TENDENCIAS 2015

EL MUNDO CORPORATIVO EN LA MIRA

ENJOY SAFER TECHNOLOGY™

ÍNDICE

1 Introducción

① INTRODUCCIÓN

El informe de "Tendencias 2015: el mundo corporativo en la mira" del Laboratorio de ESET los invita a repasar algunos de los casos más relevantes de 2014 en cuanto a Seguridad Informática como así también debatir y presentar los desafíos y amenazas que se presentarán para 2015. En contraparte con los últimos años, este informe buscará abordar los diferentes tipos de amenazas e incidentes de Seguridad Informática que hemos presenciado a lo largo del año en un módulo dedicado a cada una de las temáticas para así responder a la pregunta: ¿qué veremos en 2015 en materia de Seguridad Informática? y en consecuencia: ¿cómo las empresas y usuarios se pueden preparar para afrontar el próximo año de una manera segura?

A lo largo de todo el año hemos visto una gran cantidad de publicaciones sobre ataques que involucran APTs pero, ¿qué es un APT?, ¿cuál es su impacto en una empresa? y ¿por qué continuaremos viendo este tipo de amenazas en 2015? son algunas de las preguntas que responderemos a lo largo del documento, repasando los sucesos de los últimos años y preparándonos para lo que se viene.

Además, 2014 fue un año con muchos sucesos importantes en relación a la Seguridad Informática, ya que en más de una ocasión nos hemos encontrado hablando de reportes de fuga de información, la explotación de vulnerabilidades y la aparición de diferentes amenazas que pusieron en jaque la seguridad y la privacidad de la información de las personas y empresas.

En nuestro documento del año pasado, hicimos hincapié en la importancia de la privacidad por parte de los usuarios, y qué podrían hacer para navegar de manera segura en Internet. Sin embargo, con incidentes relacionados en los que fotos y videos de los usuarios se filtraron, se remarcó la importancia que se le da a la privacidad y cómo se intenta resguardar la información por parte de los servicios en la nube y diferentes redes sociales. Asimismo, también continuó la preocupación de los usuarios por mantener su privacidad en línea y aparecieron sus quejas cuando los servicios en los que confiaron fueron vulnerados, pero ¿qué métodos pueden utilizar para mantenerse seguros en línea? Y asimismo, ¿cuáles son los desafíos de las empresas en torno a la privacidad, tanto propia como de sus clientes y empleados?

Por último, también destacamos que desde finales de 2013 hemos presenciado una nueva oleada de amenazas que cifran la información de sus víctimas para luego extorsionarlos con el pago de una suma de dinero para recuperar sus datos. El ransomware, con Cryptolocker como estandarte, se convirtió en un dolor de cabeza tanto para empresas como para usuarios, llegando incluso a los dispositivos móviles. ¿Se trata de una amenaza pasajera o es una modalidad que llegó para quedarse?

En resumen, a lo largo de este documento se hará un repaso de casos de códigos maliciosos que cifran la información de los usuarios; la fuga de datos de millones de tarjetas de crédito y débito a la venta por parte de cibercriminales que atacaron puntos de venta; vulnerabilidades en sistemas utilizados de forma masiva que pusieron en jaque la seguridad de muchas empresas alrededor del mundo, sin importar si se trataban de grandes corporaciones o PyMEs; y ataques dirigidos que fueron parte de los desafíos que las empresas y usuarios debieron afrontar a lo largo de 2014 y que seguramente también estarán presentes (y en algunos casos, hasta se profundicen) en 2015. Los invitamos a que descubran cuáles serán las tendencias en Seguridad Informática para el año 2015 y cuáles son las mejores prácticas para estar preparado para afrontarlas, tanto a nivel corporativo como hogareño.

El Laboratorio de Investigación de ESET Latinoamérica

2 Evolución de las APT

- El peligro de las APT
- Los cambios en los ciberataques
- APTs y la puerta abierta al ciberespionaje
- APTs a la vanguardia de los ataques en las empresas para 2015

② EVOLUCIÓN DE LAS APT

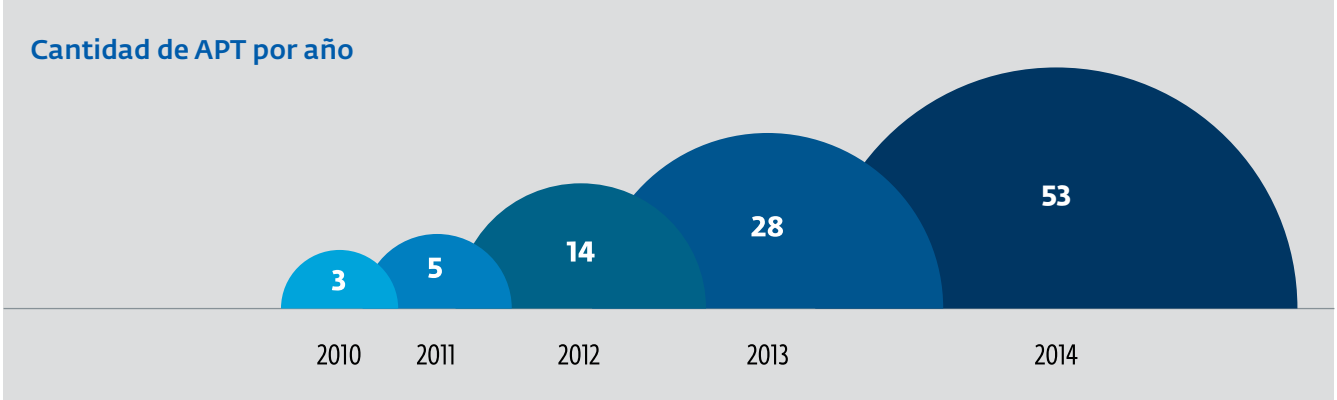

Gráfico 1. Crecimiento en la cantidad de APT estudiadas

Sin lugar a dudas en los últimos años hemos sido testigos de un cambio en la forma en que los ciberdelincuentes llevan a cabo sus ataques. Si bien las "amenazas tradicionales" son un riesgo significativo para las organizaciones tal como lo mencionamos en nuestro ESET Security Report 2014, ha habido una evolución hasta llegar a lo que vimos a lo largo de 2014: ataques puntuales desarrollados a la medida de cada víctima.

Este tipo de amenaza se denomina como APT (del inglés *Advanced Persistent Threat*, o Amenazas Persistentes Avanzadas). De acuerdo al Instituto Nacional de Normas y Tecnología de los EE.UU. (NIST) una APT es un "ataque dirigido con niveles sofisticados de pericia y recursos que le permiten a los atacantes por medio del uso de múltiples vectores de ataque (malware, vulnerabilidades, Ingeniería Social, entre otras), generar oportunidades para alcanzar sus objetivos, que habitualmente son establecer y extender su posicionamiento dentro de la infraestructura de tecnología de la información de organizaciones con el objetivo de filtrar información hacia el exterior continuamente, minar o impedir aspectos importantes de una misión, un programa o una organización, o ubicarse en una posición que le permita hacerlo en el futuro."

Tal como se puede ver en el Gráfico 1, la cantidad de análisis y estudios realizados sobre las APT se ha incrementado en los últimos cinco años, llegando incluso a duplicar la cantidad del año pasado durante los primeros diez meses de 2014.

Pero el crecimiento en la cantidad de estas amenazas no hace que sean más ampliamente utilizadas. De hecho son cada vez más discretas ya que tienen como objetivo lograr darle el acceso a un atacante a información y control de sistemas. Las APT requieren dedicación y pericia para lograr ataques efectivos a un blanco específico, y tal como hemos mencionado, la idea es permanecer dentro de la red el mayor tiempo posible para así poder obtener la mayor cantidad de información.

La evolución en la aparición de las APT no tiene un patrón de comportamiento en la forma en que surgen. Tal como se ve en el Gráfico 2, el único patrón reconocible es el crecimiento en la cantidad de estas amenazas. De hecho si se analiza mes a mes, se ven valores crecientes para los últimos cinco años.

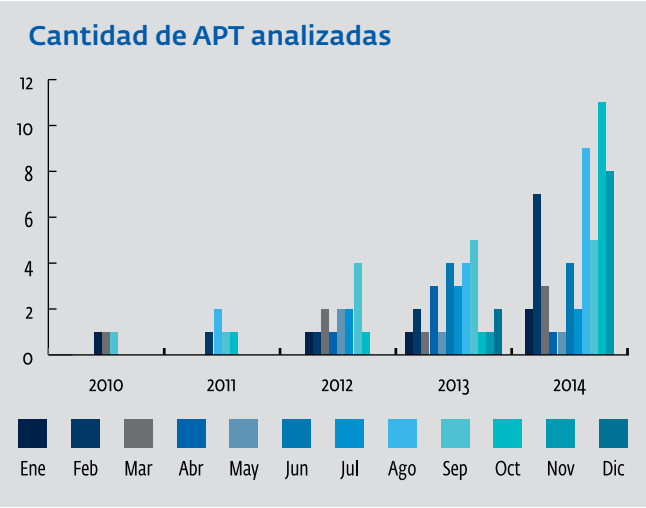

Gráfico 2. Evolución en la cantidad de APT

▶ El peligro de las APT

Los ciberdelincuentes al desarrollar las APT logran tener una amenaza que puede mantenerse durante un largo tiempo cambiando e infectando la mayor cantidad de sistemas posibles dentro de una misma red afectada.

A esto se suma el hecho de que aprovechan vulnerabilidades 0-day, haciendo que estos sean más complejos en su detección y por lo tanto pueden generar mayores pérdidas a sus víctimas.

Si bien queda claro que los ataques que utilizan APT vienen en crecimiento durante los últimos años, hay algunos casos que han tenido un mayor impacto. Por ejemplo el caso de Flame una amenaza que en 2012 afectó al Ministerio del petróleo de Irán, o sus predecesores, Duqu y Stuxnet, códigos maliciosos que a partir de explotar vulnerabilidades 0-day lograron afectar programas nucleares en oriente medio.

Incluso durante este año, tal como se ve en el Gráfico 3 amenazas como la familia BlackEnergy fueron utilizadas para ataques distribuidos de denegación de servicio, distribución de spam, fraudes bancarios e incluso en ataques dirigidos, lo cual demuestra la versatilidad que ofrecen estas amenazas para los cibercriminales.

Podríamos escribir todo un listado con ejemplos de los casos más recientes, pero agotaríamos las páginas de este documento. Lo realmente importante, es que debe quedar claro que independiente del rubro de la empresa, es necesario tomar consciencia de este tipo de ataques para poder tomar las medidas de protección adecuadas.

▶ Los cambios en los ciberataques

Cuando hablamos de un ciberataque, tradicionalmente se trata de campañas en las cuales se afecta la infraestructura tecnológica de una empresa buscando aprovechar alguna vulnerabilidad y robar algún tipo de información sensible que le genere algún tipo de ganancia económica al atacante.

En cambio con las APT, si bien los objetivos finales pueden ser muy similares a los ataques tradicionales, empezamos a ver que son campañas con una duración mucho más amplia, más dirigidas y sigilosas que buscan recabar mayor cantidad de información, afectar sistemas de forma prolongada o incluso hacer monitoreo de lo que pasa al interior de los sistemas de las víctimas.

Dadas estas diferencias, nos encontramos con campañas de Ingeniería Social más complejas y no solamente limitadas al uso de exploits y códigos maliciosos de uso genérico o adquiridos en el mercado negro.

▶ APTs y la puerta abierta al ciberespionaje

Después de conocer qué es lo que diferencia este tipo de amenazas de las que se suelen ver corrientemente, y dado que cada vez es más común ver empresas y entidades afectadas, es importante no olvidar que lo que buscan los atacantes es robar datos específicos o causar daños concretos. Dado que buscan datos muy puntuales y sensibles, es normal que sean ataques que duren meses, o incluso años, durante los cuales el atacante identifica vulnerabilidades,

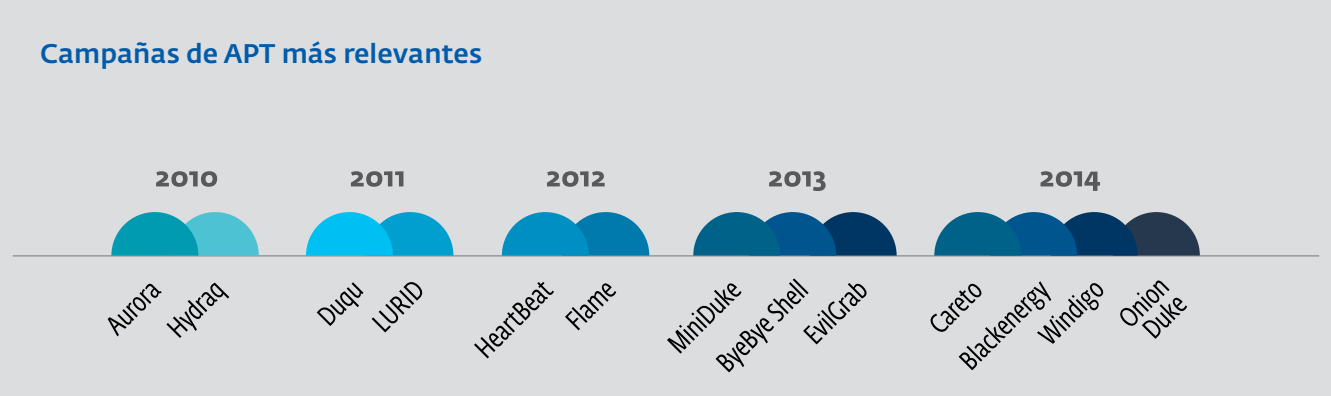

Gráfico 3. Evolución de las APT

evalúa cuáles son los controles de seguridad con los que cuentan los sistemas-objetivo, para de esa manera lograr el acceso de confianza a información privilegiada y extraerla sin que se generen sospechas.

En los últimos años desde el Laboratorio de análisis e investigación de ESET Latinoamérica se ha anunciado el descubrimiento de ataques de estas características en la región. Por ejemplo el ataque dirigido con la intención de robar información sensible a instituciones y empresas de Perú. La Operación Medre, logró recolectar más de 10.000 archivos de planos y proyectos realizados con el programa Autodesk AutoCAD.

La reaparición de BlackEnergy en 2014, da cuenta de que es un fenómeno que podemos encontrar a escala global. Este troyano creado originalmente para llevar a cabo ataques distribuidos de denegación de servicio (DDoS), evolucionó hasta convertirse en un malware sofisticado con arquitectura modular: una herramienta adecuada para enviar spam y cometer fraudes bancarios online, así como para realizar ataques dirigidos.

También en 2014 el equipo de investigación de ESET en Canadá informó de una campaña llamada Operación Windigo que en los últimos dos años llegó a afectar más de 25.000 servidores Linux y Unix, buscando redirigir a quienes visitan los sitios web infectados a contenido malicioso, además de enviar spam.

En el caso de Windigo es importante resaltar que en América Latina, los reportes indican aproximadamente 900 servidores infectados en Brasil, más de 250 en Argentina y 300 en México. Además si se tiene en cuenta que cada uno de estos sistemas tienen acceso a ancho de banda considerable, almacenamiento, potencia de cálculo y la memoria no es de sorprender que esta sola operación fuera responsable de enviar un promedio de 35 millones de mensajes de spam diarios y que cada día más de medio millón de visitantes de sitios web legítimos alojados en servidores afectados fueran redirigidos a un paquete de exploits.

▶ APTs a la vanguardia de los ataques en las empresas para 2015

Tal como se ha repasado a lo largo de esta sección es evidente el crecimiento de las APT en los últimos cinco años y se muestra una evolución que conduce al desarrollo de nuevos ataques. Por lo tanto es de esperar que durante 2015 se divulguen una mayor cantidad de empresas que han sufrido las consecuencias de una infección con una APT, además de que seguramente nos encontremos amenazas con características cada vez más complejas y evolucionadas, buscando aprovechar las brechas de seguridad que van apareciendo y que dejan las puertas abiertas para que sean cada vez más frecuentes las fugas de información confidencial de las empresas.

Algo para tener en cuenta es que probablemente varios de los casos que se den a conocer durante 2015, habrán sido perpetrados en 2014 dada la naturaleza de este tipo de amenazas. Lamentablemente, en ese tipo de casos la divulgación y el conocimiento de la infección se da una vez que la empresa ya ha sido comprometida por lo que es importante tomar todas las medidas de precaución para evitar ser víctima de este tipo de ataques, ya sea mediante la implementación de tecnología como a través de la educación de los usuarios y una correcta gestión de la seguridad por parte de la compañía.

Asimismo, algo importante para destacar es que, a pesar que las grandes compañías pueden parecer un blanco más interesante para los atacantes, lo cierto es que ninguna organización está exenta de sufrir un ataque de este tipo, dado que lo que el atacante busca es información valiosa, algo que con lo que cualquier empresa, organización o entidad cuenta. Por lo tanto es un desafío para empresas de cualquier tamaño adoptar las medidas de seguridad necesarias para no sufrir ningún incidente.

Por último, en lo referido a América Latina, ya se ha visto que ha habido empresas afectadas por APTs aunque es de esperarse que en 2015 (y de aquí en adelante) se hagan más frecuentes este tipo de ataques en la región, tal como ha sucedido en el pasado con otras amenazas que en un principio tenían preponderancia en otras regiones y al tiempo "desembarcaban" en la región.

3 Malware en los puntos de ventas

- El objetivo: la información
- PoS Malware y 2015

③ MALWARE EN LOS PUNTOS DE VENTAS

Desde finales de 2013 hemos sido testigos de múltiples reportes que llegaron a las noticias hablando de cómo los puntos de venta de grandes cadenas de retail habían sido comprometidos por códigos maliciosos. Si bien sonó extraño al comienzo, con el pasar de las semanas quedó en claro que una nueva ola de ataques puso en jaque a muchas empresas y en tan solo unos pocos meses, millones de tarjetas de crédito y débito quedaron en mano de los cibrercriminales. En los próximos párrafos compartiremos con ustedes algunos de los hechos más importantes en relación a estos ataques y por qué para el 2015 las empresas en Latinoamérica deberán prestar atención a este tipo de ataques.

Point of Sale Malware (en español, malware en los puntos de venta) o "POS Malware" como se lo suele identificar, hace referencia a diferentes familias de códigos maliciosos que infectan las terminales o puntos de venta y buscan robar los datos de tarjetas de crédito o débito al momento que un usuario realiza una compra. Para lograr este objetivo, los cibercriminales no solo deben infectar las máquinas por las cuales los usuarios pasan la banda magnética de sus tarjetas, sino que además deben sortear todas las protecciones de las empresas. Grandes compañías como Target, Home Depot y UPS entre tantas otras, fueron víctimas de este tipo de ataques a pesar de los controles que habían implementado. Una particularidad que une los ataques a Target y Home Depot se centra en que el código malicioso utilizado para robar los datos de las tarjetas desde los puntos de ventas fueron variantes de BlackPOS. El código de esta familia de malware se filtró en 2012, lo que al igual que lo que sucedió con Zeus podría haber dado origen a múltiples variantes.

El robo de la información se produce directamente en el punto de venta, donde familias de códigos maliciosos como JacksPos, Dexter, BlackPOS y otras amenazas detectadas por los productos de ESET como Win32/BrutPOS o Win32/POSCardStealer extraen los datos de las tarjetas de crédito desde la memoria RAM utilizando diferentes técnicas y funcionalidades. Aunque este proceso pareciera ser sencillo, implica que los cibercriminales tuvieron que eludir muchos otros controles de seguridad y aún al día de hoy se desconoce, o no se divulgó, cómo es que lograron acceder a las terminales para infectarlas en un primer lugar. Está más que claro que nos enfrentamos a ataques complejos y a gran escala similares a las APT presentadas en otra sección de este informe, sin embargo, el objetivo final en este caso es la información de las tarjetas de crédito y no datos confidenciales de empresas o gobiernos.

▶ El objetivo: la información

Las tarjetas de crédito cuentan con bandas magnéticas que almacenan su información. Los datos necesarios para hacer una compra, como el número de la tarjeta de crédito, el titular, la fecha de vencimiento y el código de seguridad se encuentran almacenados en tres tracks que componen la banda magnética. Al momento de realizar un pago y deslizar nuestra tarjeta por el lector, toda esta información se carga en el sistema de punto de venta, para validar la compra.

Por normas de seguridad, toda la comunicación entre la entidad emisora de la tarjeta de crédito y el negocio en el cual se realiza la compra debe viajar cifrada, como así también el almacenamiento de los datos. Sin embargo, existe una pequeña ventana de exposición en la que los datos de la tarjeta no están cifrados, y es en el momento en que son leídos y almacenados en la memoria RAM. Es aquí donde amenazas como Dexter entran en juego y se encargan de leer la memoria del proceso correspondiente al sistema de pagos para luego extraer los datos de la tarjeta. Una vez que se han extraído, el siguiente paso que el código malicioso realiza es el envío de las credenciales, y según diferentes investigaciones este paso puede ser de lo más variado: en algunos casos la información se enviaba a través del protocolo HTTP o FTP y en otros casos lo recolectado se alojaba en un servidor interno de la organización atacada al cual los cibercriminales accedían luego para extraerla.

Este año en Virus Bulletin, una de las conferencias más importantes de la industria antivirus, tuvimos la posibilidad de presenciar la charla de Hong Kei Chan y Liang Huang, "Swipe away we're watching you", en donde nos describieron en detalle los meca-

nismos implementados por las familias más utilizadas en este tipo de ataques para leer la memoria de los procesos, extraer la información de las tarjetas de crédito y los mecanismos con los cuales enviaban la información a los atacantes.

Lo que es importante entender acerca de la seriedad de estas amenazas es que fueron responsables de la fuga de 40 millones de tarjetas de crédito y débito en el caso de Target, evento que llevó a la renuncia de su CEO. Otro de los casos de mayor renombre fue el de UPS, en donde se registraron casi 105.000 transacciones de tarjetas de crédito y débito. Finalmente, el caso que se convirtió en la fuga de datos más grande fue el de Home Depot, donde la cifra asciende a 56 millones de tarjetas robadas. En este caso, las tiendas afectadas no solo se encontraban en los Estados Unidos sino que también afectó a las tiendas en Canadá. El incidente de Home Depot se convirtió en el hecho de fuga de información más grande registrado, por lo menos en lo referido a información financiera de los usuarios.

Uno de los puntos críticos ante este tipo de ataques se centra en el tiempo que se tardó en identificar que las redes de las empresas se encontraban comprometidas, algo que es hoy en día uno de los mayores desafíos de las empresas, y en particular de los equipos de seguridad. Según los datos de Verizon's 2013 Data Breach Investigations Report, al 66% de las empresas que fueron víctimas del robo de datos en 2012 les llevó algunos meses darse cuenta del incidente. En uno de sus análisis, Brian Krebs comenta que en el caso de Target, los primeros registros de fuga de tarjetas datan del 27 de noviembre de 2013, lo que le dio a los atacantes algunos meses para operar sin siquiera ser descubiertos. Acorde a las declaraciones del CEO de Target, el incidente fue detectado luego de que fuerzas de seguridad los contactaran para comentarles del caso, el 15 de Diciembre de 2013.

En el caso del robo de información en Neiman Marcus, de un total de 1.100.000 registros, luego de estudios se confirmó que el número real de tarjetas de crédito y débito filtradas fue de 350.000, entre el 16 de Julio y el 30 de Octubre de 2013. De ese número, se registraron aproximadamente 9.200 casos en los cuales fueron utilizadas para realizar compras.

Puntualmente en lo que refiere al caso de Home Depot, desde abril hasta que se publicó la nota de prensa reconociendo el incidente (el martes 2 de septiembre) 56 millones de registros se filtraron a través de la red de la compañía.

En toda Latinoamérica existen múltiples compañías de retail, con cientas, y hasta miles, sucursales en toda la región, por lo que ser víctimas de casos como

Con el fin de proteger los puntos de ventas existen ciertas cuestiones a tener en cuenta por parte de las empresas para así minimizar el riesgo de exposición ante este tipo de incidentes:

↘ Usa una contraseña fuerte

En este caso es importante notar que muchas de las máquinas infiltradas tenían las contraseñas predeterminadas o simples variantes del nombre del fabricante del PoS. Por ejemplo, las tres contraseñas más comunes fueron "aloha12345", "micros" y "pos12345". Es mucho más conveniente utilizar una frase de contraseña en lugar de una simple palabra, ya que una frase se puede recordar fácilmente y aun así llevaría demasiado tiempo adivinarla debido a su longitud. Nunca se deben dejar las contraseñas por defecto en un software de PoS.

↘ Limita los intentos de inicio de sesión

Un rango común es bloquear a las personas tras 3-5 intentos incorrectos. Esta acción reduce drásticamente la eficacia de los ataques por fuerza bruta, ya que el atacante no logrará probar la suficiente cantidad de contraseñas incorrectas hasta poder adivinarla.

↘ Limita el acceso

Limitar el acceso siempre que se pueda. Por ejemplo: si no se necesita acceder remotamente a la máquina, no habilitar el RDP. Si necesitas habilitar el RDP, verifica que sea seguro.

↘ Revisa los procesos de actualización

Entre algunas de las medidas de seguridad de los PoS, es posible encontrarse además con una solución de seguridad con herramientas de whitelisting de procesos. Estas herramientas permiten que solo se ejecuten procesos que han sido marcados como seguros. En algunos de los incidentes, las amenazas se instalaron durante este tipo de procesos que, según la cantidad de equipos a actualizar, puede durar entre un par de semanas a algunos meses.

los que presentamos es realmente una preocupación ya que muchas veces una vulnerabilidad en un servidor o una falta de controles en los procesos de actualización de software podría abrir una puerta a que toda la red de puntos de venta de la compañía se vea comprometida.

▶ PoS Malware y 2015

Está claro que desde finales de 2013 y a lo largo de todo 2014 hemos sido testigos de los casos más importantes de ataque al retail. Sin embargo, en lo que respecta al año que viene no todo está dicho. Los cibercriminales han sido capaces de encontrar vulnerabilidades en las redes o en la infraestructura de algunas de las cadenas más importantes a nivel mundial. Es importante para las empresas replantearse el modo de proteger sus puntos de venta como así también toda la infraestructura asociada a ellos.

Grandes volúmenes de información conllevan la implementación de controles y pruebas de lo más rigurosas que se puedan imaginar. Si bien algunos de los casos que mencionamos en párrafos anteriores parecieran haber sido perpetrados por diferentes grupos que están en contra de los Estados Unidos, no hay información que descarte que otras cadenas de retail o tiendas fuera de este país sean atacadas con variantes de BlackPOS.

2015 será un año que le permitirá a los equipos de seguridad que manejan sistemas de puntos de ventas rever cómo protegerlos y de qué manera los logran aislar para que sucesos como los que hemos visto en los últimos 12 meses no se sigan repitiendo. Un caso de fuga de información de esta índole es un golpe directo al negocio, que ciertas empresas simplemente no se podrán permitir, ya sea por impacto económico o por la reputación de la compañía frente a sus clientes.

Es por esto que luego de los incidentes de Target y Neiman Marcus, empresas como VISA han realizado una invitación abierta a través de Charlie Scharf, su CEO, a reforzar las medidas de seguridad en los sistemas de pago y donde el uso de dispositivos móviles podría ser una solución o bien, un nuevo problema para el próximo año.

④ Fuga de Información

- ¿Qué se puede hacer frente a la fuga de información?
- Por qué implementar un doble factor de autenticación en las empresas
- Los ataques y sus números
  - Incidentes en los últimos 5 años
  - Cantidad de datos filtrados
- 2015, la información y la protección de las empresas

④ FUGA DE INFORMACIÓN

A lo largo de los últimos años, los casos de fuga de información que afectaron a empresas, gobiernos y otras entidades han llegado a las noticias e impactado en miles o millones de usuarios. 2014 no fue la excepción, hemos sido testigos de grandes casos de fuga de información e incluso de la aparición de información sustraída de las empresas en distintos foros del *underground* del cibercrimen.

Arrancamos 2014 con la noticia de que la seguridad de una empresa de retail fue vulnerada durante los últimos meses del año pasado, dejando en posesión de los atacantes más de 40 millones de tarjetas de crédito y débito. Si bien los sistemas de Punto de Venta (PoS) fueron algunas de las principales víctimas de la fuga de información, no fueron los únicos.

Empresas como eBay o Yahoo! se vieron en la necesidad de notificar a miles de usuarios que sus contraseñas habían sido filtradas a través de un ataque. Pero como era de esperarse, los incidentes no se detuvieron allí, ya sea que las empresas fueron afectadas directamente o a través de herramientas de terceros, la lista contiene nombres como KickStarter, Spotify, Bit.ly Snapchat, y Dropbox entre otros. Uno de los últimos casos de 2014 involucró nuevamente a Sony, en donde los cibercriminales lograron vulnerar sus sistemas y entre la información que se filtró, se encuentran películas completas que todavía no se estrenaron.

▶ ¿Qué se puede hacer frente a la fuga de información?

En nuestro anterior informe "Tendencias 2014: El desafío de la privacidad en Internet", hicimos hincapié en la doble autenticación como una herramienta necesaria para elevar la seguridad al momento del inicio de sesión de los usuarios. Según los datos relevados por Risk Based Security en el 70% de los incidentes de seguridad ocurridos en la primera parte de 2014 se filtraron contraseñas. Esta cifra vuelve a remarcar la importancia de contar con un segundo factor de autenticación para las empresas, un reto que deberán afrontar durante el 2015.
Si nos basamos en los servicios o sitios que incorporaron la doble autenticación para proteger a sus usuarios, nos encontramos con empresas como Google, Facebook, Twitter, Github y otras más. Incorporar un segundo factor de autenticación a través del método OTP (One-Time-Password) incrementa la seguridad al momento de inicio de sesión como así también ofrece un resguardo en el caso que las contraseñas de los usuarios sean robadas o filtradas, ya sea a través de una infección de malware en sus propios sistemas o mediante un incidente de seguridad de la empresa.

▶ Por qué implementar un doble factor de autenticación en las empresas

Implementar un doble factor de autenticación al momento de conectarse a la VPN de una empresa, el CRM u otros servicios Web, no es solo una protección para los empleados, sino que también es un valor agregado que se les puede ofrecer a clientes y proveedores para interactuar con la empresa. En pos de enfrentarse a los desafíos que presenta la fuga de información y los ataques que las empresas pueden sufrir, la implementación de un doble factor de autenticación ayudará a proteger a las empresas en 2015.

▶ Los ataques y sus números

Muchos de los incidentes de seguridad de este año tuvieron como objetivo los sistemas de punto de venta tal como podrán ver en otra de las secciones de este informe, pero otras industrias también se vieron afectadas. Uno de estos casos es el del Comunity Health System (CHS) en los Estados Unidos, que fue víctima de la fuga de 4.5 millones de registros médicos. Acorde al comunicado de la entidad, sus sistemas fueron víctimas de una APT que fue originada en China de acuerdo a los resultados arrojados por la investigación realizada entre la compañía y Mandiant.

El caso de CHS no fue el único que tuvo como víctima a la industria de la salud. Según el reporte realizado por el Identity Theft Resource Center de Estados Uni-

dos, a diciembre de 2014 se han reportado 304 brechas de seguridad en instituciones médicas, lo que representa el 42,2% del total de incidentes. Si bien según este informe la mayor cantidad de ataques fue recibida por entidades de salud, aproximadamente el 80% de los datos que se filtraron corresponden al sector de negocios, que fue víctima de 3 de cada 10 casos de fuga de información (Tabla 1).

La información que forma parte del reporte del ITRFC contabilizó una menor cantidad de ataques si tomamos en cuenta el reporte de Risk Based Security. Según la firma de seguridad, durante los primeros seis meses de 2014 se registró un número menor de ataques que en años anteriores, sin embargo a pesar de ser la mitad de incidentes que en 2013, durante 2014 se filtró un 60% más de información que el año anterior, dejando en claro que más ataques no significa una mayor cantidad de fuga de datos.

En cuanto al análisis de los datos que se sustrajeron de las empresas o entidad afectadas, quedó claro que el objetivo principal de los cibercriminales son los usuarios y las contraseñas, con un incremento de casi el 25% en relación al año anterior.

▶ 2015, la información y la protección de las empresas

Proteger la información es un requerimiento cada vez más significativo para las empresas y una de las garantías para la continuidad del negocio. En base a los principales incidentes que se vieron durante 2014 y a algunas de las metodologías utilizadas para vulnerar las defensas de las empresas, podemos asegurar que durante el año que viene los equipos de IT de las empresas tendrán que enfrentarse a ataques más complejos y sigilosos. Tanto la evolución en la complejidad de los ataques, como los actores que forman parte de los mismos son un desafío constante para la seguridad de las empresas, ya que no solo deben estar atentos a las vulnerabilidades que los atacantes intenten explotar sino que además deberán comprender los motivos por los cuales su negocio podría ser objetivo de los atacantes.

Industria	Cantidad de incidentes (% del total)	Registros robados (% del total)
Banca/Créditos/Financiera	41 (5,7%)	1.182.492 (1,4%)
Comercio	237 (32,9%)	64.731.975 (79,3%)
Educación	54 (7,5%)	1.243.622 (1,5%)
Gobierno/Ejército	84 (11,7%)	6.494.683 (8%)
Medicina/Cuidado de la Salud	304 (42,2%)	7.944.713 (9,7%)
Total	**720**	**81.597.485**

Tabla 1

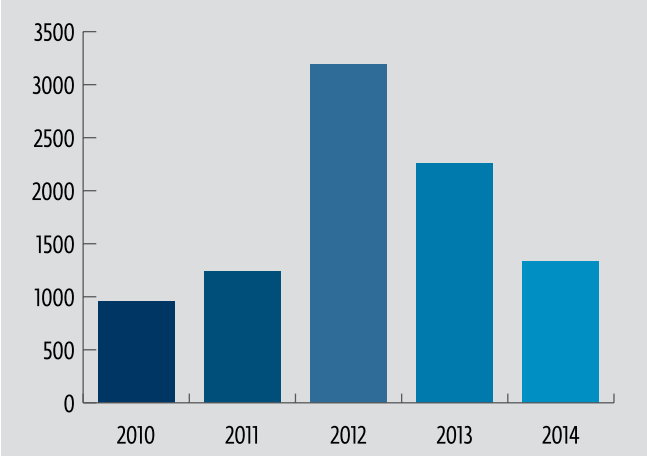

Gráfico 4. Número de incidentes en los últimos 5 años

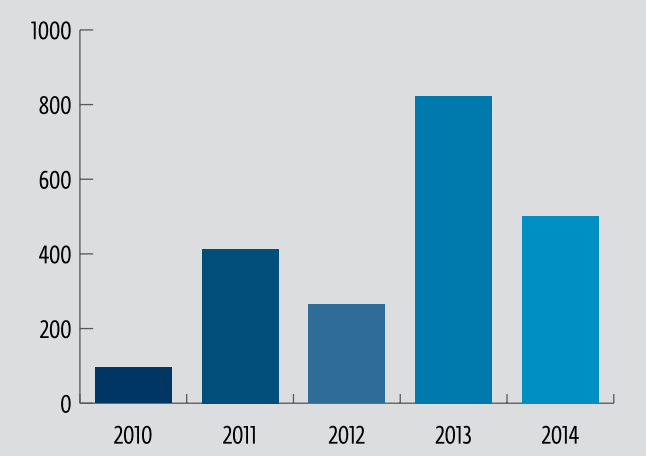

Gráfico 5. Cantidad de datos filtrados en millones de registros

Según los datos presentados en el ESET Security Report 2014 para Latinoamérica, solo el 10,5% de las empresas utilizan un doble factor de autenticación, 2 de cada 10 implementan el cifrado de información y una de cada diez cuenta con una solución de seguridad para su flota de dispositivos móviles. Si nos enfocamos en estos tres parámetros, y en los incidentes de fuga de información que se dieron a lo largo de 2014, vemos que todavía queda mucho trabajo por hacer.

Implementar el cifrado de los datos, ya sea en los dispositivos móviles, en los servidores de la empresa o en la flota de laptops para aquellos perfiles móviles, minimiza la posibilidad que ante una infección de malware, la pérdida de un equipo o una intrusión no autorizada, la información de la compañía no quede expuesta. Por otro lado, el doble factor de autenticación incrementa la seguridad de los sistemas de la empresa al momento de iniciar sesión. Basados en los datos del reporte de Risk Based Security, el 57% de los incidentes durante la primera mitad del 2014 involucraron nombres de usuarios, direcciones de correo y contraseñas de los usuarios. Para el 2015, las empresas de América Latina y del resto del mundo podrán mejorar la protección de sus sistemas e infraestructura a través de la implementación del doble factor de autenticación, que garantizará un acceso controlado a la información de la compañía.

5 La incidencia de las botnets en Latinoamérica

- Botnets más detectadas
- Variedad en las detecciones
- Distribución de las detecciones en Latinoamérica
- Comportamiento de las botnets
- Perspectivas de los bots

⑤ LA INCIDENCIA DE LAS BOTNETS EN LATINOAMÉRICA

No cabe duda que las botnets han sido desde hace varios años una de las principales amenazas utilizadas por los cibercriminales, y es posible que esto siga sucediendo por muchos años más. No obstante, en Latinoamérica hemos visto comportamientos interesantes y que se repiten en los diferentes países de la región de forma individual. En esta sección del documento abordaremos este tema para inferir alguna conclusión que nos de luces acerca de cómo podría ser el comportamiento de estas amenazas durante el próximo año.

▶ Botnets más detectadas

En cuanto a los códigos maliciosos del tipo bot detectados en la región, la primera posición la ocupa Dorkbot, una amenaza que afecta usuarios de Latinoamérica desde 2012. Con un porcentaje muy similar también está el gusano Agent.NDH, el cual tiene un comportamiento malicioso parecido a Dorkbot.

Lo que resulta interesante de este par de amenazas es que los porcentajes de detección son muy similares. Tal como se puede observar en el Gráfico 6 estas dos botnets se llevan casi el 90% de total de detecciones en Latinoamérica y, adicionalmente, cada una de estas familias se lleva la mitad de este porcentaje de detección.

Si bien las dos amenazas anteriores son las más detectadas dentro de los códigos maliciosos del tipo bot, en los casos donde los equipos cuentan con alguna solución de los productos de ESET, encontramos que los códigos maliciosos restantes tienen un comportamiento parecido. Por ejemplo, entre las detecciones de la familia IRCBot y la de Zbot ocurre que tienen porcentajes similares, lo mismo que sucede en el caso de otras familias como Neuvret, RBot y DragonBot que si bien no tienen niveles altos, siguen el mismo patrón.

▶ Variedad en las detecciones

Un comportamiento esperado en cuanto a la propagación de amenazas, es que entre aquellas familias más propagadas se suele encontrar una mayor cantidad de variantes. Una razón posible es que cada nueva variante puede tener alguna pequeña modificación en el comportamiento del código malicioso para alterarla de tal forma que sea, por ejemplo, más complicado para una solución de seguridad detectarla.

Sin embargo, si hacemos un listado de las botnets más detectadas en la región, organizándolas por la cantidad de variantes detectadas (Gráfico 7) nos encontramos que las firmas Agent.NDH y Dorkbot no se encuentran en los primeros puestos. De hecho, la familia con la mayor cantidad de variantes tiene apenas un nivel de detección cercano al 4%.

En cambio, para el caso de las familias con mayor cantidad de detecciones, la suma de variantes son las menores que podemos encontrar en el listado.

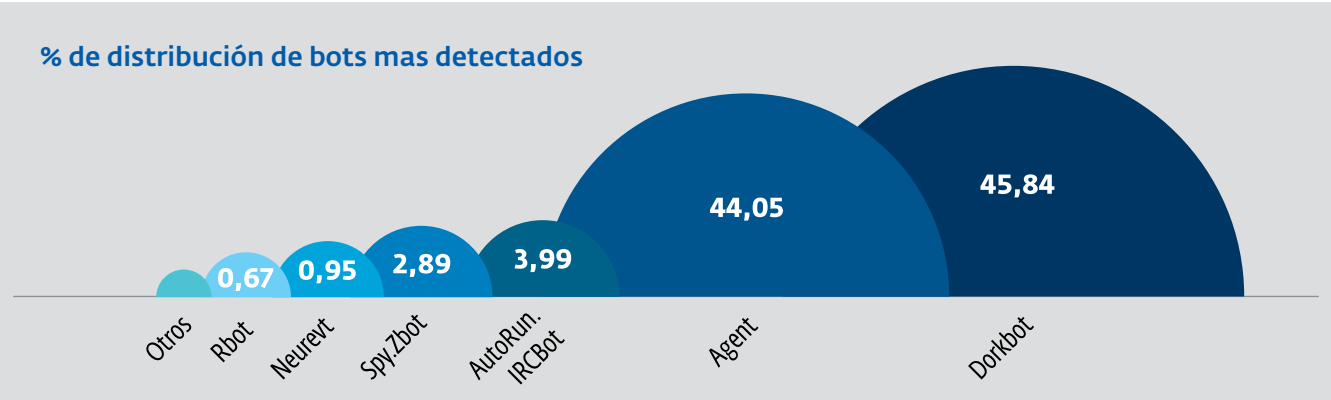

Gráfico 6. Botnets más detectadas en Latinoamérica

▶ Distribución de las detecciones en Latinoamérica

Conocer cuál es la concentración de detecciones de algún tipo de código malicioso nos puede dar una idea de cómo se comportan las campañas de propagación de malware y sus víctimas potenciales.

En el caso de los países de Latinoamérica (Gráfico 8) resulta interesante notar como México y Perú tienen casi la mitad de detecciones de los códigos maliciosos del tipo Bot.

Venezuela es el otro país que tiene un nivel de detecciones superior al 10%, mientras Argentina, Ecuador, Guatemala y Colombia tienen porcentajes menores, pero entre los cuatro suman un poco más de la cuarta parte de detecciones de toda la región.

▶ Comportamiento de las botnets

Contar con la cantidad de variantes o los países más afectados no nos brinda información adicional que nos permita inferir comportamientos particulares en la región o en algún determinado país. Sin embargo, después de analizar por separado la cantidad de detecciones de las familias de códigos maliciosos con niveles de reporte similares, empezamos a encontrar comportamientos que resultan por demás interesantes.

Si aislamos la cantidad de detecciones de aquellas familias de botnets con niveles de detección similares encontramos conductas con cierto nivel de simetría. Por ejemplo, en el caso de Dorkbot y Agent.NDH (Gráfico 9) vemos un comportamiento inverso durante los meses analizados. De esta manera, podemos demostrar que al caer las detecciones de Dorkbot, aumentan las de la familia Agent.NDH.

Si pasamos a los códigos maliciosos que tienen niveles de detección similares (Gráfico 10), nos encontramos con un caso parecido. Si bien aquí la distribución es diferente, la tendencia de crecimiento y decrecimiento se mantiene idéntica al caso anterior.

En el caso de las familias analizadas en el Gráfico 11, las últimas con porcentajes significativos en la cantidad de detecciones, encontramos conductas, que si bien no son tan simétricas como en los casos anteriores, resultan relevantes dado que justo en el mes que decaen de forma abrupta las detecciones de la familia RBot empezamos a notar un crecimiento de la familia DragonBot.

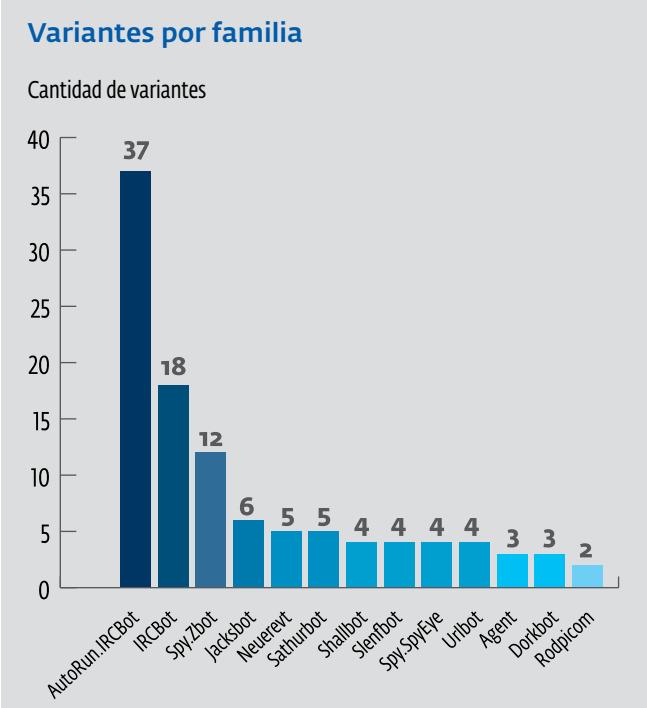

Gráfico 7. Relación entre las familias y las variantes

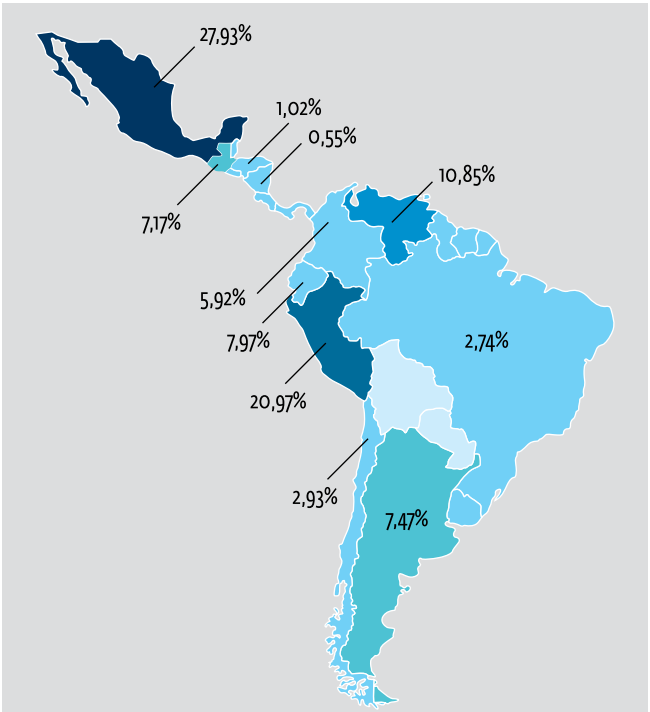

Gráfico 8. Porcenaje de bots por país

Si bien los gráficos mostrados corresponden al total de detecciones en todo Latinoamérica, resulta interesante destacar que en cada uno de los países de la región se dan comportamientos inversos similares, aunque no necesariamente con las mismas siluetas.

▶ Perspectivas de los bots

Que los códigos maliciosos del tipo botnet dejen de tener relevancia en la escena del cibercrimen latinoamericano es algo que seguramente no suceda durante el año próximo. Si bien hay otras amenazas, como el ransomware o los BitCoin miners, que han tenido un crecimiento en las detecciones, la versatilidad que ofrecen las botnets las convierte en la amenaza preferida por los ciberdelincuentes.

Por otra parte, los comportamientos de las diferentes familias de códigos maliciosos dejan en evidencia que existe cierto orden en la forma de propagación de estas amenazas. Este tipo de comportamientos es el indicio de que existen grupos organizados en la región detrás de la propagación y administración de estas herramientas maliciosas.

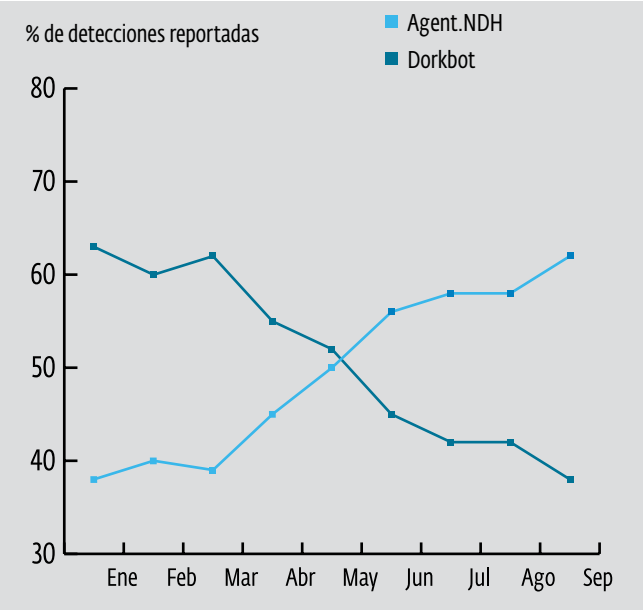

Gráfico 9. Cantidad de detecciones Dorkbot vs. Agent.NDH

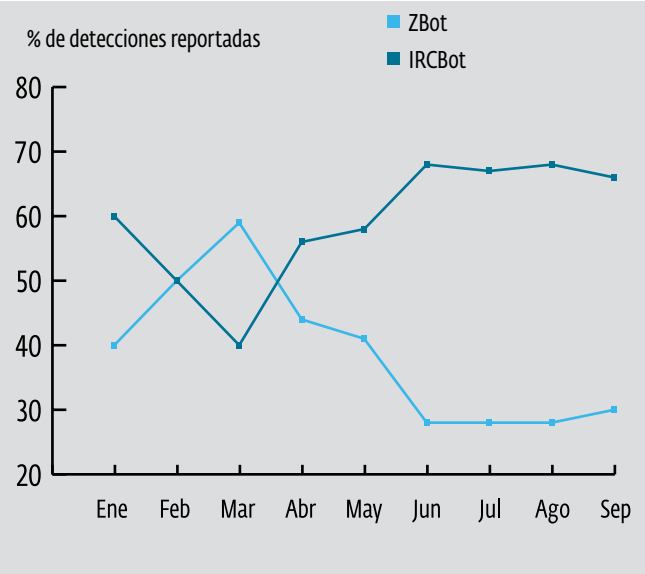

Gráfico 10. Cantidad de detecciones Spy.Zbot vs. AutoRun.IRCBot

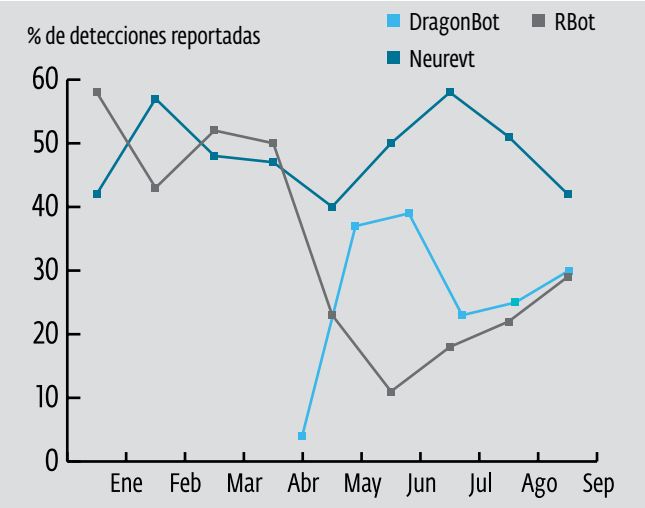

Gráfico 11. Cantidad de detecciones DragonBot, Rbot y Neurevt

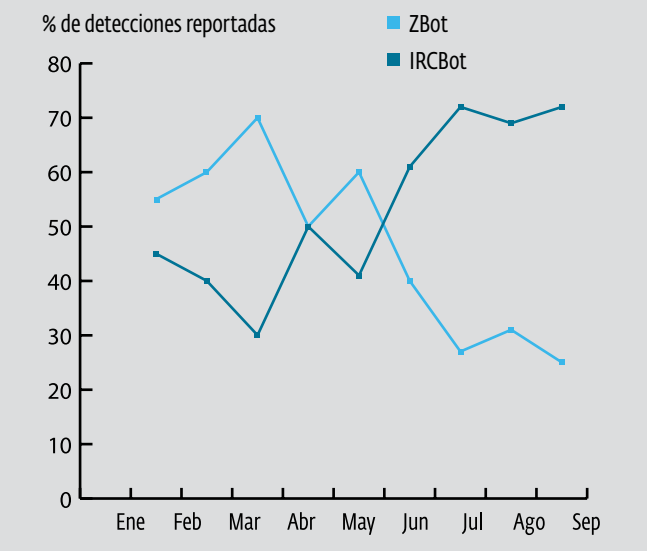

Gráfico 12 . Peru - IRCBot vs ZBot

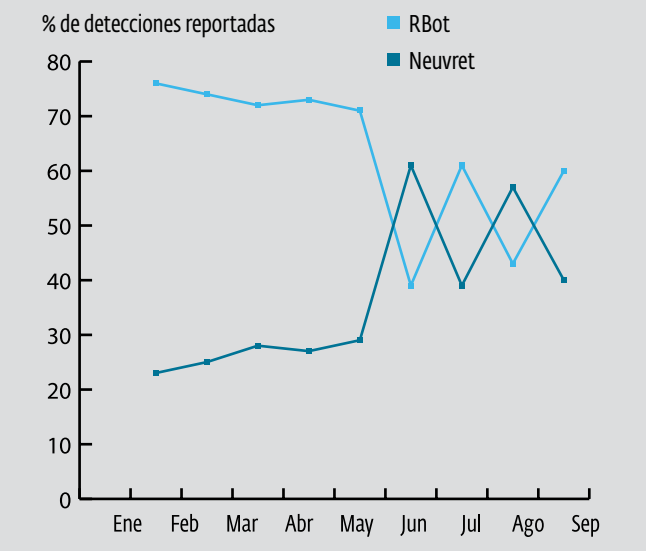

Gráfico 13 . Argentina - Neuvret vs RBot

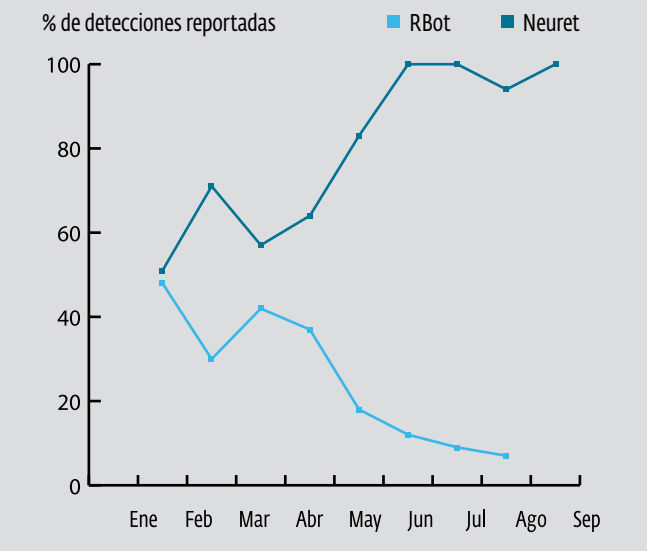

Gráfico 14 . Colombia - Neuvret vs RBot

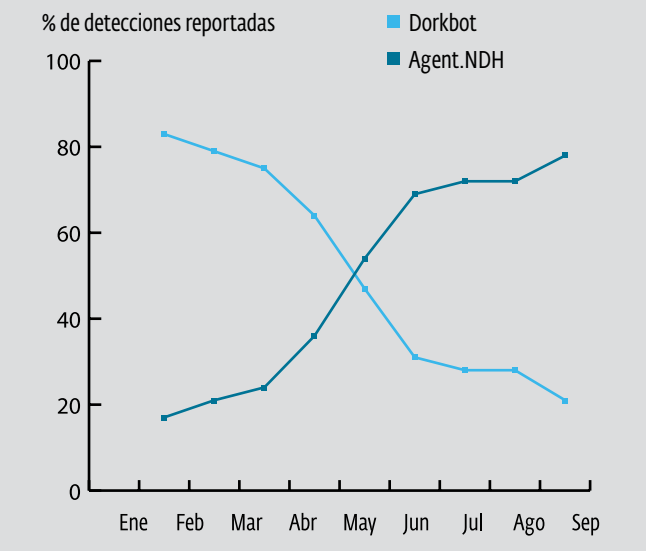

Gráfico 15 . Peru - Dorkbot vs Agent.NDH

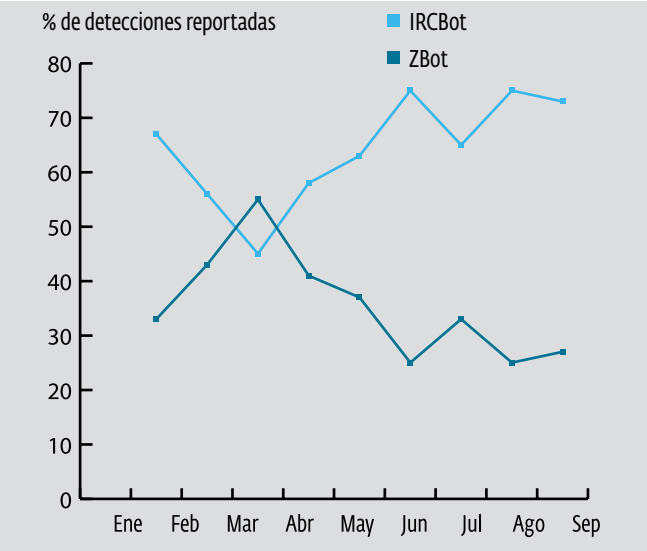

Gráfico 16 . Mexico - IRCBot vs ZBot

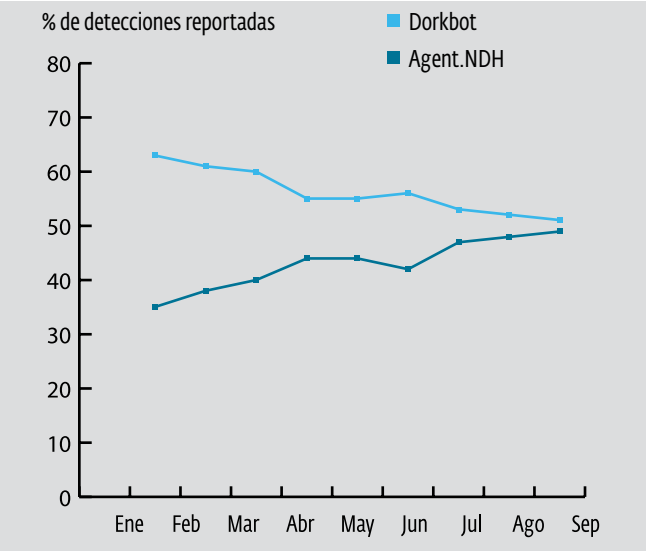

Gráfico 17 . Mexico - Dorkbot vs Agent.NDH

6 Vulnerabilidades, su impacto y el desafío en 2015

⑥ VULNERABILIDADES, SU IMPACTO Y EL DESAFÍO EN 2015

2014 fue un año más que importante en lo referido a las vulnerabilidades de software, no solo por el impacto que éstas han causado en los sistemas afectados, sino también por la magnitud de los sistemas involucrados. Tan solo con nombrar los casos de Heartbleed, Shellshock y Poodle, junto con la repercusión que tuvieron en los medios y en el accionar de los equipos de seguridad, es más que suficiente. Sin embargo, por más que hayan sido algunas de las vulnerabilidades con mayor impacto en los últimos tiempos, no han sido las únicas. Con la aparición de una vulnerabilidad desconocida que se aprovecha de una falla de software, los cibercriminales han logrado comprometer sistemas pertenecientes a empresas, entidades gubernamentales y demás.

El impacto que causa una vulnerabilidad crítica es más que importante, sobre todo si afecta a dos terceras partes de los servicios que hay en Internet, como sucedió en el caso de Heartbleed. Las repercusiones de esta vulnerabilidad en OpenSSL afectaron a miles de servidores a nivel mundial ya que le permitían a un atacante leer una porción de memoria en donde se pueden alojar credenciales de acceso o las claves con las cuales se cifra la información. A raíz de este incidente la comunidad del Software Libre dio respuesta al incidente a través de la solución de la vulnerabilidad y además surgió LibreSSL, un nuevo proyecto alternativo a OpenSSL por parte del grupo de OpenBSD. Asímismo, múltiples servicios y servidores continuaron utilizando versiones vulnerables de OpenSSL, lo que dio orígenes a diferentes casos de fuga de información.

Otra de las vulnerabilidades fue Shellshock, una falla en el intérprete de comandos más utilizado de GNU/Linux y en otros sistemas basados en UNIX tales como Android y Mac OS X. Esta falla permitía la ejecución remota de código haciendo que un atacante pudiera tomar el control de un sistema afectado por esta vulnerabilidad. Shellshock fue la segunda vulnerabilidad que se reportó en el año que afectaba a una gran cantidad de sistemas. Nuevamente, la comunidad Open Source dio una pronta respuesta y los administradores de sistemas pudieron instalar los parches de seguridad. Sin embargo, se reportaron ciertos casos en que esta vulnerabilidad se utilizó para la propagación de malware.

Más allá del descubrimiento de una vulnerabilidades crítica (0-day), los atacantes suelen utilizar estos exploits para realizar diferentes tipos de ataques. Desde los laboratorios de ESET se han reportado múltiples casos en los que los cibercriminales utilizaron exploits específicos para saltear las medidas de seguridad. Entre las vulnerabilidades que se explotaron podemos mencionar las campañas de BlackEnergy dirigidas contra Ucrania y Polonia, en un caso en el que los cibercriminales eligieron exploits de Microsoft Word (CVE-2014-1761) o para Microsoft PowerPoint (CVE-2014-4114) con el fin de lograr infectar diferentes objetivos. En otras instancias, se reportaron casos de sitios web que una vez que habían sido comprometidos por los atacantes, se utilizaban para explotar vulnerabilidades en los sistemas que visitaban la página, como el caso que se relacionó con Win32/Aibatook, un troyano bancario que se propagó a través páginas para adultos en Japón, en este caso se utilizaba una vulnerabilidad de Java descubierta en el 2013.

Las vulnerabilidades de software son difíciles de predecir, pero una vez que aparecen se puede ver cómo, con el pasar del tiempo, los cibercriminales comienzan a utilizarlas, ya sea para la realización de ataques dirigidos (como parte de un APT o para que se incluyan en un Exploit Kit) o bien para propagar malware a través de un sitio web que ha sido vulnerado. Los usos son múltiples y conforman un desafío tanto para equipos de seguridad como para los usuarios hogareños: minimizar o eliminar la brecha de exposición a una vulnerabilidad es uno de los factores más importantes para poder garantizar la seguridad de un sistema.

A lo largo 2015, las vulnerabilidades serán una pieza importante en el rol de la seguridad en las empresas, ya que siempre representan un riesgo. Tal como lo hemos visto en los datos del ESET Security Report 2014, el 68% de los profesionales de América Latina que participaron del informe marcaron como su mayor preocupación la explotación de vulnerabilidades de software. Si bien no es algo para perder el sueño, sí es algo para ocuparse y aquellas empresas que decidan tomar un rol proactivo les permitirá estar un paso delante, no solo de los posibles ataques, sino

también con las técnicas para proteger sus sistemas e información. La definición de las correctas políticas de seguridad, implementación de soluciones de seguridad que permitan detectar los intentos de explotación y diferentes medidas de seguridad son las principales armas para combatir estos ataques. Algunos de los desafíos que presentan las vulnerabilidades de software se pueden mitigar con la instalación de los parches de seguridad, actualizaciones del sistema operativo o los aplicativos. En el caso de las vulnerabilidades desconocidas, los 0-days, su complejidad es mayor, por lo que la proactividad de un equipo de seguridad es una de las mejores defensas.

7 Internet of Things... ¿o Internet of Threats?

- Una puerta a las nuevas amenazas
- Más dispositivos conectados, más amenazas en línea
- Las preocupaciones de seguridad en IoT
- Las amenazas siguen la ruta de la tecnología

Dispositivos móviles

⑦ INTERNET OF THINGS... ¿O INTERNET OF THREATS?

El término "Internet of Things" (IoT) se viene manejando desde hace un par de años, y se refiere a la red de dispositivos físicos que cuentan con la tecnología necesaria para comunicar e interactuar con otros dispositivos o con humanos acerca de lo que los rodea, todo sobre Internet.

En este momento nos encontramos con ejemplos de estos dispositivos tales como automóviles, sistemas de iluminación, refrigeradores, sistemas de seguridad de casas, televisores y teléfonos. Estos son quizá los equipos más comunes hoy en día pero la lista es mucho más extensa e incluso se podría extender al ambiente empresarial considerando por ejemplo sistemas SCADA o cualquier sistema de control industrial.

Dada su creciente masividad, este tipo de dispositivos han empezado a estar en el radar de los atacantes, y dado que durante 2014 empezamos a ver algunas pruebas de concepto de amenazas para estos dispositivos, 2015 supone un reto interesante para los desarrolladores de estos productos en cuanto a seguridad se refiere.

▶ Una puerta a las nuevas amenazas

Son muchos los electrodomésticos que han evolucionado a tal punto que las últimas generaciones de una gran variedad de ellos incluyen la posibilidad de conectarse a Internet para consumir contenidos o intercambiar información que puede llegar a ser sensible.

Si bien durante el año pasado ya veíamos pruebas de concepto de, por ejemplo, amenazas en Smart TV, ya durante 2014 fuimos testigos de vulnerabilidades encontradas en estos mismos dispositivos que permitirían ataques en masa.

Incluso durante los primeros meses del año más de 300 mil enrutadores fueron atacados a nivel global y también algunos servicios de contenidos en línea fueron víctimas de fuga de contraseñas. Lo cual demuestra que no solamente los equipos utilizados son sensibles a estos ataques sino que también los mismos servicios se vuelven atractivos para los atacantes.

▶ Más dispositivos conectados, más amenazas en línea

Pero no son solamente los dispositivos del hogar los afectados. Claramente los Smart TV son los dispositivos en los que empezamos a ver los primeros ataques y vulnerabilidades, dado que son los que más se han masificado en su uso. Pero también hay otros que están empezando a utilizarse cada vez con más frecuencia y para los cuales ya vemos vulnerabilidades explotables.

De la misma manera que el año pasado vimos las primeras pruebas de concepto de ataques para afectar Smart TV, durante 2014 vimos las primeras muestras de spyware para Google Glass, lo cual puso en evidencia la preocupación por los dispositivos *wearables* y la privacidad.

▶ Las preocupaciones de seguridad en IoT

La idea de estar en ambientes cada vez más autónomos que nos faciliten la vida puede parecer muy tentador para muchos. Pero es una realidad que los fabricantes deben abordar los temas relacionados con seguridad.

Tal como algunos fabricantes de autos empezaron durante este año a ofrecer recompensas a los investigadores de seguridad para encontrar problemas de seguridad en las nuevas generaciones de sus automóviles, deberíamos empezar a ver durante 2015 cómo estos temas se vuelven relevantes.

Hay un factor adicional en cuanto a la seguridad con estos dispositivos asociados al IoT. Si bien las computadoras tuvieron tiempo para desarrollarse antes de empezar a comunicarse en complejas redes de comunicación, y cuando lo hicieron, estos entornos eran confiables por lo que la tecnología tuvo su espacio para desarrollarse. Para los nuevos dispositivos el ambiente de interacción es mucho más hostil y por lo tanto deben ser pensados desde el principio para la seguridad.

▶ Las amenazas siguen la ruta de la tecnología

La posibilidad que IoT se convierta en algo más parecido en "Internet of Threats" (Internet de las Amenazas) va a estar ligado en gran medida a dos factores fundamentales: los fabricantes y los usuarios. Hasta el momento las amenazas van a enfocarse allí donde haya una mayor cantidad de usuarios y como esto seguramente no cambie, la seguridad debe depender de otros factores.

Por lo tanto las principales consideraciones de seguridad que deberían tenerse en cuenta para el 2015 están en torno a las siguientes cuestiones:

→ Conectividad

La principal característica de estos dispositivos es permitir la interacción en Internet, por lo tanto cuidar la forma en que se conectan e intercambian información es primordial.

→ Fácil actualización

Dado que es una tecnología emergente y en desarrollo, será común encontrar vulnerabilidades que deban resolverse una vez que el usuario tiene su dispositivo. Por lo tanto la velocidad de este despliegue y la facilidad de hacerlo será importante para ganarles la carrera a los atacantes.

→ Autenticación

Al ser equipos que van a estar todo el tiempo conectados a Internet, es muy importante que se garantice que aquellos que interactúan con la información son quienes realmente dicen ser y así evitar fugas de información.

→ Aplicaciones confiables

Las particularidades de esta tecnología abren muchas posibilidades para desarrollar tareas cotidianas de forma automática. Garantizar que esto no sea aprovechado a través de aplicaciones modificadas de forma maliciosa es necesario para generar confianza en su uso.

→ Cifrado de datos

Como se maneja información que es sensible, esta debe emplearse de forma segura. Así que cifrarla es una opción para que terceros no puedan accederla para modificarla o robarla.

⑦ DISPOSITIVOS MÓVILES

Desde hace ya algunos años, siempre hemos mencionado en los informes de Tendencias del Laboratorio de ESET el rol cada vez más importante de los dispositivos móviles. La evolución de las amenazas para los *smartphones* continuó a lo largo de 2014, y hemos sido testigos de amenazas que afectaron a plataformas como Android y iOS. Con estos precedentes, queda en claro que los cibercriminales continúan dándole importancia a la información y diferentes tipos de contenidos que los usuarios almacenan en ellos.

Por el lado del sistema operativo de Google, hemos visto la aparición de SimpLocker, el primer ransomware para Android que cifra las imágenes, videos y otros archivos del *smartphone*, para luego reclamar por el pago de un rescate.

Esta familia de códigos maliciosos que afectó a los usuarios de Android fue reportada por el Laboratorio de ESET, y tras el análisis de sus instrucciones para el cifrado de la información fue posible el desarrollo de una herramienta, ESET SimpLocker Decryptor, que ayuda a los usuarios a recuperar sus archivos sin tener que pagarle a los cibercriminales.

También se han reportado nuevas variantes del malware conocido como "Virus de la Policía", que se propagaba a través de sitios maliciosos y en donde también los archivos del usuario eran cifrados.

Una situación similar se reportó también en iOS, donde la aparición de WireLurker, un malware que afectaba a dispositivos de Apple fue capaz de infectar alrededor de 400 aplicaciones según la BBC. Si bien la mayor parte de los usuarios afectados fueron de China, quedó en claro que los cibercriminales intentarán atacar las plataformas que los usuarios estén utilizando.

En base a lo que se pudo observar a lo largo de este año, para 2015, la aparición de amenazas que intenten secuestrar la información del usuario serán más recurrentes. Una vez más, las amenazas que vemos para las computadoras, tal como es el caso de CryptoLocker, comienzan de a poco a incorporar variantes para los dispositivos móviles persiguiendo el mismo objetivo: sacarle dinero a los usuarios.

⑧ Conclusión

⑧ CONCLUSIÓN

A lo largo del documento de Tendencias 2015, hemos repasado algunos de los incidentes más importantes del año. Debatimos acerca del rol de las APT en los ataques informáticos y el riesgo que representan para las empresas; recordamos cómo se fugaron más de 100 millones de tarjetas de crédito y débito a través de ataques al retail; y vimos como el ransomware logró cifrar la información de usuarios y empresas para luego pedir un rescate por ello. Pero, ¿existe una relación entre los ataques? ¿Quiénes son los afectados? ¿Cuáles con las complicaciones que esto generó a lo largo del año?

Según pasan los años, los cibercriminales continúan perfeccionando sus técnicas de persuasión y engaño, ya sea para convencer a los usuarios a través del uso de Ingeniería Social o mediante la utilización de vulnerabilidades para saltear los mecanismos de protección. La aparición de vulnerabilidades críticas, errores de programación y casos masivos de fuga de información impactaron en el mundo corporativo. Las empresas protegen su información para garantizar la continuidad del negocio, y los datos valiosos para las organizaciones son uno de los principales objetivos de los cibercriminales.

En este marco en el que la información es valiosa, el desafío de las empresas para 2015 radica en cómo van a proteger sus datos, cómo proteger su negocio y en particular, cómo lograrán que sus empleados sean parte de los programas de seguridad. En un mundo donde cada vez estamos más conectados, donde no dejamos de vivir en línea, en donde el Bring Your Own Device se convirtió en algo común en muchos lugares, los usuarios tendrán que convivir con un doble perfil. Este doble perfil del usuario consiste en que ser usuarios de diferentes servicios online como cuentas de correo, redes sociales, almacenamiento en la nube, etc. y al mismo tiempo, muchos de los usuarios de estos servicios se desarrollan profesionalmente y mantienen acceso a información clasificada. Incluso, son las personas encargadas de proteger los datos de las empresas, gobiernos u otras organizaciones.

En base a lo que hemos visto durante los últimos años con los ataques dirigidos, los casos de fuga de información y la evolución de los cibercriminales para secuestrar los datos de los usuarios y empresas; podemos asegurar que 2015, será un año lleno de desafíos en lo que respecta a la Seguridad Informática. Los equipos de seguridad informática de las empresas y gobiernos deberán adoptar un rol más proactivo en cuanto a sus defensas, previendo a través del uso de diferentes herramientas los posibles ataques y apostando a la educación como un método de defensa. Más allá de las probabilidades de lo que se puede predecir, la tendencia de que las empresas sean uno de los objetivos principales de los cibercriminales está más que claro y es algo a tener en cuenta como los riesgos para afrontar en 2015.

SOBRE ESET LATINOAMÉRICA

Fundada en 1992, ESET es una compañía global de soluciones de software de seguridad que provee protección de última generación contra amenazas informáticas y que cuenta con oficinas centrales en Bratislava, Eslovaquia, y de Coordinación en San Diego, Estados Unidos; Buenos Aires, Argentina y Singapur. En 2012, la empresa celebró sus 20 años en la industria de la seguridad de la información. Además, actualmente ESET posee otras sedes en Londres (Reino Unido), Praga (República Checa), Cracovia (Polonia), Jena (Alemania) San Pablo (Brasil) y México DF (México).

Desde 2004, ESET opera para la región de América Latina en Buenos Aires, Argentina, donde dispone de un equipo de profesionales capacitados para responder a las demandas del mercado en forma concisa e inmediata y un Laboratorio de Investigación focalizado en el descubrimiento proactivo de variadas amenazas informáticas.

El interés y compromiso en fomentar la educación de los usuarios en seguridad informática, entendida como la mejor barrera de prevención ante el cada vez más sofisticado malware, es uno de los pilares de la identidad corporativa de ESET. En este sentido, ESET lleva adelante diversas actividades educativas, entre las que se destacan la Gira Antivirus que recorre las universidades de toda la región, el ciclo de eventos gratuitos ESET Security Day y la Plataforma Educativa Online que ofrece cursos gratuitos sobre diferentes temáticas de seguridad.

Además, el Equipo de Investigación de ESET Latinoamérica contribuye a We Live Security en español, el portal de noticias de seguridad en Internet, opiniones y análisis, cubriendo alertas y ofreciendo tutoriales, videos y podcasts. El sitio busca satisfacer a todos los niveles de conocimiento, desde programadores aguerridos hasta personas buscando consejos básicos para asegurar su información en forma efectiva.

Para más información visite: ***www.welivesecurity.com/la-es***

www.eset-la.com

ENJOY SAFER TECHNOLOGY™