INFORME TRIMESTRAL PANDALABS T1 2017

panda

pandalabs

1. INTRODUCCIÓN

1 Introducción

Internet es ya, por definición, la Red de redes; una maquinaria descentralizada de información, almacenamiento y compartición de datos. Su capacidad va más allá de cualquier fenómeno que hayamos visto en la historia y, a pesar de lo revolucionario de este fenómeno global y de sus ventajas, Internet es una ingobernable fuente de sobresaltos para instituciones, empresas y particulares.

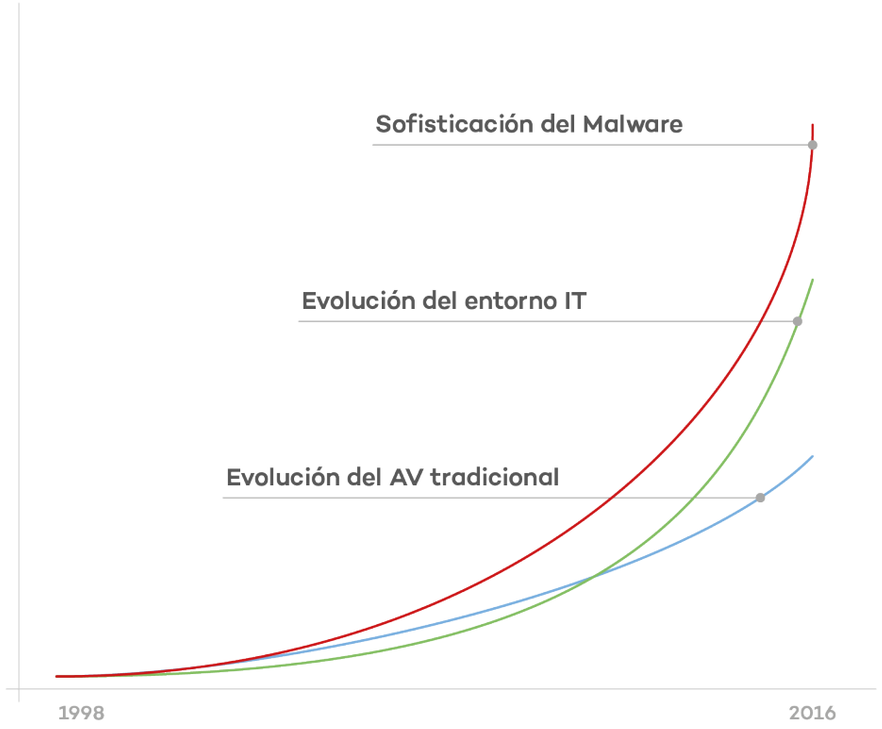
En el primer trimestre de 2017 hemos visto algunas de las consecuencias de un mundo con cada vez más sistemas que controlan todo tipo de instalaciones y procesos industriales conectados a internet, la mayoría de ellos sin protección.

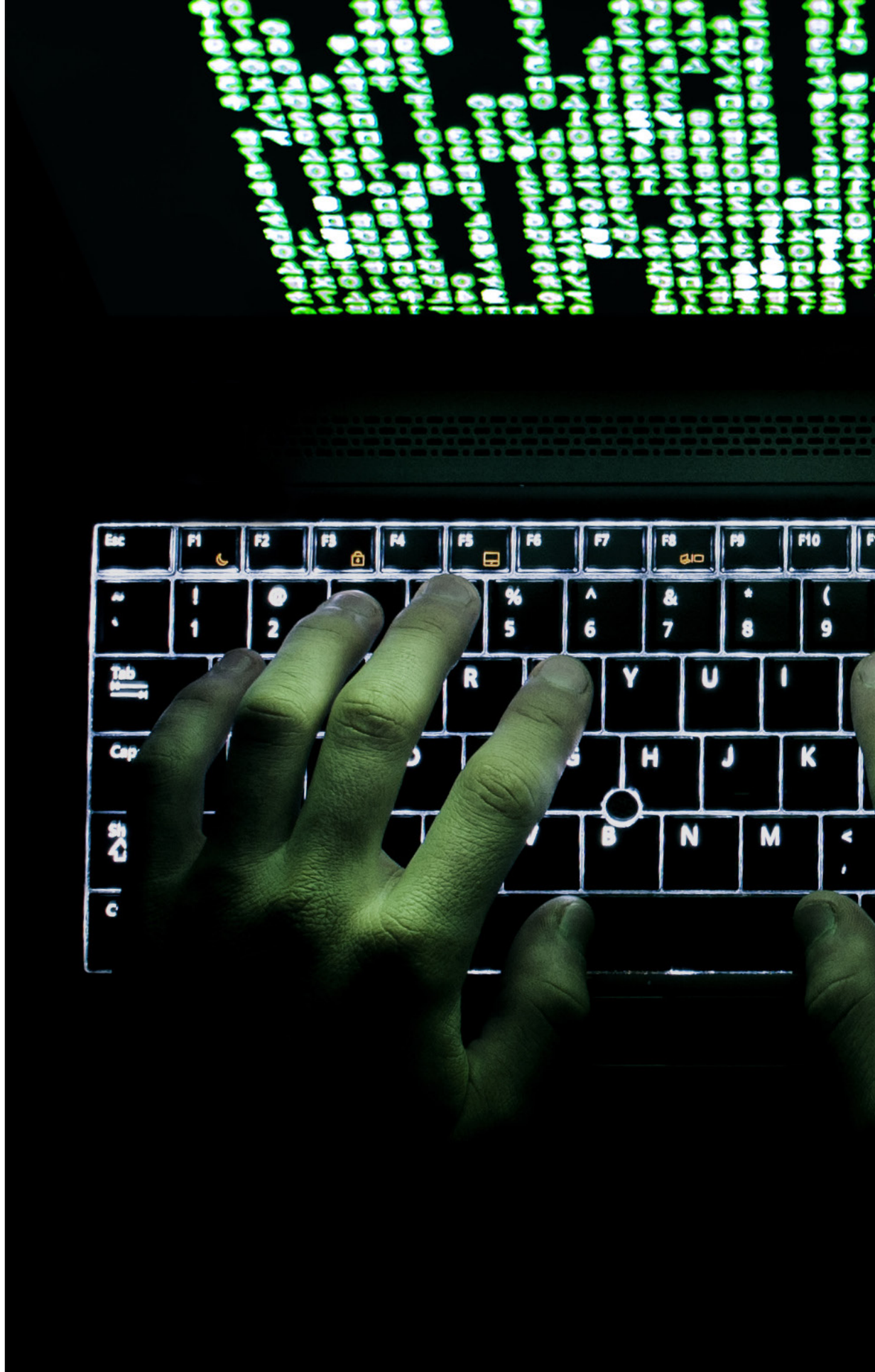
Hay más ciberataques y son más complejos; su evolución hace necesario anticiparse a los comportamientos maliciosos. Con los datos recopilados en los primeros meses del año hemos podido detectar los 3 factores del éxito de los ciberatacantes:

- Amenazas más sofisticadas, nuevos vectores de ataque y más cantidad de ofensivas.
- Entornos IT más complejos, con superpoblación de dispositivos, sistemas y conexiones.
- Los antivirus tradicionales, evolucionan pero mucho más despacio.

Si hay alguna tendencia a destacar en este entorno es el aumento de ataques personalizados a los que se tienen que enfrentar las empresas. Ahora, los atacantes interactúan en tiempo real con la red de la víctima y las defensas que están desplegadas, adaptándose a las mismas para poder conseguir su objetivo.

En estos primeros meses del año la sorpresa llega desde el Internet de las Cosas (IoT) con los televisores inteligentes- Smart TVS- como protagonistas. Hemos sido testigos de infecciones de ransomware en televisores LG con sistema operativo Android y por primera vez se ha demostrado cómo se pueden comprometer Smart TVs de forma remota a través de la señal TDT.





2. ANÁLISIS DE ATAQUES

2 Análisis de ataques

Tanto en nuestros informes como en los del resto de fabricantes de soluciones de seguridad solemos encontrar el mismo tipo de cifras sobre malware: cuánto malware nuevo ha aparecido en un periodo de tiempo ,tipos de malware, etc. Aunque estas cifras son interesantes y consiguen grandes titulares, desde PandaLabs nos hemos preguntado qué podríamos mostrar para medir los riesgos reales de infección a los que se enfrentan los usuarios, tanto en entornos domésticos como corporativos. Datos que aporten un valor añadido real.

Para conseguir datos que aporten un valor real añadido nos centramos en lo que tienen que enfrentarse todos nuestros clientes. En primer lugar, decidimos no contar ninguna detección de todo el malware que detectamos por firmas (hablamos de cientos de millones) ya que se trata de malware conocido y del que, en mayor o menos medida, todo usuario con un antivirus básico está protegido. Por otro lado, también decidimos no incluir las detecciones heurísticas, que son capaces de detectar malware que no se conoce previamente.

El razonamiento para tomar esta decisión es que los atacantes profesionales se aseguran de hacer unas pruebas mínimas con los motores antivirus para cerciorarse de que sus nuevas muestras de malware no son detectadas, y estos motores incluyen detecciones tanto de firmas como heurísticas. Es decir, podemos dar por descontadas estas cifras, ya que los usuarios estaban en todo momento protegidos y no corrían riesgo real de infección. Pero si no contamos lo que sí detectamos… ¿qué datos podemos sacar?

En Panda Security desde siempre nos ha obsesionado la protección del cliente, así que desde el laboratorio hace unos pocos años creamos una capa de protección que decidimos añadir a todas nuestras soluciones. Esta sólo se pone en

marcha cuando todas las demás capas de protección fallan, de esta forma sabemos que todo lo que allí paramos son ataques completamente nuevos.

De esta manera no sólo contamos los ataques protagonizados por malware, sino que también se añaden ataques sin fichero (fileless) o aquellos realizados a través del abuso de herramientas legítimas del sistema, algo cada vez más habitual en entornos corporativos.

Esta capa extra es la que nos ha permitido tener unos ratios de detección excelentes en todos los test llevados a cabo con una metodología que imita los ataques tal y como suceden en el mundo real. En los tests llevados a cabo por AV-Comparatives en el primer trimestre de 2017 podéis ver cómo en el Real-World Test tests, tenemos un 100% de detección en las 2 pruebas realizadas, y en el Malware Protection Test obtenemos el máximo galardón, con un 99,89% de ratio de detección y 1 falso positivo, por delante de todos nuestros competidores.

De todas las máquinas protegidas por alguna solución de Panda Security, el 2,25% de ellas ha sufrido ataques de amenazas desconocidas.

Si miramos por tipo de cliente, los usuarios domésticos tienen un 2,19% de ataques mientras que en el caso de empresas la cifra es del 2,45%. Si bien puede parecer algo contra-intuitivo, ya que las empresas cuentan con muchas más defensas que los ordenadores domésticos conectados directamente a Internet, hay que recordar que estamos hablando de ataques más profesionales y las corporaciones poseen información es infinitamente más valiosa que la que posee un PC doméstico.

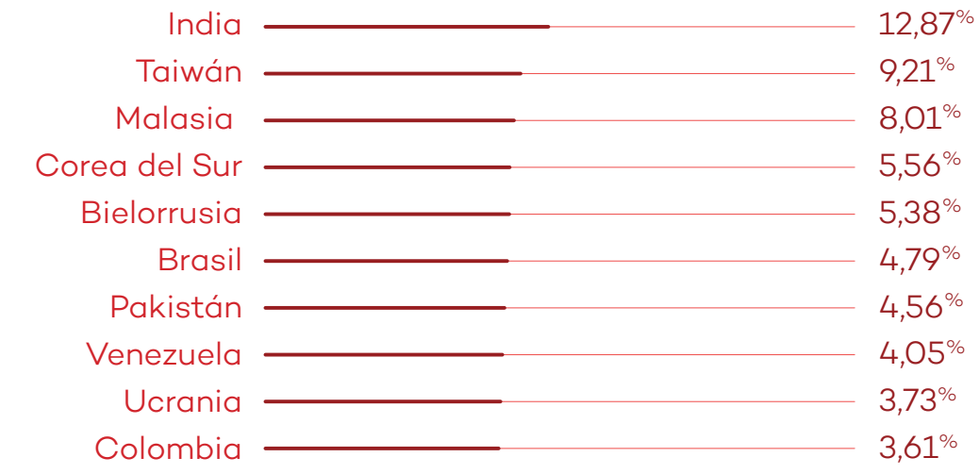
Dentro de nuestros clientes corporativos tenemos aquellos que utilizan soluciones tradicionales y los que optan por nuestra solución EDR (llamada Adaptive Defense), que va mucho más allá de un antivirus y ofrece funcionalidades extra, niveles de protección mucho más amplios, clasificación y monitorización en tiempo real de todos los procesos que se ejecutan en servidores y estaciones de todo el parque, análisis forenses, etc.

Parece lógico que el nº de ataques que consiguen saltarse todas las capas de protección en Adaptive Defense de EDR sean mucho menores que aquellos que se tienen que enfrentar sólo con tecnologías tradicionales. Tiene sentido, ¿pero es realmente así?

Bien, el 2,83% de las máquinas protegidas por soluciones tradicionales reciben ataques de amenazas desconocidas, mientras que esa cifra en aquellas protegidas por nuestras soluciones de nueva generación baja hasta el 0,83%.

¿Cómo se reparten a nivel geográfico? Hemos calculado el porcentaje de máquinas atacadas en cada país. A, mayor porcentaje mayor probabilidad de sufrir un ataque de nuevas amenazas si utilizamos ordenadores en esos países.

PAÍSES CON MAYOR ÍNDICE DE INFECCIÓN EN ESTE TRIMESTRE



Asia y Latinoamérica son las regiones con mayores infecciones. A continuación podemos ver los 10 países con menor índice de infección:

PAÍSES CON MENOR ÍNDICE DE INFECCIÓN EN ESTE TRIMESTRE

El resto de países con un porcentaje menor a la media mundial son Bélgica (1,04%), Canada (1,12%), Letonia (1,19%), Alemania (1,20%), España (1,27%), Reino Unido (1,29%), Australia (1,30%), and Eslovaquia (1,31%).

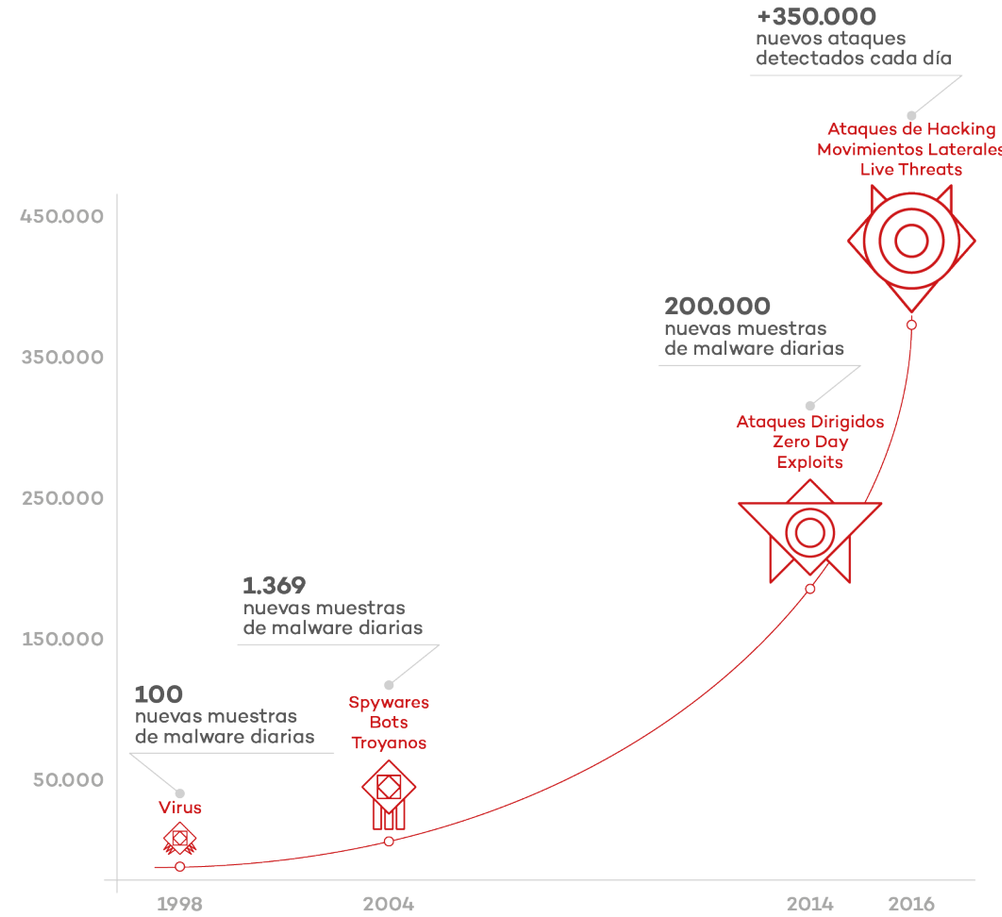
3. LA REEVOLUCIÓN DE LAS AMENAZAS

3

La reEvolución de las amenazas

¿Estamos ante una revolución de las amenazas? Parece ser que sí. El malware es cada vez más sofisticado y las técnicas de ataque están evolucionando: el objetivo no es seleccionado al azar, los ataques son dirigidos, coordinados y utilizan diferentes vectores.

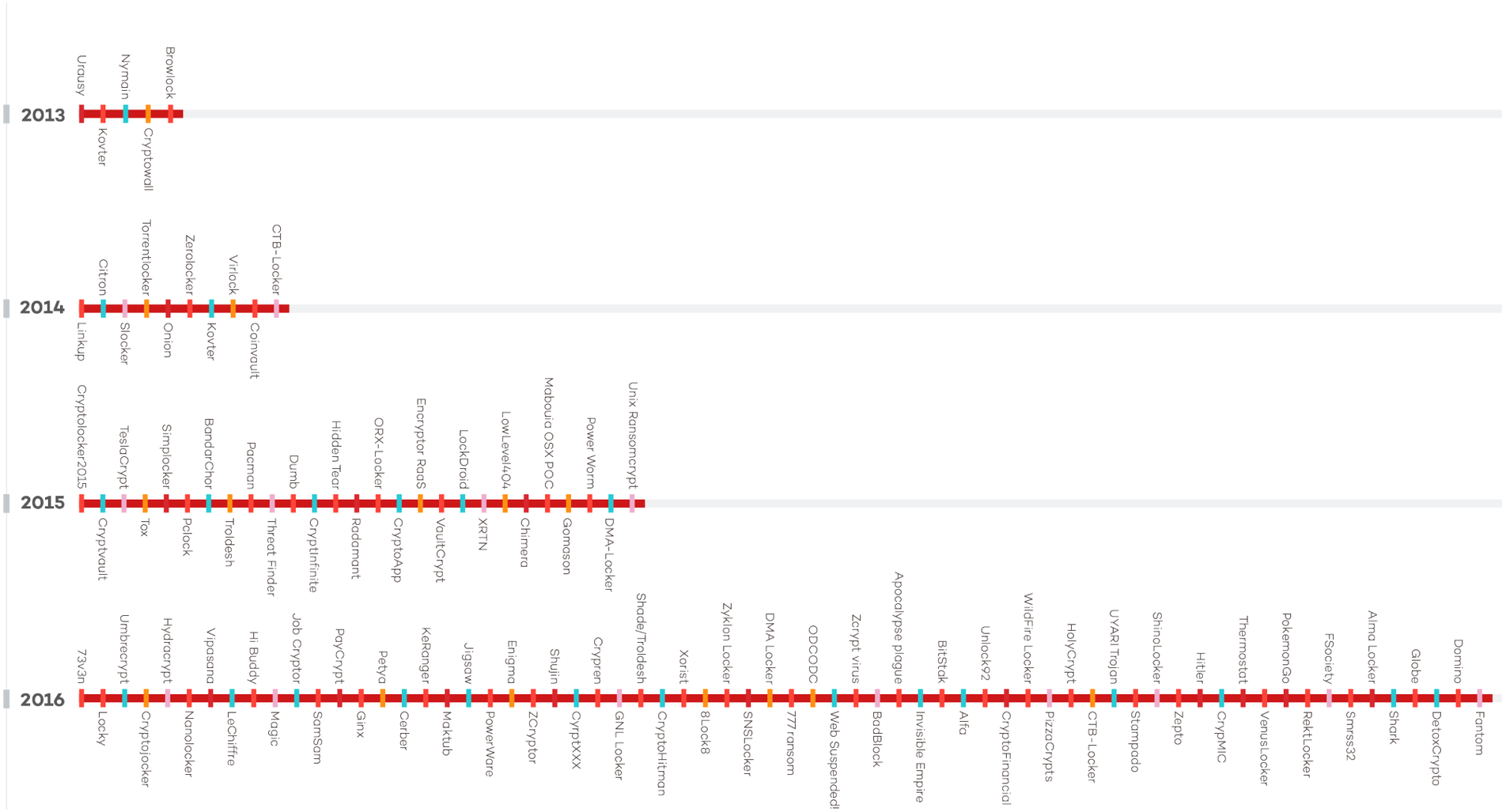
El móvil ahora ha cambiado y el interés del cibercriminal no reside en el reconocimiento personal, sino en el lucro económico.



pandalabs

La tendencia de los hacking attacks está a la cabeza y deriva en la profesionalización del cibercrimen. Ya en los últimos meses de 2016 analizamos la especialización de los Black Hat, tanto en el desarrollo de lo que podría denominarse Ransom as a Service (RaaS) como en la creación de empresas que ofrecen servicios de ataques DDoS, como Vdos, cuyos responsables habían lanzado150.000 ataques y obtenido un beneficio de 618.000$,.

Sin lugar a dudas, una industria billonaria en el último año:



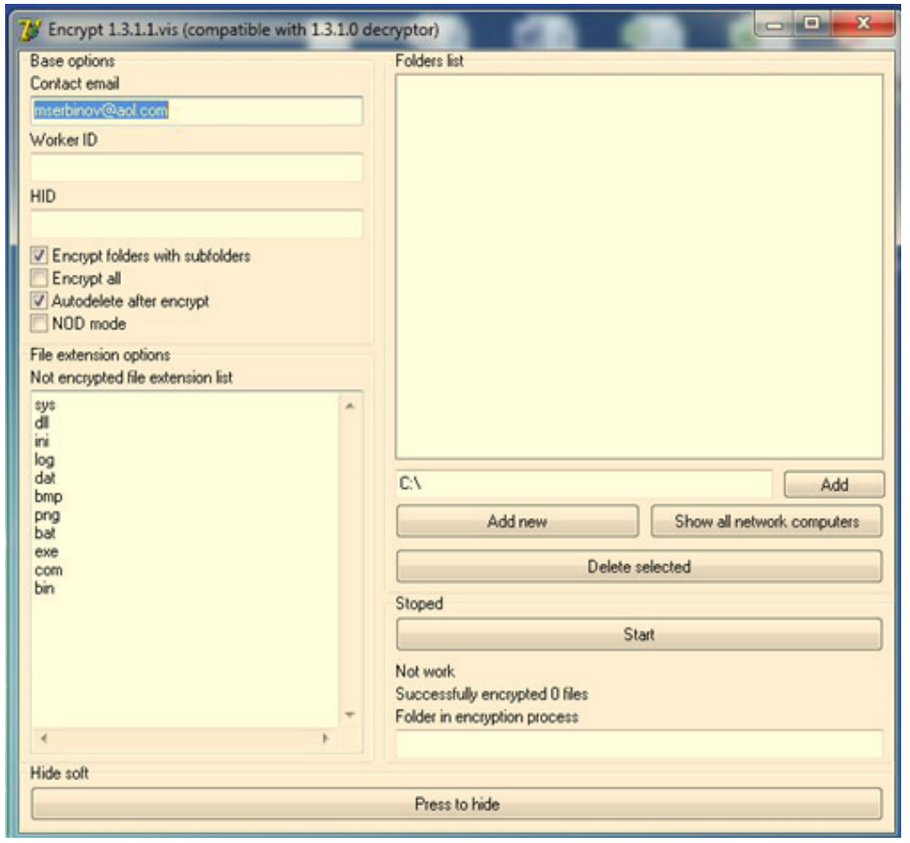
4. EL TRIMESTRE DE UN VISTAZO

Ransomware

Los ataques de ransomware siguen en auge y así seguirán mientras las víctimas paguen los cuantiosos rescates. Hay estimaciones que indican que durante 2016 los diferentes grupos de ciberdelincuentes que se dedican estos ataques cobraron mil millones de dólares. La preocupación es creciente en todos los ámbitos y hasta se están aprobando legislaciones específicas para luchar contra este tipo de delincuencia: en California ya es delito distribuir ransomware.

Sin embargo el que existan legislaciones no influye en que sigan los ataques y se creen nuevas familias de ransomware. Una de estas nuevas familias, Spora, comenzó a distribuirse nada más iniciarse el año, en este caso buscando sus víctimas principalmente en Rusia.

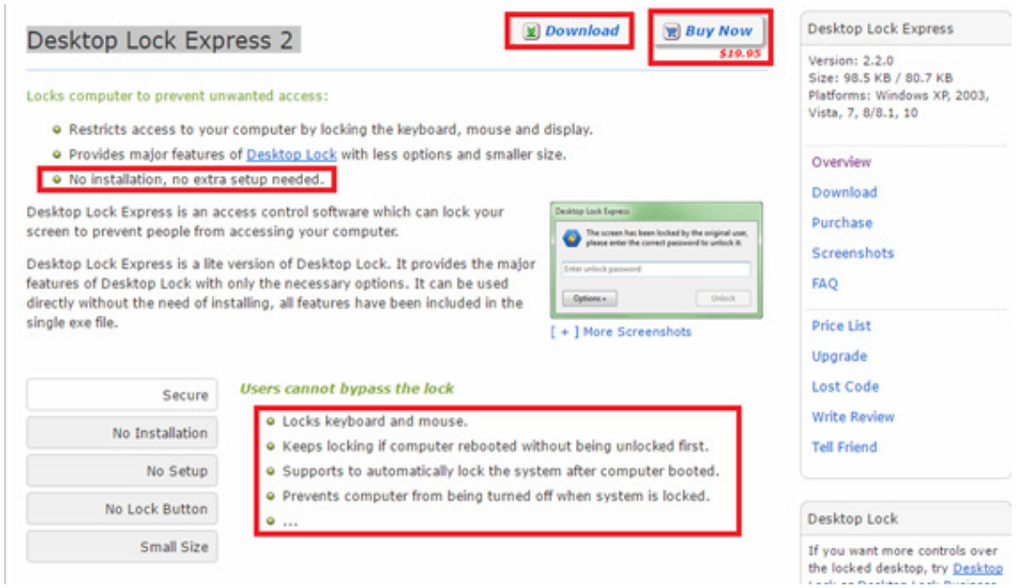
Los ataques dirigidos a empresas no dejan de crecer. A las archiconocidas familias de ransomware (Locky, Cerber, etc.) se le suman ataques más personalizados para este tipo de víctimas. Uno de ellos ha sido descubierto por PandaLabs este trimestre: se trata de un ransomware con interfaz propia –bautizado como WYSIWYE que permite al delincuente seleccionar las diferentes carpetas cuyo contenido se cifrará, los ordenadores de la red, auto-borrado, la dirección de email a la que deben dirigirse las víctimas, etc.:



Uno de los métodos más populares –y relativamente sencillos- de penetrar en una red corporativa es a través de ataques de fuerza bruta por el RDP, el popular Escritorio Remoto que viene con Windows. Los atacantes van escaneando Internet en busca de ordenadores que lo tienen activado y una vez encuentran una potencial víctima lanzan un ataque de fuerza hasta que dan con las credenciales correctas. Una vez dentro pueden hacer y deshacer a su antojo.

Durante estos primeros meses de 2017 hemos visto bastantes casos de atacantes de origen ruso. Todos ellos siguen un

esquema similar: una vez acceden al ordenador tras el ataque a través de RDP instalan software de minería de bitcoins –como método para obtener un beneficio añadido- y luego o bien cifran ficheros o bloquean el acceso al ordenador. No siempre utilizan malware para esto, por ejemplo, en uno de los casos que analizamos utilizaron la aplicación comercial "Desktop Lock Express 2" para llevar a cabo el bloqueo del ordenador:



Especialmente cruel ha sido el "software" malicioso llamado Popcorn Time. La novedad reside en el morboso modo de propagación, ya que pretende que las víctimas colaboren con el ciberdelincuente para infectar a nuevos usuarios. Aparte de reclamar a la víctima el pago de un bitcoin (unos 800 euros) por devolverle el control de los archivos que ha cifrado, le ofrece la posibilidad de recuperarlo gratuitamente si contribuye a su propagación. De ahí que se diga que se propaga como un meme.

Las consecuencias inmediatas de un ataque de ransomware son claras, pierdes el acceso a tus ficheros. Sin embargo, los casos de secuestro digital pueden ir mucho más allá de esto, como pudieron comprobar los clientes de un hotel en Austria. que tras ser atacado por ciberdelincuentes éstos bloquearon las puertas de las habitaciones –imposibilitando su entrada- e inutilizaron el software de programación de las tarjetas de entrada a las habitaciones. Todo esto en la semana de apertura de la temporada, con 180 clientes con reserva. Los responsables del hotel decidieron pagar los 1.500€ y así pudieron recuperar el control de sus sistemas.

Cibercrimen

El negocio del cibercrimen está más profesionalizado que nunca, lo que significa que hay grupos especializados en diferentes aspectos del mismo: creación de malware y exploits, distribución del malware, robo de información, lavado de dinero, etc. Un ejemplo claro lo podemos ver con RDPatcher, un ataque descubierto por PandaLabs cuya finalidad es dejar el equipo de la víctima listo para ser alquilado al mejor postor. Una vez llegan al equipo los atacantes realizan un perfilado del mismo, recopilando todo tipo de datos de hardware, software instalado, velocidad de conexión, páginas web visitadas, etc.

Una vez hecho esto, lo dejan listo para ofrecerlo en el mercado negro.

Y es que el ingenio de los ciberdelincuentes parece no tener fin. Para evitar ser detectados, hemos visto como han optado por no usar malware para perpetrar sus ataques. En este caso descubierto por PandaLabs se ve cómo, tras llegar a un equipo, los atacantes dejan abierta una puerta trasera por la que

entrar al mismo sin tener que instalar malware con ayuda de las "Sticky keys".

Los ataques DDos también merecen ser mencionados. En la segunda mitad de 2016 hubo varios ataques de este tipo muy sonados y en este trimestre se han visto más ataques de este estilo, aunque no tan brutales. De hecho, nada más comenzar el año, clientes de Lloyds tuvieron problemas para acceder a sus cuentas online como consecuencia de un ataque DDoS lanzado contra la entidad.

La policía de Estado italiana desarmó en enero una central de ciberespionaje, bautizada como Eye Pyramid creada por dos hermanos italianos con el objetivo de controlar instituciones y administraciones públicas, estudios profesionales, empresarios y políticos. Esta red accedía a la información confidencial de los sujetos instalando un virus en los ordenadores, robando datos sensibles para las finanzas y la seguridad del Estado. Entre los afectados estarían los antiguos primeros ministros Matteo Renzi y Mario Monti, además del presidente del Banco Central Europeo, Mario Draghi, y otras personas poseedoras de información reservada. Alcaldes, cardenales, presidentes regionales, economistas, empresarios y policías completan la lista de víctimas.

El hackeo de cuentas de redes sociales es un habitual, y uno de los casos más llamativos de este trimestre sucedió en enero, cuando la cuenta de Twitter oficial de vídeos del New York Times fue comprometida. En cuanto recuperaron el control de la misma borraron los tweets que había publicado los atacantes:

This is an example of one of the tweets that was posted from the compromised account, claiming that Russia was about to launch an attack against the US:

El mismo grupo es conocido por haber hackeado otras cuentas de empresas como Netflix o Marvel.

Los robos de datos también han protagonizado titulares durante estos meses. Sanrio, la compañía propietaria de "Hello Kitty", vio como datos personales de 3,3 millones de sus clientes les habían sido robados. Entre la información sustraída estaban el nombre, apellido, nombre de usuario, fecha de nacimiento, preguntas de seguridad para recuperar la contraseña, etc.

Analizamos casos ciertamente irónicos como el de Cellebrite, compañía israelí que se dedica a facilitar el hackeo de teléfonos –más concretamente la extracción de información de los mismos-, la cual fue hackeada y le robaron 900Gb de datos. En esta información se encuentran datos de clientes, bases de datos e información técnica sobre los productos de la empresa.

Tampoco Apple ha escapado del cibercrimen en lo que va de año. Un grupo de ciberdelincuentes denominado "Turkish Crime Family" chantajeó a la compañía, pidiéndole un rescate si no quiere que borren remotamente los datos de los iPhones, iPads y Macs de 250 millones de usuarios. Si bien aparentemente este grupo tiene credenciales válidas de usuarios, Apple niega que haya sido comprometida y achaca el problema a la reutilización de credenciales y el hackeo de sitios de terceros. Por supuesto, el gigante tecnológico se ha negado a ceder al chantaje.

Móviles

Si bien la cantidad de nuevo malware creado para dispositivos móviles sigue siendo muy inferior al que vemos en PCs, siguen los mismos pasos. Por ejemplo con el ransomware, una técnica que está dando excelentes resultados a los delincuentes y que trasladan a este tipo de dispositivos. Un buen ejemplo es un nuevo malware para Android, conocido como "Charger", que tras ser instalado en el teléfono roba los contactos y mensajes de SMS. A continuación bloquea el terminal, solicitando un rescate o comenzarán a vender parte de tu información en el mercado negro cada 30 minutos. El rescate solicitado es de 0,2 bitcoins.

Internet of Things (IoT)

De un tiempo a esta parte, la mayoría de edificios se han ido adaptando para registrar el consumo eléctrico de hogares y oficinas mediante los 'smart meters' o contadores inteligentes. Más allá del posible efecto en la factura de la luz que algunas asociaciones de consumidores ya han denunciado, lo cierto es que la generalización de este tipo de aparatos entraña algunos riesgos menos conocidos en materia de seguridad.

Tal y como ha explicado el investigador Netanel Rubin durante la pasada edición del Chaos Communications Congress, celebrada en Hamburgo (Alemania), estos contadores suponen un peligro en varios frentes. En primer lugar, como registran todos los datos de consumo de hogares y oficinas para mandarlos a la compañía eléctrica, un atacante que lograra tomar el control podría ver la información y utilizarla con fines maliciosos. Por ejemplo, podría averiguar si la vivienda u oficina está vacía para perpetrar un robo. Incluso, dado que todo dispositivo electrónico deja un rastro en la red eléctrica, podrían detectar las variaciones para averiguar qué dispositivos de valor tendrán a su alcance cuando accedan al lugar.

Otro dispositivo cada vez más común es la Smart TV o televisión inteligente. Algunos utilizan versiones de Android como sistema operativo, lo que tiene sus ventajas y también sus inconvenientes, como pudo comprobar el desarrollador estadounidense Darren Cauthon cuando contaba en Twitter que el televisor de un miembro de su familia había sufrido uno de estos ataques. Según explicó Cauthon, todo sucedió después de que la víctima instalara una aplicación para ver películas en internet, al parecer desde un sitio de terceros.

Se trataba de un modelo de la marca LG, fabricado en el 2014, que funciona con Google TV, una versión de Android específica para televisores. Una vez hubo infectado el dispositivo, el 'software' malicioso pidió al afectado 500 dólares (unos 471 euros) por el desbloqueo en una pantalla que simulaba un aviso del Departamento de Justicia estadounidense.

Existen sin embargo ataques mucho más peligrosos, que pueden darnos una idea de lo que está por llegar en este terreno. En febrero, durante el European Broadcasting Union Media Cyber Security Seminar, fue mostrado el exploit creado por el consultor de seguridad Rafael Scheel, que permite tomar control de una Smart TV sin acceso físico a la misma, mandando el ataque a través de la señal TDT.

Robots y asistentes personales

La “cuarta revolución industrial” parece estar a la vuelta de la esquina. Un reciente informe del Foro Económico Mundial ha puesto cifras a un debate que lleva tiempo sobre la mesa: de aquí a 2020, desaparecerán 7,1 millones de puestos de trabajo en los países avanzados y se crearán 2,1 millones. Dicho de otro modo, se perderán 5 millones de empleos para siempre.

Otro informe reciente, en este caso de la Organización para la Cooperación y el Desarrollo Económico (OCDE), ha señalado a España, Austria y Alemania como los países a los que más afectará la evolución de la robótica. En concreto, este fenómeno hará que un 12% de los trabajadores de estos tres países se vean sustituidos por máquinas, frente a una media del 9% en el conjunto de la OCDE.

A raíz de estos datos el Parlamento Europeo ha elaborado un conjunto de normas para regular la relación entre robots, ciudadanos y empresas comunitarias. Ahora esta propuesta de marco legal deberá ser debatida por la Comisión Europea, que será quien decida finalmente si regula o no la implantación de los robots en la sociedad para minimizar los desajustes provocados por las máquinas.

En el mes de febrero, el comando de voz “Ok, Google” hizo que se activara el altavoz inteligente Google Home en el anuncio que el gigante de Mountain View presentó en la Super Bowl. Para sorpresa de muchos telespectadores, la orden hizo que los dispositivos de sus hogares también respondieran. De hecho, sus dotes para escuchar las conversaciones y almacenarlas hace que los asistentes virtuales puedan incluso ayudar a resolver crímenes. La policía de una localidad estadounidense ha pedido a Amazon que le permita acceder a la información de un Amazon Echo. El altavoz del gigante comercio electrónico podría haber guardado información sonora que ayude a esclarecer un crimen.

Ciberguerra

Más que nunca los ciberataques y la política están relacionados. Tras la resaca de las elecciones estadounidenses del pasado año, las acusaciones de ciberataques de EEUU a Rusia han dado paso a sanciones. Antes de abandonar su cargo, Obama anunció sanciones al país acusándolo de orquestar ataques informáticos para dañar la campaña de la demócrata Hillary Clinton y favorecer a Donald Trump, expulsando a 35 diplomáticos rusos y cerrando 2 centros propiedad del Gobierno ruso.

Todo esto ha tenido repercusión en otros países del mundo. En Francia, por ejemplo, han descartado el uso del voto electrónico por parte de sus ciudadanos residentes en el

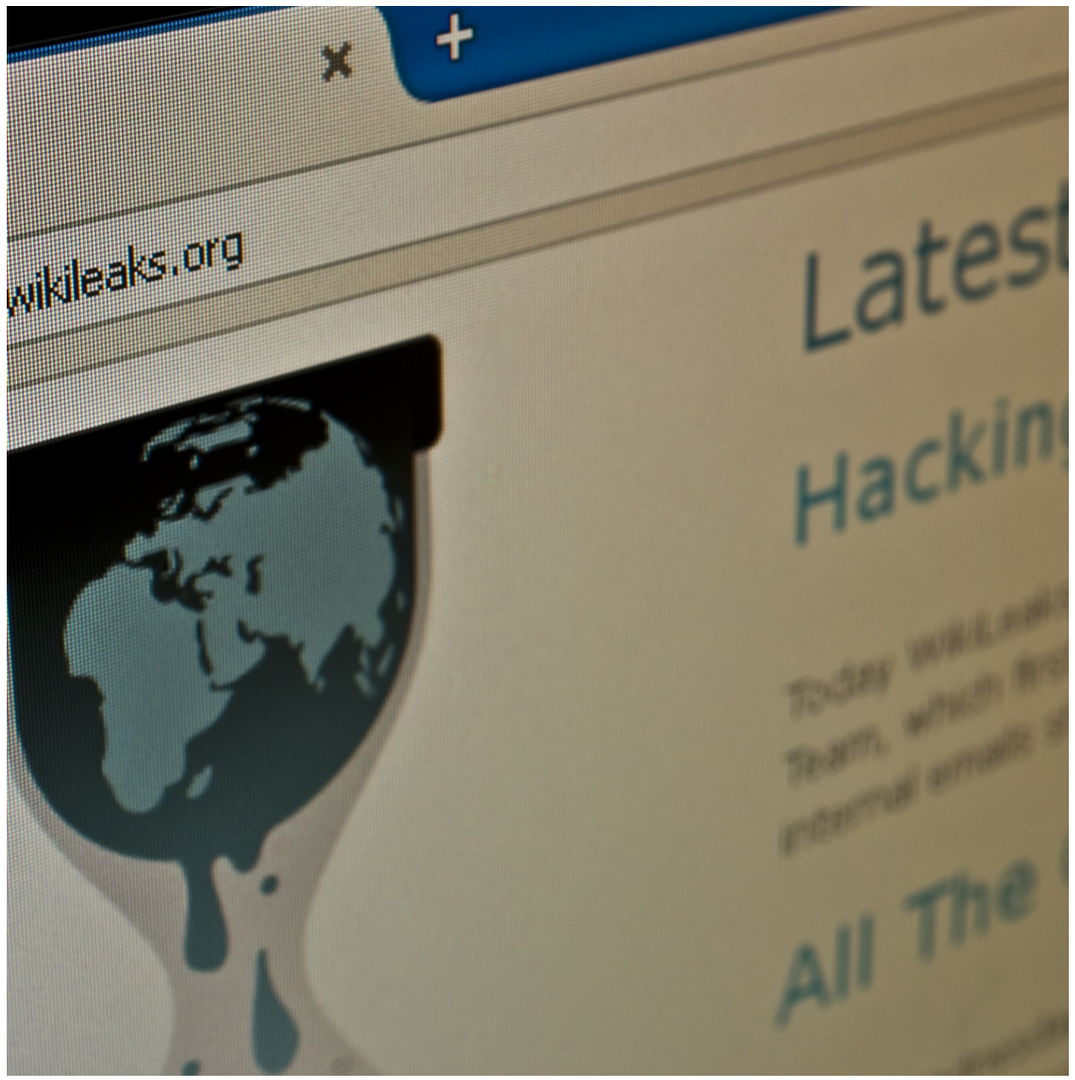
extranjero ante el riesgo “extremadamente elevado” de que tengan lugar ciberataques. En Holanda han ido aún más lejos, y sus autoridades anunciaron que contabilizarían a mano los votos en la noche electoral y comunicarían los resultados por teléfono para evitar el riesgo de un posible ciberataque. Un anuncio que tuvo lugar después de que un experto en seguridad asegurara que el ‘software’ utilizado en las mesas electorales era vulnerable.

La misma Holanda pidió en febrero la creación de una alianza internacional de defensa cibernética, a través de la OTAN, que tenga capacidades de defensa, control y ataques de respuesta, contra la creciente amenaza de los ciberataques.

La canciller alemana Angela Merkel dijo en marzo que proteger las infraestructuras alemanas de potenciales ciberataques era una de las mayores prioridades del momento. Poco después se supo que el ejército alemán formará su propio cibercomando para reforzar sus defensas online. En principio contará con 260 empleados, que irán aumentando hasta alcanzar los 14.500 para el año 2021.

Pero si hay un evento en la ciberguerra y ciberespionaje de lo que llevamos de año, es el protagonizado –a su pesar- por la CIA. El 7 de marzo, Wikileaks comenzó a publicar una serie de documentos bajo el título “Vault 7” que contenían detalles de técnicas y herramientas de software utilizadas para entrar en smartphones, ordenadores e incluso televisores con conexión a Internet.

Wikileaks está publicando los documentos en una sección de su página web (https://wikileaks.org/vault7/), y la cantidad de herramientas y técnicas utilizadas asombra a muchos. Lo que está claro es que la agencia de espionaje norteamericana dispone de todo tipo de herramientas para espiar a quien quiera, y ahora ha perdido el control de las mismas. La parte buena es que se puede utilizar el conocimiento publicado para protegerse mejor contra estos ataques, la parte mala es que otros actores pueden aprender para poner en práctica tácticas similares que busquen violar la privacidad de sus ciudadanos.



4. CONCLUSIÓN

4 Conclusión

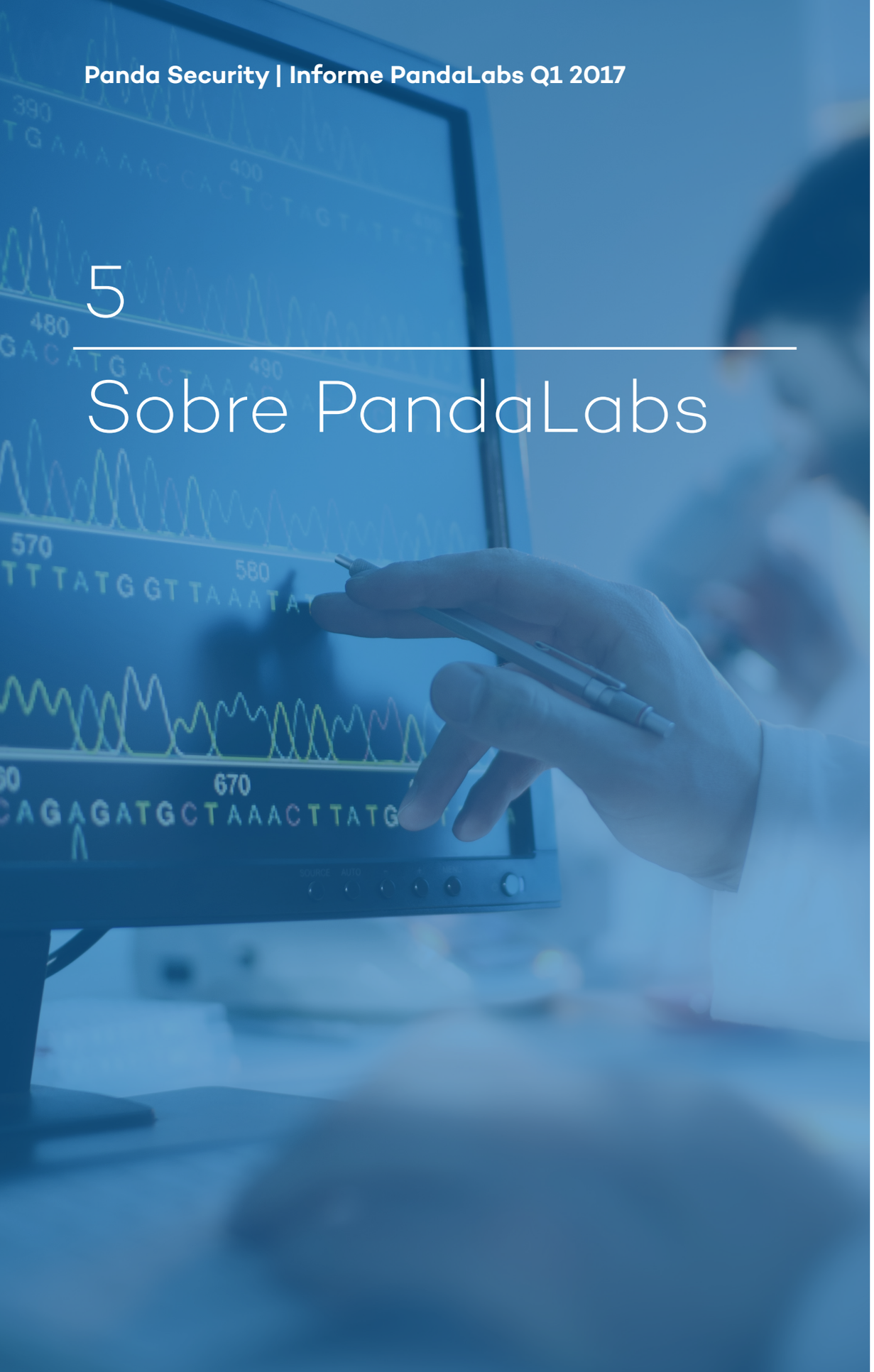
Wikileaks va a seguir publicando información de Vault 7 que sin duda analizaremos en el próximo informe. Debemos seguir atentos a la evolución del Internet de las Cosas –IoT- que a nivel de seguridad está demostrando tener mucho que mejorar.

Los ataques de ransomware seguirán liderando los tipos de ataques y mientras haya un porcentaje de víctimas que pague los rescates y las fuerzas de seguridad no puedan rastrear el dinero pagado a través de bitcoin esta tendencia no cambiará.

Seguiremos de cerca los ataques a empresas con el uso y abuso cada vez más frecuente de herramientas no maliciosas en sí mismas pero que los atacantes utilizan para infiltrarse en redes corporativas y robar información tratando al mismo tiempo que las soluciones de seguridad no se den cuenta de lo que está sucediendo.

Desde PandaLabs os mantendremos informados de todas las novedades del mundo de la seguridad a través de nuestro Media Center, y nos vemos dentro de 3 meses para analizar lo sucedido durante el segundo trimestre de 2017.

5. SOBRE PANDALABS



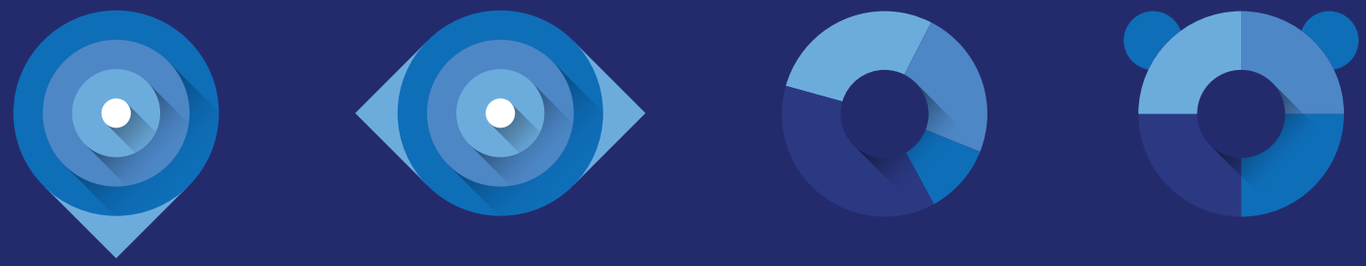
5 Sobre PandaLabs

PandaLabs es el laboratorio antimalware de Panda Security, y representa el centro neurálgico de la compañía en cuanto a tratamiento del malware se refiere:

- Desde PandaLabs se elaboran en tiempo real y de forma ininterrumpida las contramedidas necesarias para proteger a los clientes de Panda Security de todo tipo de códigos maliciosos a escala mundial.
- PandaLabs se encarga asimismo de llevar a cabo el análisis detallado de todos los tipos de malware, con la finalidad de mejorar la protección ofrecida a los clientes de Panda Security, así como para informar al público en general.

PandaLabs mantiene un continuo estado de vigilancia, siguiendo muy de cerca las diferentes tendencias y evoluciones acontecidas en el campo del malware y la seguridad.

El objetivo es avisar y alertar sobre inminentes peligros y amenazas, así como formular previsiones de cara al futuro.



panda

pandalabs