9368d8/1746749985/0f7bdaadc2/

69 http://www.idtheftcenter.org/Alerts/itrc2013breachreport.html

# 3.6. ACCESO A LA INFORMACIÓN

## 3.6.1. ATAQUES DE DENEGACIÓN DE SERVICIO

Estos ataques tienen por objetivo evitar el acceso normal a servicios web, mediante técnicas que saturan la capacidad de proceso del servidor o de transferencia de datos de las redes a través de las que se puede acceder al mismo.

Esto se puede conseguir de dos formas:

1. Una o varias botnets (red de ordenadores comprometidos con un malware) con decenas o centenares de miles de ordenadores esclavos se lanzan a solicitar servicios contra un mismo objetivo. Los ataques más potentes registrados hasta el momento con este método han sido a OVH y KrebsOnSecurity, usando el malware MIRAI, que consiste en usar como elementos de la botnet dispositivos IoT (Internet de las Cosas) que están mal configurados y tienen un usuario y contraseña muy fáciles de adivinar o los que ha asignado el fabricante por defecto en el momento de la instalación. Con esta técnica se han conseguido generar anchos de banda del orden de 1Tbps (1 millón de Mbps).

2. Un solo o reducido número de ordenadores lanza a otros una petición en nombre de la víctima (spoofing), usando un protocolo de "amplificación", de forma que la víctima recibe un volumen de tráfico decenas o centenares de veces mayor que el generado por el atacante hacia los servidores "involuntarios". Los protocolos más usados para este tipo de ataques son DNS, SSDP, NTP, SNMP, aunque hay más, como CHARGEN, etc.

Los DDoS suelen usarse para socavar la reputación de una empresa rival, que pasará largos periodos sin poder ofrecer sus servicios de forma adecuada, al estar bajo un bombardeo que se come su ancho de banda.

| | country | year | dns | ntp | snmp | ssdp | mirai | weighted |
|---|---|---|---|---|---|---|---|---|
| 1 | Brazil | 2016 | 100 | 100 | 100 | 98 | 100 | 99 |
| 2 | Colombia | 2016 | 96 | 82 | 83 | 94 | 74 | 89 |
| 3 | Argentina | 2016 | 92 | 86 | 76 | 100 | 82 | 88 |
| 4 | Spain | 2016 | 87 | 85 | 80 | 95 | 72 | 87 |
| 5 | Mexico | 2016 | 99 | 93 | 68 | 83 | 82 | 86 |
| 6 | Venezuela, Bolivarian Republic of | 2016 | 76 | 69 | 61 | 97 | 66 | 76 |

**Figure 11:** Países con más ordenadores vulnerables para ataques DDoS en LatAm durante 2016.

| | country | dns | ntp | snmp | ssdp | mirai | weighted |
|---|---|---|---|---|---|---|---|
| 1 | Brazil | 91 | 89 | 100 | 89 | 97 | 92 |
| 2 | Argentina | 82 | 77 | 75 | 96 | 83 | 82 |
| 3 | Colombia | 83 | 72 | 82 | 86 | 75 | 81 |
| 4 | Spain | 78 | 76 | 79 | 89 | 79 | 80 |
| 5 | Mexico | 86 | 83 | 73 | 78 | 85 | 80 |
| 6 | Chile | 67 | 69 | 66 | 76 | 78 | 70 |

**Figure 12:** Países con mayor número de ordenadores vulnerables para ser usados en ataques DDoS en LatAmCaribe al final de 2016

En el período que abarca el informe, la denegación de servicio (DoS) ha producido una presencia impresionante: es la amenaza en el punto de intersección de dos objetivos principales del ciberespacio: monetizar actividades maliciosas y delito cibernético como servicio. Junto con las botnets, el DoS ha sido el principal instrumento que llevó a la extorsión y a interrumpir (tango-downs) servicios e infraestructuras[70], y finalmente las brechas de datos. En la siguientes tablas (Figure 11, Figure 12) se muestra el índice de peligrosidad de los países con mayor número de servidores de red usables en ataques DDoS de amplificación según la metodología propuesta por Cybergreen[71]. En ellas vemos que todos los países han mejorado al final del año (Figure 11), comparado con la media de 2016 (Figure 12). En el mapa adjunto (Figure 13) se observa la distribución geográfica de los servidores usables en estos tipos de ataque de amplificación en Latino-América y Caribe. Los mapas muestran los índices de todos los países de LatAmérica, Caribe y España para ataques de amplificación (Figure 13) y de IoT (Mirai) (Figure 14).

**Figure 13:** Distribución geográfica de los servidores usables en ataques DDoS de amplificación en LatAm. al final de 2016.

70 http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter.

71 http://cybergreen-stats.herokuapp.com/

**Figure 14:** Distribución geográfica de los dispositivos IoT usados en el ataque Mirai en España y LatAm-Caribe.

**Ataques con dispositivos IoT**

Un ataque con un ancho de banda de aprox. 1 TB se ha producido en septiembre de 2016, materializando las predicciones de 2015 sobre la viabilidad de ataques de este tamaño. Un punto alarmante con respecto a este ataque fue la eficiencia en la infección de una enorme red de dispositivos IoT simples con el malware MIRAI. El ataque se repitió en un par de ocasiones, y preocupa mucho el hecho de que un ataque de esta magnitud puede convertirse en una seria amenaza para todo el Internet.

**1. Ataques de amplificación de ancho de banda**

Mediante la optimización de la relación paquete-por-ancho de banda, reflexión y ofuscación, los efectos de DDoS han sido uno de los principales desafíos de seguridad. En todo tipo de sistemas y sectores hemos visto en 2016 un mayor número de ataques DDoS.[72]

72 https://content.akamai.com/PG6852-q2-2016-soti-security.html.

**2. Durante 2016 hemos evaluado que:**

- Los suplantadores de navegadores web han sido los bots DDoS más frecuentes (45%). Cabe destacar el nivel de avance en las capacidades de ofuscación de ataques a aplicaciones (web): el 36% de los ataques de aplicaciones se saltan la protección existente para ciber-ataques convencionales como las cookies o firmas JavaScripts[73], lo cual representa un aumento de aprox. 6% respecto a 2015.

- Los ataques de un solo vector continúan prevaleciendo con aprox. 50% de todos los ataques. Esto se debió al aumento de la reflexión del NTP[74] que ha creado ataques vectoriales únicos.

- El tráfico de red generado por ataques DDoS a gran escala puede causar problemas de conectividad en Internet y / o provocar la falta de servicios importantes, tanto de los proveedores de servicios de protección contra DDoS como de los ISP. Aunque los proveedores de servicios de protección DDoS son una solución eficaz, se considera que una serie de medidas de seguridad, incluidos los ISP, son más eficaces. Mediante la implementación de controles relevantes a nivel de ISPs, se puede lograr una mitigación significativa de DDoS (ver también medidas de mitigación a continuación).

- En 2016, continúa la tendencia al aumento del número de ataques multi-vectoriales. Dependiendo de la muestra reportada y los sectores cubiertos, los ataques multi-vectoriales representan aprox. 35-50% de todos los ataques. Esto es un aumento de aprox. 10% en este año. Esta tendencia es una indicación de que los ataques botnets más eficientes son los llamados híbridos, que pueden crear ataques que van desde vectores únicos a múltiples, en particular para ataques a gran escala (es decir, más de 300 Gbps).

- A principios de 2016, hemos visto que los ataques DDoS se utilizan como intentos de extorsión, es decir, un medio de presión para la monetización. Este es un cambio en el motivo DDoS, pasando de las interrupciones activistas a la monetización directa. Como tal, esta tendencia sigue el cambio contemporáneo de los motivos observados en 2016 con la clasificación de la monetización en la primera posición.

- Continuando la tendencia del año pasado, en 2016 el DDoS es un elemento principal en los mercados "underground". En este año los precios han pasado de unos 25-30 $ por hora a 5 $, convirtiendo así DDoS en una mercancía que es asequible para casi todo el mundo.

- Un evento notable en el negocio DDoS es la publicación del código fuente de Mirai, el malware que se ha utilizado para atacar el sitio web KrebsOnSecurity. Se ha evaluado que, si bien este movimiento podría tener como objetivo obstaculizar el trabajo de la aplicación de la ley, abre nuevas vías para la creación de bots DDoS basados en dispositivos simples.

73 https://www.incapsula.com/blog/banishing-bad-bots.html.

74 https://www.incapsula.com/ddos/attack-glossary/ntp-amplification.html.

- Siguiendo la tendencia de ataque de capa de red, los ataques de aplicación aumentaron aprox. 30% según los informes de Akamai. Los vectores de ataque más populares son Local File Inclusion (LFI) y SQL-injection (SQLi), ya que representan un 88% de todo el tráfico. Aprox un tercio del tráfico pasa a través del servicio de anonimato (Proxy/VPN). Además, se ha evaluado un aumento en la frecuencia de ataques repetidos a las víctimas (desde el 25% de los objetivos del año pasado hasta el 30% en el primer trimestre de 2016). Del mismo modo, la duración de los ataques también aumenta respecto al año pasado.

- La geografía de DDoS es interesante. En primer lugar, varía para los ataques de capa de red y aplicación: mientras que China (alrededor del 50%), EE.UU. (alrededor del 17%) y Taiwán (alrededor del 5%) atacan la capa de red, Brasil (aproximadamente 25%), .23%) y Alemania (alrededor del 9%) son las tres principales fuentes de ataque de aplicaciones. Respectivamente, las víctimas de los ataques de red son la industria del juego (aproximadamente el 55%), el software y la tecnología (aproximadamente el 25%) y los servicios financieros (aproximadamente el 5%); (43%), Hotel & Travel (que oscila entre el 10% y el 20%) y Servicios Financieros (alrededor del 12%) 103. En general, se ha evaluado114 que el 73% de todas las organizaciones han sufrido un ataque DDoS, de las cuales el 85% han surgido múltiples ataques.

- En muchos casos, los ataques DDoS son "cortinas de humo" para otros tipos de ataques. Un estudio114 ha indicado que la infección por virus (alrededor del 46%), la activación de malware (alrededor del 37%), el compromiso de la red (alrededor del 25%), la pérdida de confianza del cliente (aproximadamente 23%) y el robo de datos del cliente %) Son los cinco principales objetivos detrás del ataque DDoS.

- Dado el nivel de atención que los ataques DDoS han alcanzado en el otoño de 2016, tanto el gobierno de los EE.UU.115 como el EU116 han anunciado / canalizado actividades relacionadas con niveles mínimos de seguridad para dispositivos / dispositivos IoT que pueden estar conectados a Internet. Dado el impacto de estos ataques DDoS, se espera que el tema atraiga la atención de más actores gubernamentales / públicos.

## 3.6.2. SECUESTRO DE LOS DATOS: RANSOMWARE

El ransomware ha vivido una explosión en 2016, convirtiéndose en la principal amenaza de ciberseguridad para usuarios y empresas. Es ya el malware más rentable de la historia, con beneficios que se doblan año tras año. Es también el malware que más evoluciona en todos los aspectos: número de campañas, de víctimas, precio del rescate, métodos de infección usados, importancia del daño causado y beneficios para los cibercriminales.

Un ransomware es, dice la Wikipedia[75], "un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción". La mayoría de ransomware en la actualidad cifran los archivos del sistema operativo para dejar el dispositivo inoperativo.

Este ataque ha vivido un incremento del 267%, con la aparición de 400 nuevas variantes en 2016[76] y 62 nuevas familias. Un fabricante tan bregado en el mundo del malware como Kaspersky, no ha dudado en calificar de "inquietante" el ratio de aparición de nuevos especímenes.[77]

En España en 2016 se denunciaron 1.700 casos de ransomware. Si se hubiesen pagado todos los rescates, habrían representado unos beneficios de 740.000 euros para los criminales. Pero el número real de casos es mucho más elevado de los que se denuncian, pudiendo multiplicarse tranquilamente por diez.[78]

La impunidad con la que actúan los criminales del ransomware sufrió un revés en febrero de 2016 cuando la justicia española condenó a seis años de cárcel al autor del primer tipo de ransomware que empezó a actuar en España, conocido como el "Virus de la Policía". El resto de su banda tuvo penas de entre seis meses y tres años de cárcel. El "Virus de la Policía" actuaba en España desde 2012 y pedía un rescate, para desbloquear el ordenador, de 100 euros.[79]

A nivel mundial, los principales países víctimas del ransomware fueron Estados Unidos (28%), Canadá (16%), Australia (11%) y la India (9%) (ENISA Threat Landscape Report 2016). En Latinoamérica, Brasil, México y Perú son los países que registraron más ataques.[80]

75 https://es.wikipedia.org/wiki/Ransomware

76 https://blog.malwarebytes.com/malwarebytes-news/2017/02/2016-state-of-malware-report

77 https://securelist.com/analysis/kaspersky-security-bulletin/76858/kaspersky-security-bulletin-2016-executive-summary

78 http://www.elmundo.es/economia/2017/01/08/586fc1d222601d6f4b8b4584.html

79 http://www.elmundo.es/espana/2016/02/29/56d48bfc22601d6c5f8b4581.html

80 https://www.symantec.com/es/mx/security_response/publications/threatreport.jsp

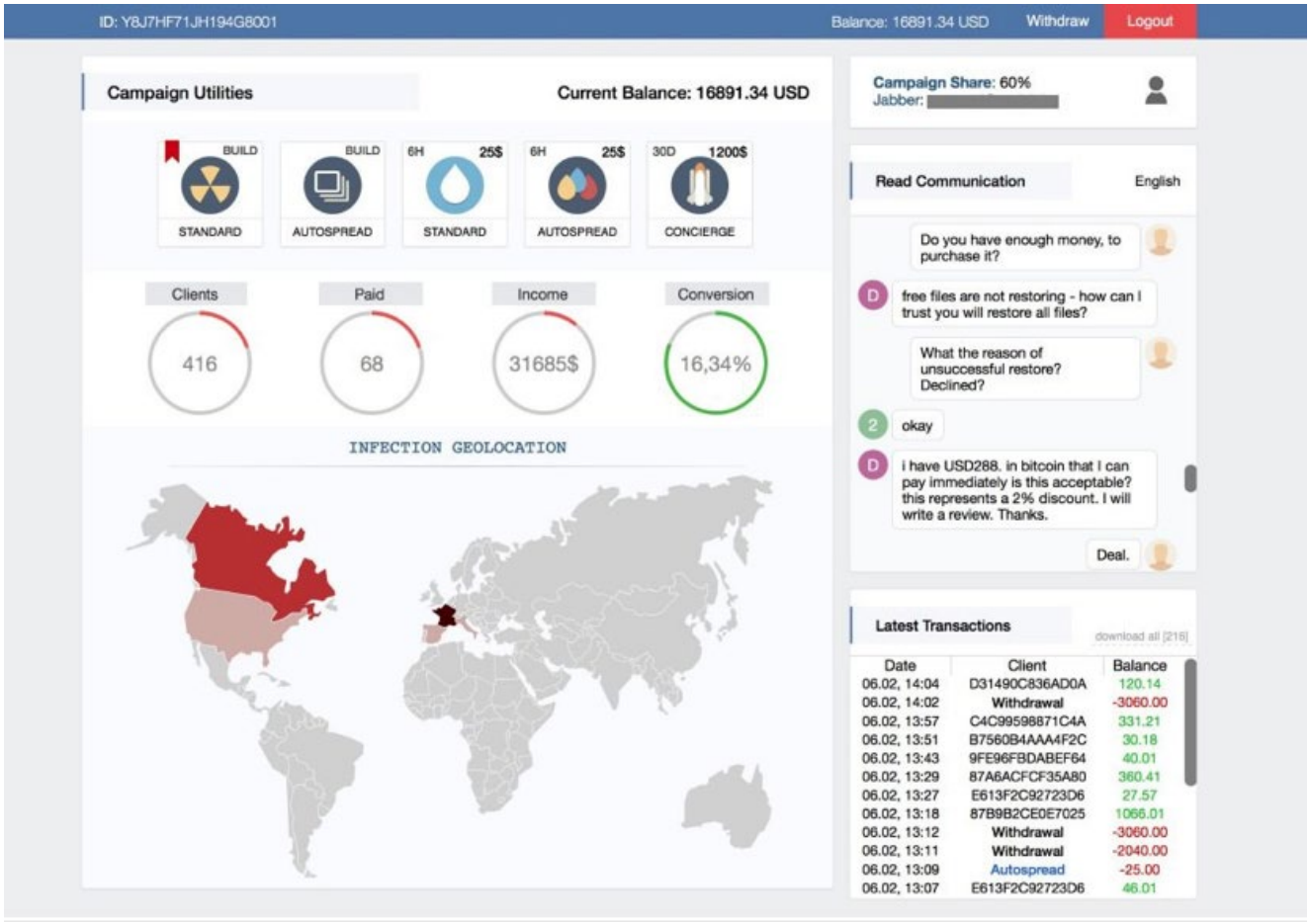


**Figure 14:** Distribución geográfica de los dispositivos IoT usados en el ataque Mirai en España y LatAm-Caribe.

Las víctimas siguen siendo mayoritariamente usuarios domésticos pero en 2016 ha habido un incremento importante de las infecciones en empresas, que pagan mayores rescates[81]. Las cifras varían según quien las presente. Kaspersky Labs asegura que sólo pertenecían al sector empresarial el 22,6% de usuarios víctimas de ranwomare en 2016[82]. En cambio, ENISA asegura las empresas coparían ya el 40% de infecciones, siendo las más afectadas las del sector servicios, seguidas a distancia por la manufactura, administración pública y el sector financiero y de seguros.[83]

El viraje del ransomware hacia el sector corporativo se ha traducido en la aparición de nuevas tácticas, como la usada por el ransomware Rakhni, que manda un documento .docx adjunto a departamentos de Relaciones Humanas de corporaciones en países de habla rusa. El documento simula ser una demanda de trabajo[84]. Algunas botnets grandes han empezado a mandar emails de phishing con documentos Office adjuntos, como Word o Excel, con Macros; scripts que simulan ser facturas y otro material habitual en los ámbitos empresariales[85].

81 https://www.fireeye.com/current-threats/what-is-cyber-security/ransomware.html

82 https://securelist.com/analysis/kaspersky-security-bulletin/76858/kaspersky-security-bulletin-2016-executive-summary

83 ENISA Threat Landscape Report 2016

84 https://securelist.com/analysis/kaspersky-security-bulletin/76858/kaspersky-security-bulletin-2016-executive-summary

85 https://blog.malwarebytes.com/malwarebytes-news/2017/02/2016-state-of-malware-report

Las principales puertas de entrada del ransomware son el phishing mandado desde botnets dedicadas al spam y la publicidad maliciosa, aunque algunos han empezado a usar kits de exploit para aprovechar vulnerabilidades de los servidores y redes. Se espera que pronto cojan características de "gusanos", para autopropagarse cara a atacar a más empresas[86].

El ransomware más activo en 2016 ha sido el veterano CTB-Locker, seguido de Locky y TeslaCrypt[87]. Aunque la mayoría de nuevas versiones de ransomware son experimentos poco cualificados, otros como Locky, Cerber y CryptXXX se han convertido en importantes amenazas que conviven con los más veteranos.

La aparición de especímenes de poca calidad, incluso con errores gramaticales en las notas de rescate, es una muestra de que el éxito del ransomware no ha pasado desapercibido entre la criminalidad informática y está atrayendo a nuevos actores deseosos de dinero fácil que hasta ahora se dedicaban a otros tipos de fraude.

En cuanto al ransomware de calidad, su evolución ha sido fulgurante por los réditos económicos que aporta. Los criminales han iniciado una búsqueda más inteligente de víctimas que se ha traducido en el aumento de ataques a usuarios profesionales y empresas. Esto ha conllevado a su vez el uso de técnicas que hasta ahora sólo se usaban para cibercrimen de alto nivel, como el phishing focalizado o "spear phishing", el cifrado fuerte, la gestión de claves, las formas de evadir la detección y otros[88].

Se ha evolucionado también en técnicas de infección, que usan todo tipo de infraestructuras para la propagación, desde botnets de spam y exploit kits (aprovechando básicamente vulnerabilidades de Adobe Flash)[89] hasta descargas inducidas o USBs infectados[90]. Muchos ransomware han implementado mejoras funcionales destinadas a provocar más daño, como cifrar también las copias de seguridad, o atacar a tipos concretos de archivos (de bases de datos, fiscales, páginas web)[91].

En cuanto a la razón última del ransomware, el rescate, la cantidad media exigida en 2016 ha sido de 600-700 dólares, lo que supone un incremento del 100% respecto al año anterior. Se estima que sólo en Estados Unidos las pérdidas este año rondan los mil millones de dólares[92]. La evolución del ransomware ha incluido también aplicar nuevos métodos para incrementar el rescate si el usuario tarda en pagar. También han cambiado los métodos de comunicación con las víctimas para mejorar la negociación del rescate, por ejemplo, usando comunicación por mail y no por ventanas.

Por último, una tendencia que ha empezado a verse en 2016 y que conlleva peligros importantes es la aparición del "ransomware-como-servicio". Este tipo de oferta tiene mucha aceptación, especialmente por los precios: 40 dólares por una licencia de ransomware[93].

**Vectores de mitigación**

• Hacer copias de seguridad en dispositivos que no estén conectados a la red porque, si así fuera, correrían el riesgo de que su información también fura cifrada en un ataque de ransomware.

• Usar antivirus y cortafuegos y tenerlos actualizados y bien configurados.

• Usar un programa específico contra el ransomware, como Anti Ransom[94].

• Evitar abrir mensajes de desconocidos, aunque parezcan de una persona conocida con una dirección nueva.

• No pinchar enlaces en mensajes sino teclearlos a mano en el navegador.

• Evitar visitar páginas web desconocidas.

• En caso de infección, no pagar el rescate. Nadie nos asegura la recuperación de los archivos perdidos.

86 http://www.cisco.com/c/m/es_es/offers/sc04/2016-midyear-cybersecurity-report/index.html

87 https://securelist.com/analysis/kaspersky-security-bulletin/76858/kaspersky-security-bulletin-2016-executive-summary

88 https://www.symantec.com/es/mx/security_response/publications/threatreport.jsp

89 http://www.cisco.com/c/m/es_es/offers/sc04/2016-midyear-cybersecurity-report/index.html

90 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-the-reign-of-ransomware.pdf

91 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf

92 https://www.symantec.com/es/mx/security_response/publications/threatreport.jsp

93 http://securityaffairs.co/wordpress/49362/breaking-news/stampado-ransomware.html

94 http://www.securitybydefault.com/2016/06/anti-ransom-v3.html

## 3.6.3. HACKTIVISMO

El hacktivismo se convierte, años tras año, en un peligro mayor para las organizaciones. El hacktivismo ya es la principal amenaza externa en ciberseguridad para las organizaciones (17%), sólo superada por los cibercriminales (44%). Detrás vienen el ciberterrorismo (15%), los ataques gubernamentales (12%) y la competencia (11%)[95]. Prueba del creciente protagonismo del hacktivismo son las múltiples veces que ha copado las portadas de los medios de comunicación en 2016, básicamente por filtraciones de datos y ataques DdoS, sus principales armas.

La celebración de los Juegos Olímpicos en Brasil fue el evento de 2016 que congregó más ataques hacktivistas en Latinoamérica, buscando la notoriedad que les ofrecía ser un país que estaba siendo mirado por todo el mundo. El hacker argelino conocido como "Red Hell Sofyan" modificó en junio la portada del sitio web oficial de la compañía de telecomunicaciones brasileña Oi y buena parte de sus subdominios. El hacktivista dejó un mensaje de apoyo a Palestina.[96]

Pero la mayoría de ataques se concentraron durante los Juegos Olímpicos de Brasil y fueron orquestados por la organización hacktivista Anonymous, en protesta contra el evento. El 5 de agosto, día en que se inauguraban los Juegos, Anonymous Brasil tiró mediante un importante ataque de Denegación de Servicio (DDoS) diversos sitios web del gobierno de aquel país, entre ellos el sitio oficial del gobierno federal para los Juegos del 2016, el portal del Gobierno Estatal de Río de Janeiro, el Ministerio de Deportes, el Comité Olímpico de Brasil y el sitio oficial de los Juegos Olímpicos de Río 2016.[97]

En la segunda fase de aquella operación, bautizada como #OpOlympicHacking, Anonymous Brasil filtró diversos documentos con detalles personales del alcalde y el gobernador de Río de Janeiro, el Ministro de Deportes, el Presidente del Comité Olímpico Brasileño y tres hombres de negocios involucrados en casos de corrupción. Diez días después el mismo grupo filtró bases de datos de los Servicios Olímpicos de Radiodifusión[98].

Anonymous Brasil fue especialmente activo en 2016, protagonizando también ataques que no tuvieron que ver con los Juegos Olímpicos: el 20 de julio lanzaron un bombardeo DDoS contra el sitio web de la corte judicial de Río que prohibió el uso del sistema de mensajería WhatsApp en todo el país, decisión que fue ampliamente comentada en el mundo entero.[99]

Otra operación de Anonymous que tocó a países hispanohablantes fue la #OpIcarus, orquestada para atacar los bancos de todo el planeta. Fueron afectados el Banco Central de la República Dominicana, el Banco Central de las Maldivas, el Banco Nacional de Panamá y el Banco Central de México.[100]

95 http://dtr.thalesesecurity.com/

96 https://www.hackread.com/brazilian-telecom-giant-oi-websites-hacked

97 https://www.hackread.com/anonymous-ddos-brazilian-government-websites/

98 https://www.hackread.com/anonymous-ddos-brazilian-government-website96 https://www.hackread.com/brazilian-telecom-giant-oi-websites-hacked

99 http://news.softpedia.com/news/anonymous-launches-ddos-attack-against-rio-court-that-blocked-whatsapp-in-brazil-506468.shtml

100 http://www.ibtimes.co.uk/op-icarus-anonymous-launches-ddos-attacks-8-international-banks-1558987


**Figura 16:** Defacement de la Cámara de Comercio de Madrid

A diferencia de Latinoamérica, donde los ataques DDoS han sido los protagonistas, en España lo han sido las filtraciones de bases de dados. De especial importancia fue este año la publicación en Internet de gran cantidad de datos personales de miembros de las fuerzas de la ley: el hacker Phineas Fisher, actuando por primera vez en España, hizo públicos datos de 5.540 policías de Catalunya (Mossos d'Esquadra)[101]. Dos semanas después, el grupo @FkPoliceAnonOps hizo lo mismo con datos de 5.446 miembros de la Policía Nacional.[102]

La facción española de Anonymous también se prodigó en el asalto a bases de datos: en febrero filtraron listados de patrocinadores y donaciones realizadas por el Corte Inglés a entidades públicas y privadas[103], y en diciembre accedieron a datos de la Cámara de Comercio de Madrid[104]. Anonymous se declaró también responsable de ataques DDoS en febrero contra el grupo de atracciones turísticas Loro Parque, tan fuertes que habrían provocado graves daños en la red de Vodafone Ono y puesto en peligro las conexiones del archipiélago canario con la península.[105]

En cuanto a las filtraciones de bases de datos en Latinoamérica por parte de grupos hacktivistas, destacaron internacionalmente algunas de ellas: en enero de 2016, en nombre de la operación #OpPuraVida contra el Tratado de Libre Comercio entre Estados Unidos, Centroamérica y República Dominicana, alguien bajo el apodo Hanom1960 filtró bases de datos de los ministerios de educación e información de Colombia.[106]

En febrero, en Bolivia, un grupo de hackers entró en los servidores de correo del ejército, descargó emails y filtró algunos de ellos en Internet[107]. También en febrero, un grupo de hacktivistas chilenos entró en las bases de datos de la Corporación Nacional de Desarrollo Indígena y robó datos personales de más de 300.000 ciudadanos a la espera de ayudas del gobierno.[108]

101 https://www.helpnetsecurity.com/2016/05/20/phineas-fisher-records-latest-attack/

102 https://www.hackread.com/anonymous-hacks-spanish-police-against-gag-law/

103 http://www.naciodigital.cat/noticia/102592/anonymous/filtra/totes/despeses/corte/ingl

104 http://www.elconfidencial.com/tecnologia/2016-12-21/anonymous-hackers-camara-comercio-madrid_1307801/

105 http://www.laopinion.es/canarias/2016/02/12/ataque-anonymous-loro-parque-puso/655546.html

106 https://ghostbin.com/paste/mbjqa

107 http://news.softpedia.com/news/hackers-breach-bolivian-army-email-servers-500233.shtml

108 http://news.softpedia.com/news/hacktivists-leak-details-for-300-000-chilean-citizens-looking-for-state-benefits-500232.shtml

# 4. CONCLUSIONES

Si las principales explosiones de este año han sido el "ransomware" y el ataque al CEO, todos los expertos dan por seguro que la del año que viene será la "Internet de las Cosas", o lo que es peor "sistemas de control industrial", que no dejan de ser "cosas" con las que se controlan servicios esenciales para la Sociedad. Lo hemos visto ya en 2016 pero se afianzará en 2017, con un incremento del 100%, a medida que la cibercriminalidad dé con nuevas herramientas y usos, además de los ataques de DDoS, para estos millones de dispositivos. Instituciones y empresas están mejorando mucho en su protección informática, pero seguirá habiendo un cabo suelto: el usuario, víctima perfecta del "phising", un ataque para el que no pasan los años.

El gobierno de Alemania prohibía recientemente la venta de una muñeca conectada a Internet, por el potencial peligro de que pueda espiar lo que dicen los niños y mandarlo a terceros. Días después, se descubría que alguien había hackeado la base de datos de unos muñecos llamados CloudPets: padres y niños podían grabar mensajes y guardarlos en esta base de datos, totalmente insegura. Estos muñecos son la avanzadilla de los peligros nada pueriles de la Internet de las Cosas. Peligros que empezamos a intuir en 2016 pero marcarán definitivamente la agenda en ciberseguridad de 2017.

La unión de una muy insegura Internet de las Cosas con unos a veces más inseguros sistemas de ciberseguridad industrial e infraestructuras críticas puede dar lugar a un cóctel explosivo de dimensiones desconocidas, que es actualmente una de las principales preocupaciones de los expertos en ciberseguridad. Al haber cada vez más sistemas conectados e interconectados, se multiplican exponencialmente los ataques y las vulnerabilidades, creadas por fabricantes no bregados en ciberseguridad.

El resultado son situaciones muy complicadas, como las vividas en 2016 cuando la delincuencia ha unido dos "trending topics" en ciberseguridad como son las infraestructuras críticas y el "ransomware", dando lugar a más de un hospital obligado a dejar de operar durante 24 horas, porque un virus había cifrado sus principales archivos. La cada vez mayor complejidad de la ciberseguridad se muestra en ataques como estos, donde una delincuencia informática muy a la vanguardia entrelaza amenazas, dispuesta a aunar las armas más peligrosas para robar cada vez más datos y dinero. Una delincuencia totalmente por delante de las medidas de defensa del empresariado medio y la ciudadanía

Conociendo esto, el nuevo año se nos presenta imprevisible, tal como lo ha sido 2016 a partir de que fuimos confrontados con espectaculares ataques como la Denegación de Servicio que tumbó al mega-proveedor estadounidense Dyn, afectando la estabilidad de clientes como Twitter, Spotify y Reddit. Lo imprevisible de este bombardeo fueron las armas con que se realizó, que multiplicaron su poder: dispositivos de la Internet de

las Cosas con contraseñas por defecto.

En 2016 hemos visto también el recrudecimiento de ataques que arrastramos ya desde 2015, 2014 e incluso antes. Ataques que no paran de aumentar y así seguirán, muy posiblemente, en 2017. Un buen ejemplo es el phishing, que aumentó en 2016 un 25%. El phishing, veterano engaño donde los haya y base de cada vez más ataques, se nutre de nuestra ignorancia e inocencia para "colarnos" mensajes de correo falsos que infectan nuestros ordenadores, nos roban las contraseñas e incluso ordenan a nuestro contable una transferencia millonaria a la cuenta de las "ciber-mafias".

Las empresas se han visto en 2016 más rodeadas que nunca. Por ataques como el mencionado, llamado "Fraude al CEO", que obliga con engaños al contable a hacer transferencias fraudulentas, que provocan pérdidas de 600.000€ de media anual a las empresas atacadas. También el "ransomware", esos virus que cifran todo lo que haya en nuestro disco duro para pedirnos un rescate por recuperarlo, han empezado este año a cebarse en las empresas (PyME), que tienen más dinero y cuya producción depende de que funcionen los ordenadores. 2017 será definitivamente el año en que el "ransomware" tomará por asalto a las organizaciones, desde corporaciones hasta la empresa más pequeña.

Otra tendencia que seguirá al alza en 2017 será el robo de ese nuevo "oro líquido" que son los datos y su comercio para la minería de datos, inteligencia artificial y otros usos dirigidos a mejorar la manipulación de las masas. Las bases de datos, donde se guardan los datos como en los bancos se guarda el dinero, han seguido siendo en 2016 objeto de robos, la mayoría desconocidos porque entre el 80 y el 90% de estos robos no se declaran.

Esto nos lleva al gran reto para 2017: la creación de legislaciones que pongan un poco de orden y permitan a la ciudadanía estar informada si sus proveedores de servicios sufren algún daño que les afecte. España trabaja siguiendo básicamente las directrices europeas. En Latinoamérica, solo seis países (Brasil, Jamaica, Uruguay, Panamá, Trinidad y Tobago, Colombia y Panamá) tienen algún tipo de legislación relacionada con seguridad cibernética.

Es importante resaltar que el "Informe sobre Ciberseguridad en América Latina y el Caribe" constata que cuatro de cada cinco países de la zona no presentan estrategias en materia de ciberseguridad, como planes de seguridad online y de protección de las infraestructuras críticas, dos de cada tres países no tienen ningún centro de comando y control de seguridad cibernética y la gran mayoría de ministerios carece de capacidad para hacer frente a los delitos cibernéticos. 2017 deberá ser el año en que los gobiernos aborden de forma más seria y exhaustiva esta realidad que se nos viene encima.

viu | Universidad Internacional de Valencia

Síguenos en:

www.viu.es