TENDENCIAS EN CIBERSEGURIDAD 2018: EL COSTO DE NUESTRO MUNDO CONECTADO

ENJOY SAFER TECHNOLOGY™

ÍNDICE

	Introducción	3
1	La revolución del ransomware	6
2	Aumentan los ataques a infraestructuras críticas	11
3	Ataques a la democracia: ¿puede haber procesos electorales seguros?	15
4	Condena para el cibercrimen: La policía y la investigación contra el malware se unen en la lucha	19
5	La información personal en la nueva era de la tecnología y la legislación	23
	Conclusión	27

INTRODUCCIÓN

El año en que la seguridad llegó a los grandes titulares

Dos de los hechos más resonantes de este año sin dudas fueron las infecciones masivas de ransomware de WannaCryptor primero, y de Petya/NotPetya después. Las capacidades de autorreplicación de estas amenazas ocasionaron que miles de equipos y servidores alrededor del mundo fueran tomados de rehén, a una escala y una velocidad sin precedentes hasta ese momento. Pero también ocasionaron que más y más personas empezaran a preocuparse por cuestiones de seguridad.

Estas infecciones masivas no fueron los únicos sucesos que llegaron a los medios masivos de comunicación. Recordemos la brecha en Equifax que podría haber afectado a más de la mitad de la población adulta de los Estados Unidos, o el ataque a HBO en el que fue filtrada información privada de sus actores y materiales asociados a sus producciones, como guiones o capítulos de la serie Game of Thrones. Inclusive este año Yahoo! admitió que durante la brecha de 2013 toda su base de datos había sido vulnerada, o sea que los datos de 3 billones de cuentas que incluían nombres, direcciones de correo electrónico, fechas de nacimiento, contraseñas y, en algunos casos, preguntas y respuestas de seguridad, fueron comprometidos.

Y esto no es todo: durante este año también se habló de las acusaciones de interferencia rusa durante las elecciones presidenciales de los Estados Unidos en 2016; del descubrimiento de KRACK, una vulnerabilidad en el sistema de cifrado WPA2 que dejaba inseguras a las conexiones Wi-Fi; y de Industroyer, la mayor amenaza para sistemas de control industrial desde Stuxnet, que podría adaptarse para afectar distintos tipos de infraestructuras críticas como suministros de agua, luz y gas.

Como podrás ver, este fue un año ajetreado en términos de seguridad y que vino a cristalizar varias de las preocupaciones que venimos planteando los últimos años en los documentos de Tendencias, escritos por los expertos en seguridad de ESET. Las noticias de seguridad abarcan cada vez más espectros de nuestra vida cotidiana e impactan sobre audiencias cada vez mayores y más diversas.

El avance de la tecnología y su rápida adopción genera que varios escenarios que hace algunos años parecían impensados, hoy se encuentren en el terreno de lo posible. Sobre todo ahora, cuando empieza a aflorar la evidencia de que muchos sistemas y protocolos que usamos no fueron diseñados considerando la seguridad, porque no fueron creados para ser conectados a Internet. ¿Cómo solucionar esto sin volver hacia atrás en nuestras capacidades tecnológicas?

En este informe, los especialistas de seguridad de ESET van a presentar los principales ejes de seguridad que creemos que serán clave para el próximo año y analizarán las formas de enfrentarlos. Confiamos en que este ejercicio de mirar hacia adelante permita a todos los actores involucrados y preocupados por la seguridad de la información reflexionar, debatir y prepararse para los desafíos de hoy y de mañana.

1

La revolución del ransomware

- Ransomware con características de gusano
- Brotes globales
- Rescate sin .ware
- Otros tipos de ransomware
- RaaS: Ransomware como Servicio

AUTOR

David Harley
ESET Senior Research Fellow

La revolución del ransomware

Aquí es donde yo entré en escena, hace casi 30 años. El primer brote de malware sobre el que presté servicios de consultoría fue el extraordinario troyano del SIDA del Dr. Popp, que dejaba los datos de la víctima inaccesibles hasta que pagaba una "renovación del contrato de software". Y hasta mucho tiempo después, no hubo otros casos que pudieran considerarse ransomware, a menos que contemos las amenazas a organizaciones mediante ataques de denegación de servicio distribuido (DDoS) persistentes.

(De)negación plausible

Mientras que los ataques de denegación de servicio (DoS), intensificados por el uso de redes de equipos infectados con bots, se convirtieron en un problema notable hacia el cambio de siglo, las amenazas de extorsión mediante la denegación de servicio distribuido también fueron aumentando a la par del ransomware en los últimos años, aunque menos dramáticamente.

Sin embargo, es probable que las estadísticas no sean precisas por dos razones: en primer lugar, muchas organizaciones que son víctimas de ataques prefieren no revelarlo al público y, en segundo, cada vez son más los ataques de DDoS cuya motivación es política en lugar de económica. Pero además existen otras interacciones complejas entre distintos tipos de malware: hubo casos de variantes de ransomware que incorporaron un bot de DDoS, y más recientemente los operadores de la botnet Mirai condujeron un ataque de DDoS contra el interruptor de apagado (o "kill switch") de Wannacryptor (también conocido como Wannacry) para que se reactivaran las copias ya inactivas de este malware.

La metamorfosis del gusano

Claro está que el malware detectado por ESET como Win32/Filecoder.WannaCryptor es mucho más complejo que el factor Mirai. La combinación del ransomware con el gusano aceleró la propagación del malware, aunque no tan dramáticamente en términos de volumen como algunos de los ataques de gusanos que observamos durante la primera década de este milenio, en parte porque su propagación se basaba en el aprovechamiento de una vulnerabilidad que muchos usuarios ya habían corregido. Sin embargo, su impacto financiero en organizaciones importantes llamó la atención de los medios de todo el mundo.

Si pagas, cruza los dedos

Una de las peculiaridades de Wannacryptor era que, con bastante frecuencia, cuando la víctima pagaba el rescate, no recuperaba todos sus datos. De todas formas, no es la primera vez que pasa: hay muchísimos ejemplos de ransomware donde los delincuentes no fueron capaces de recuperar algunos o directamente ninguno de los datos, ya sea debido a una codificación defectuosa o porque nunca tuvieron la intención de hacerlo. Ranscam y Hitler, por ejemplo, simplemente borraban archivos: no los cifraban y no había forma de que el delincuente pudiera ayudar a recuperarlos.

Por suerte, estos casos en particular no parecen haberse propagado demasiado.

Sin embargo, quizás el ejemplo más notable es un troyano similar a Petya detectado por ESET como Diskcoder.C, que sí cifra los datos. Si observamos la gran habilidad con la que se ejecuta este malware, el hecho de que carezca de un mecanismo de recuperación no parece accidental. Más bien, el objetivo de este troyano es tomar todo el dinero que pueda y escapar lo antes posible.

Limpiadores de discos

A pesar de que el malware conocido como NotPetya no se abstiene de sacar algún beneficio haciéndose pasar por un ransomware y pidiendo rescate, otros tipos de malware limpiadores de discos claramente tienen una agenda diferente, como el malware Shamoon, que reapareció hace poco. Entre los tipos de malware con funcionalidad de limpiadores de discos y que estuvieron dirigidos a objetivos ucranianos se encuentran Killdisk (asociado a Black Energy) y, más recientemente, Industroyer.

¿Qué podemos aprender de estas tendencias?

Para un atacante, secuestrar datos es una forma bastante sencilla de generar beneficios fraudulentos, y la destrucción de datos por otros motivos (como la agenda política) parece ir en aumento. Pero en lugar de especular sobre todas las posibles variaciones en torno a la destrucción de datos, veamos algunas medidas que reducen el riesgo en general.

1. Entendemos que las personas deciden pagar con la esperanza de recuperar sus datos, por más que sepan que de esta forma están alentando a los delincuentes a seguir con este tipo de ataques. Sin embargo, antes de pagar, consulta a tu proveedor de software de seguridad (a) si la recuperación es posible sin pagar el rescate y (b) si hay probabilidades de que el pago del rescate permita la recuperación de los archivos en el caso específico de la variante de ransomware que te infectó.

2. Proteger tus datos en forma proactiva es más seguro que confiar en la capacidad y la buena fe de un delincuente. Haz backups periódicos de todo lo que te importa y mantén al menos algunas copias de seguridad offline, en medios que no estén habitualmente expuestos a ataques de ransomware u otro malware, en una ubicación físicamente segura (en lo posible, en más de una ubicación). Y, obviamente, los backups protegen tus datos ante cualquier otro riesgo que puedan sufrir.

3. En la actualidad, cuando las personas y organizaciones piensan en el backup, no suelen hacerlo en términos de medios físicos como discos ópticos y unidades flash, sino en términos del almacenamiento en la nube. Pero de todas formas recuerda que, aunque dicho almacenamiento se encuentre fuera del sitio, si está "siempre encendido", su contenido puede ser vulnerable a las infecciones de ransomware de la misma manera que el almacenamiento local. Es importante que el almacenamiento fuera del sitio:

   a. No permanezca online de manera habitual ni permanente;
   b. Proteja los datos almacenados cuando el centro remoto esté online, de modo que un malware no pueda modificarlos o sobrescribirlos en forma automática y silenciosa;
   c. Proteja de infecciones a las generaciones anteriores de datos respalda-

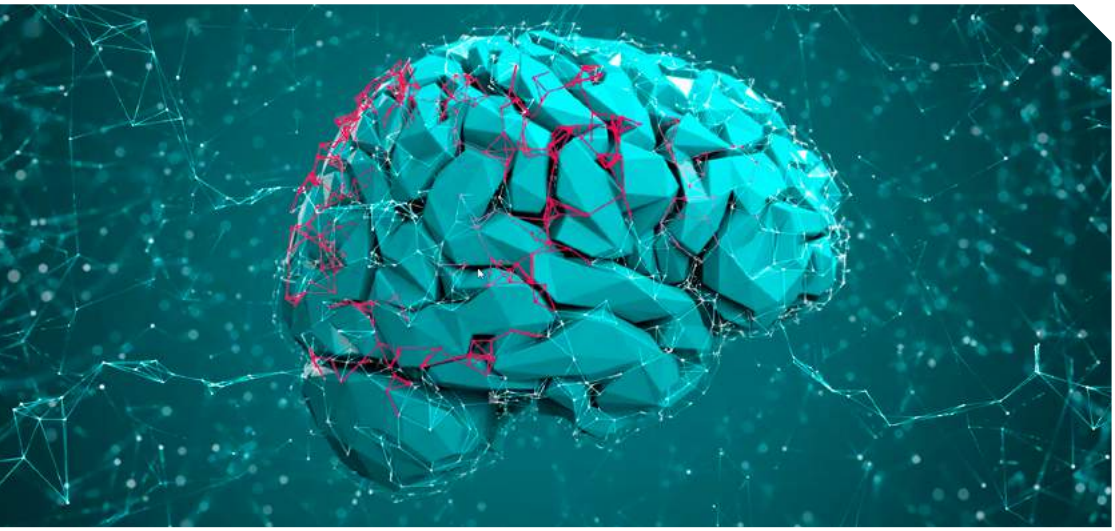
Haz respaldos de todo lo que te importe de manera frecuente y manteniéndolos offline en una locación física segura.

dos para que, incluso si ocurriera un desastre que afectara a los últimos backups, al menos puedas recuperar algunos datos, incluyendo las versiones anteriores de los datos actuales;

d. Proteja al cliente explicando las responsabilidades legales y contractuales del proveedor, indicando qué pasará si el proveedor cierra la empresa, etc.

4. No subestimes la utilidad de los medios de backup que no son regrabables o reutilizables. Si tú no puedes modificar lo que se ha escrito allí, tampoco podrá el ransomware. De vez en cuando, comprueba que tus operaciones de backup y recuperación aún sigan funcionando correctamente y que tus medios (con acceso de solo lectura, con escritura deshabilitada o con escritura habilitada) todavía sean legibles (y que los medios con escritura habilitada no se sobrescriban en forma habitual). Y haz un backup de tus backups.

5. Definitivamente no voy a decir que los backups deben reemplazar el uso de un software de seguridad, pero recuerda que una cosa es *eliminar* un ransomware activo con un software de seguridad que detecta ransomware y otra muy distinta es recuperar datos cifrados: si eliminas el ransomware y luego decides pagar, es posible que los datos ya no se puedan recuperar, incluso con la cooperación de los delincuentes, porque el mecanismo de descifrado es parte del malware. Por otro lado, bajo ningún motivo vas a querer restaurar tus datos en un sistema donde el ransomware aún sigue activo. Afortunadamente, los backups seguros pueden salvar tus datos en caso de que se filtre algún código malicioso y logre evadir tu software de seguridad.



¿Qué nos depara el futuro?

"No hagas predicciones sobre la informática que se puedan verificar durante tu vida"; sabias palabras de Daniel Delbert McCracken. Aún así, podemos arriesgarnos a hacer cierta extrapolación basándonos en la evolución reciente del ransomware para ofrecer algunas reflexiones cautelosas sobre su futura evolución.

Con objetivos específicos de ataque

El objetivo de ataque del Troyano del SIDA, por ejemplo, fue bastante específico. Incluso entonces, no mucha gente estaba interesada en las minucias de la investigación sobre el SIDA, y la distribución del troyano en un disquete era relativamente costosa, por lo que el mecanismo para pagar el rescate no llegó a funcionar realmente en beneficio del atacante. Claro que el Dr. Popp no contaba con las ventajas modernas del acceso a la criptomoneda o a la Dark Web, ni siquiera de Western Union (el medio de pago favorito de los perpetradores de la estafa nigeriana), o de monetizar fotografías de desnudos.

El ataque en sí era el "clásico" ransomware, ya que le impedía a la víctima el acceso a sus propios datos. Un poco más tarde, los ataques DoS y DDoS privaban a las empresas de beneficiarse de los servicios que brindaban: si bien quienes se veían privados de los servicios en sí eran los clientes, quien se esperaba que pagara era el proveedor. Sin embargo, así como el uso no corporativo de Internet se ha disparado, la superficie de ataque y el rango de objetivos potenciales también se extendieron, lo que probablemente influye en la distribución indiscriminada del ransomware más moderno.

Sin objetivos específicos de ataque

Mientras que los medios y los vendedores de productos de seguridad tienden a entusiasmarse cuando se divulga un objetivo muy conocido o de alto valor (como sitios de entidades médicas, instituciones académicas, proveedores de servicios de telefonía o de Internet), es inapropiado suponer que estas instituciones son siempre objetivos de ataques específicamente dirigidos.

Como muchas veces no sabemos qué vector de ataque utilizó una campaña específica, no podemos asegurar que lo sean. Pero parece que a las bandas criminales de ransomware les está yendo bastante bien con los pagos que reciben de las grandes instituciones infectadas a través de ataques laterales, donde un empleado resultó ser una víctima mientras usaba sus cuentas laborales. NHS Digital, por ejemplo, niega que los servicios de la salud sean un objetivo de ataque específico (lo que casualmente comparto en líneas generales), si bien reconoce que los sitios de entidades sanitarias a menudo han sido víctimas.

¿Esto podría cambiar?

Por el momento, todavía parece haber organizaciones que están preparadas para gastar sumas relativamente grandes en el pago de un rescate. En algunos casos, se trata de una "estrategia de respaldo" razonable, ya que es sensato tener una reserva de dinero separado en caso de que fallen las defensas técnicas.

Pero en otros casos, las empresas creen que pagar un rescate les resultará menos costoso que construir defensas adicionales complejas que no siempre van a ser totalmente efectivas. Esta concepción en sí misma incentiva a los atacantes, ya que considerarán que las empresas son incautas y sabrán que están dispuestas a pagar el rescate. El hecho de que cada vez haya más cantidad de ataques de limpiadores de discos y más casos de ransomware donde el pago no implica la recuperación de los archivos puede mitigar esta mala costumbre.

No obstante, las empresas que aún se muestran poco dispuestas a fortalecer sus defensas al máximo de sus capacidades podrían ser las que reciban más ataques dirigidos. Después de todo, es más probable que un ataque exitoso a una organización grande pague mejor y más rápido que los ataques masivos dirigidos a usuarios y a direcciones de correo electrónico al azar.

Datos versus dispositivos

Con respecto a los ataques a smartphones y otros dispositivos móviles, tienden a enfocarse menos en los datos y más en impedirle a la víctima el uso de su dispositivo y los servicios que facilita. Esto es un verdadero problema cuando la alternativa de pagar un rescate es perder configuraciones y otros datos, especialmente a medida que son más las personas que usan los dispositivos móviles en lugar de las computadoras personales o incluso las portátiles, de modo que la gama de datos que podría verse amenazada es más amplia.

A medida que la Internet de las Cosas conectadas innecesariamente se vuelve menos evitable, crece la superficie de ataque, con dispositivos en red y sensores integrados en elementos y contextos inesperados: desde routers hasta heladeras y medidores inteligentes, desde televisores hasta juguetes, desde centrales eléctricas hasta estaciones de servicio y marcapasos. Como todo se vuelve más "inteligente", aumenta la cantidad de servicios que pueden verse afectados por el malware (más allá de que exija un rescate o no).

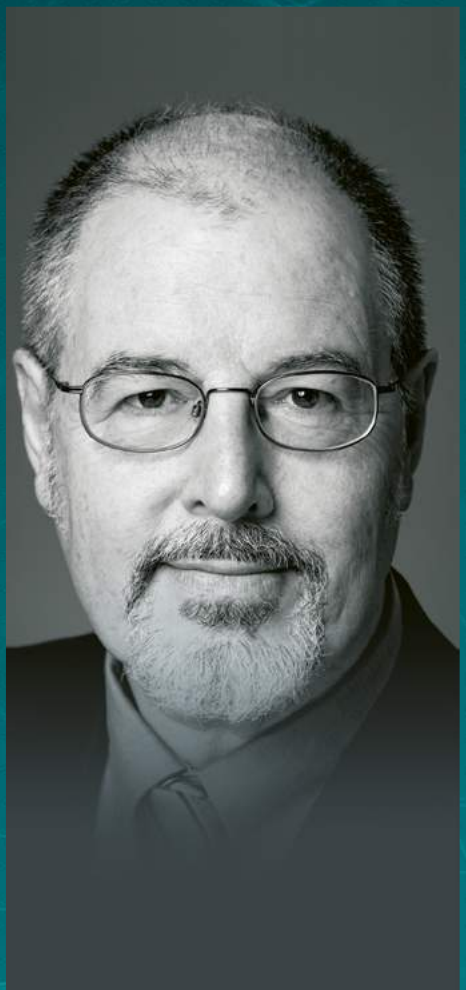
En años anteriores ya hemos discutido las posibilidades de lo que mi colega Stephen Cobb llama el Ransomware de las Cosas. Hay menos ejemplos *in the wild* de tales amenazas de lo que cabría esperar, dada la atención que atraen. Sin embargo, eso podría cambiar con facilidad, en especial si el ransomware más convencional se vuelve menos efectivo como medio de ganar dinero rápidamente. Aunque no creo que vaya a ocurrir muy pronto...

Por otro lado, no hay muchos indicadores de que la seguridad de la Internet de las Cosas esté evolucionando a la par de los dispositivos de la IoT. No obstante, ya estamos viendo un gran interés de los atacantes en la monetización de la inseguridad de la IoT. La creación y distribución de malware capaz de afectar una amplia gama de dispositivos de la IoT no es tan simple como los medios a veces nos hacen creer, por lo que no hay motivo para entrar en pánico; pero tampoco debemos subestimar la tenacidad y la capacidad del mundo digital para sorprendernos con un giro inesperado.

2

Aumentan los ataques a infraestructuras críticas

- Los ataques a infraestructuras críticas siguen creciendo
- Casos de éxito de ESET: Industroyer & Black Energy
- Ataques a cadenas de suministro
- ¿Por qué esto también podría pasar en tu país?



AUTOR

Stephen Cobb
ESET Senior Security Researcher

Aumentan los ataques a infraestructuras críticas

En enero de 2017 las amenazas a infraestructuras críticas fueron noticia cuando un informe de Reuters aseguró que el reciente corte de energía eléctrica en Ucrania "fue un ataque cibernético". En nuestro informe de Tendencias del año pasado, dijimos que los ataques a la infraestructura probablemente continuarían "llegando a los titulares y perturbando la vida cotidiana en 2017". Lamentablemente teníamos razón, y debo decir que es probable que esta misma tendencia siga vigente durante 2018 por los motivos descritos en esta actualización del informe.

Cabe señalar que la infraestructura crítica no solo abarca la red eléctrica, sino que también incluye los sectores de defensa y salud, procesos de fabricación cruciales, producción de alimentos, agua y transporte.

Apágalo y vuélvelo a prender

Veamos cómo fueron progresando las cosas con el paso del tiempo. A fines de diciembre de 2015, los ciberataques contra empresas de energía eléctrica ucranianas provocaron cortes en el suministro del servicio a cientos de miles de hogares en esa parte del mundo por varias horas. El primer artículo publicado por los investigadores de ESET en 2016 fue el análisis de Anton Cherepanov sobre BlackEnergy, el código malicioso utilizado en este ataque en particular. Este malware no manipulaba directamente los dispositivos del sistema de Control Industrial (ICS, en inglés), pero les permitía a los atacantes penetrar en las redes de empresas de distribución de energía eléctrica y dañar el software utilizado por los equipos de ese Sistema. Sin embargo, los informes de prensa de aquel momento (algunos con titulares llamativos como "Malware apaga las luces") no aclaraban esta distinción.

El ataque de fines de 2016, reportado por primera vez en enero de 2017, fue bastante diferente, como informaron los investigadores de ESET Anton Cherepanov y Robert Lipovsky en WeLiveSecurity. Habían encontrado un nuevo malware capaz de controlar directamente los interruptores de la subestación de electricidad y los interruptores de circuito; en algunos casos podía literalmente apagar los interruptores y volver a encenderlos (lo que, a gran escala, podía interrumpir gravemente el suministro energético).

Los investigadores llamaron a este malware Industroyer y dejaron en claro que se trataba de la mayor amenaza para los Sistemas de Control Industrial desde Stuxnet. Cuando presentaron su análisis del malware en Black Hat USA 2017, la sala de conferencias estaba abarrotada y el silencio era absoluto.

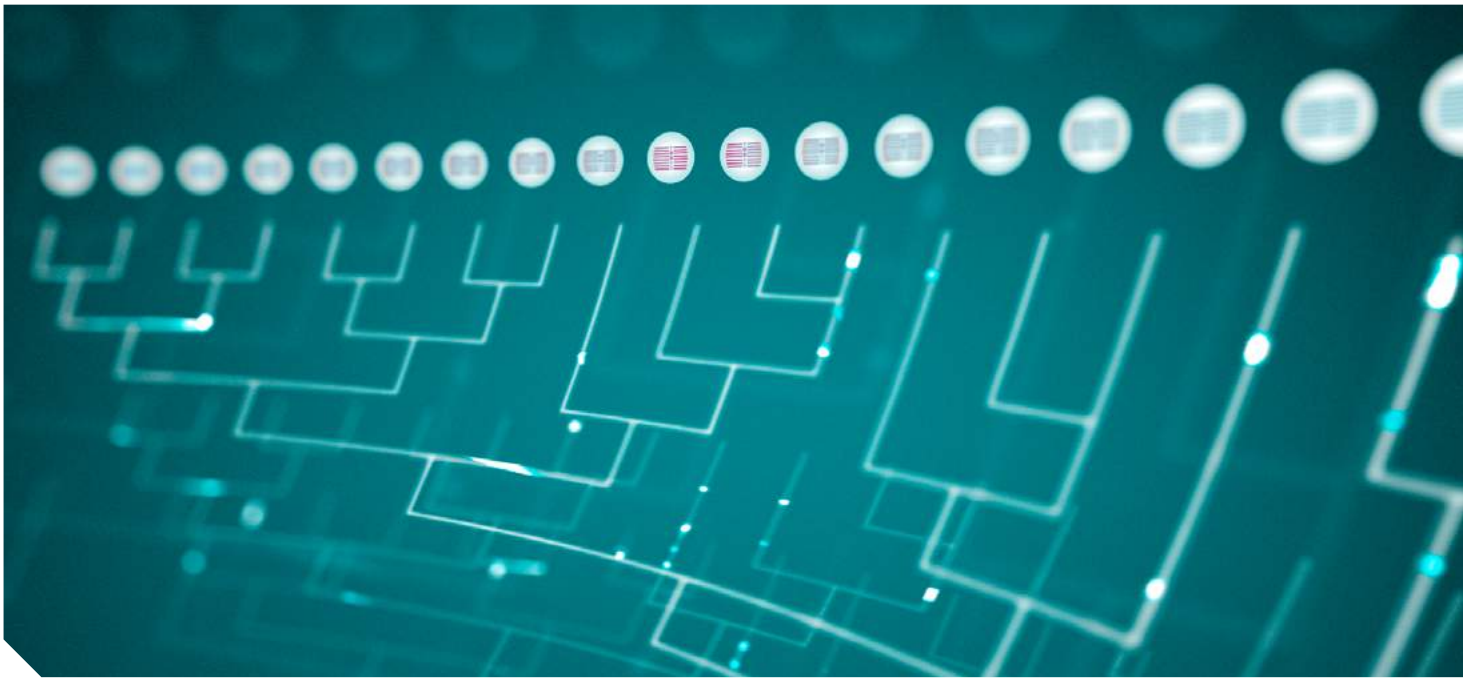
Las implicaciones de Industroyer para el futuro de las amenazas a infraestructuras críticas son, como mínimo, preocupantes, como se puede notar en esta entrevista a Robert. El equipamiento industrial al que está dirigido Industroyer es ampliamente utilizado en varias partes de mundo (no solo en Ucrania, sino también por ejemplo en el Reino Unido, la Unión Europea y los Estados Unidos) y en múltiples sectores críticos. Además, muchos de los equipos de un Sistema de Control Industrial que aún se usan hoy en día no fueron diseñados teniendo en cuenta la conectividad a Internet, por lo que las medidas de protección son difíciles de implementar.

Es cierto que muchas de las organizaciones que actualmente operan infraestructuras críticas están trabajando arduamente para protegerlas, y la investigación de ESET sugiere que los atacantes que usan Industroyer necesitarán adaptar su malware a cada objetivo específico. Esto podría limitar los ataques a empresas que cuentan con los recursos financieros suficientes, e impedir las campañas generalizadas de malware que intentan provocar apagones, paralizar el transporte o detener los procesos de fabricación cruciales.

Sin embargo, no es raro que dichos parámetros cambien con el tiempo a medida que se refina el código y se recaba más información. En otras palabras, la capacidad de llevar a cabo ataques en la red eléctrica tenderá a aumentar en 2018, a menos que se tomen medidas preventivas, como la actualización de los sistemas, la detección temprana de amenazas en la red mediante inspecciones constantes, y una mejora drástica en la detección y evasión del phishing.

Infraestructura y cadena de suministro

Desafortunadamente, actualizar equipos antiguos de Sistema de Control Industrial con nuevos equipos diseñados con conexión a Internet no mejorará automáticamente la seguridad. Como señala Stephen Ridley, fundador y CTO de Senrio, una empresa dedicada a la seguridad de los dispositivos conectados: los dispositivos industriales están cambiando de circuitos integrados de aplicaciones específicas (ASIC) a arquitecturas de sistemas en chip (SoC), más genéricos y económicos, para los cuales las bibliotecas de código se encuentran fácilmente disponibles.



Si bien este nuevo enfoque permite reducir costos, también introduce debilidades en la cadena de suministro, como los chips que tienen vulnerabilidades difíciles de corregir y la reutilización del código que genera vulnerabilidades de software. Algunos ejemplos de 2017 son la vulnerabilidad

"Devil's Ivy", que infectó a más de 200 modelos diferentes de cámaras de seguridad fabricadas por Axis Communications, y la vulnerabilidad "BlueBorne", que afectó a varios miles de millones de dispositivos en las plataformas Windows, Linux, iOS y Android. Seguramente aparecerán muchos más casos en 2018.

Un tipo diferente de amenaza ocasionada por vulnerabilidades en la cadena de suministro fue noticia en 2017, en parte porque afectó a la industria del entretenimiento. Aunque podría decirse que no se trata de una infraestructura crítica, las lecciones que este sector aprendió a la fuerza en 2017 son valiosas para las partes verdaderamente críticas de la economía. El pedido de rescate a Netflix a cambio de no filtrar contenido inédito de "Orange is the New Black" y el robo digital de la última película de Piratas del Caribe revelan dos aspectos preocupantes de la seguridad en la cadena de suministro.

En la actualidad, muchas grandes empresas parecen estar tomando en serio este problema y se aseguran de que sus equipos de seguridad cuenten tanto con el presupuesto como con el respaldo de los gerentes corporativos, ambos fundamentales para que puedan hacer un buen trabajo. No obstante, muchas empresas pequeñas que les suministran bienes y servicios a estas organizaciones más grandes tienen graves dificultades para mantenerse al día con la ciberseguridad. Dichas empresas pueden convertirse en objetivos atractivos a ataques si, por ejemplo, tienen una película multimillonaria en sus sistemas de procesamiento de audio de postproducción, que casualmente están conectados a la red de su oficina, cuyos usuarios no fueron capacitados para reconocer un correo electrónico de phishing.

En 2017, las deficiencias de ciberseguridad de esos proveedores pequeños demostraron ser un medio para comprometer objetivos más grandes, como un gran estreno de Hollywood. Como fueron varios los casos de alto perfil que llegaron a las noticias, preparé algunos consejos sobre la seguridad en las cadenas de suministro, que también son relevantes para las organizaciones involucradas en infraestructuras críticas. Después de todo, a los atacantes les puede resultar difícil comprometer la red de una gran corporación de servicios públicos de manera directa, pero ¿qué pasa, por ejemplo, con la empresa que le suministra el servicio de limpieza?

En los viejos tiempos, solíamos preocuparnos por el "ataque del conserje malvado", en el que un conserje con problemas éticos, pero con conocimientos informáticos, obtenía acceso no autorizado a la red, mientras tomaba un descanso de sus tareas de limpieza en una oficina durante el turno de la noche.

Si bien esa amenaza no ha desaparecido del todo, hay que sumarle la de una empresa de limpieza que no cuenta con ciberseguridad y que, asimismo, se conecta a los sistemas de una planta de energía eléctrica, a través de un portal de servicios para proveedores que no está suficientemente segregado de la red del Sistema de Control Industrial.

¿Cuáles son las implicancias de esto? Las organizaciones de infraestructuras críticas deben seguir mejorando su seguridad en 2018, reduciendo la efectividad de los ataques de phishing (que aún es el vector de ataque de elección), segregando y controlando el acceso a la red, revisando y probando hardware y software tanto viejo como nuevo, e incorporando diligencia debida para sus proveedores en materia digital. También deben estar atentas y ser capaces de reaccionar ante las detecciones provenientes de las inspecciones y los monitoreos de su red que puedan estar indicando la presencia de un ciberataque.

Los atacantes podrían encontrar dificultades en ingresar directamente en una compañía, pero en su lugar podrían atacar a la empresa que brinda los servicios de limpieza.

3

Ataques a la democracia: ¿puede haber procesos electorales seguros?

- Voto electrónico y voto en Internet
- Hacktivismo y ataques durante campañas electorales
- Cómo la seguridad puede cambiar la dirección de un país

AUTOR

Camilo Guttierrez
ESET Head of Awareness and Research

Ataques a la democracia: ¿puede haber procesos electorales seguros?

En los últimos dos años hubo contiendas electorales en muchos de los países más influyentes a nivel mundial. Luego de estas elecciones quedaron muchas preguntas, pero la principal es: ¿podría un ciberataque influir en un fraude electoral a tal punto que cambie el rumbo político de una nación?

Cualquier respuesta a la pregunta sería temeraria, pero sin lugar a dudas estamos en un panorama que plantea desafíos. Hay suficiente evidencia para afirmar que el voto electrónico dista de tener una implementación segura en los países que lo probaron, como revisaremos más adelante.

Sumado a eso, hay otros dos ejes sobre los cuales es necesario volcar la atención. En primer lugar, la influencia de las redes sociales en la opinión pública y su uso como herramientas de hacktivismo; y en segundo lugar, la necesidad de incluir asuntos de ciberseguridad nacional dentro de la gestión política.

Sistemas de voto electrónico inseguros

La inclusión de la tecnología en los procesos electorales era cuestión de tiempo, especialmente considerando las razones por las que algunos países (como Argentina, Brasil, Alemania o Estados Unidos) decidieron implementar en alguna medida el voto electrónico: acabar con el fraude, regularizar y acelerar el conteo, y complementar los registros en papel.

El problema empieza cuando no se complementan, sino que se reemplazan. Es verdad que no se puede frenar el avance de la tecnología, pero quizá se deben reorientar todos los esfuerzos hacia mecanismos adicionales de control y no hacia un modelo que, en realidad, lo que hace es agregar nuevos puntos de falla, sin eliminar los riesgos: así como jefes de campaña, militantes u otros actores han encontrado la forma de hacer fraude a lo largo de los años, explotando el sistema electoral físico, los cibercriminales encontrarán la forma de explotar el sistema digital, sobre todo si cuentan con algún tipo de patrocinio.

Ya en 2006 Harri Hursti había demostrado en el célebre documental *Hacking Democracy* que podía comprometer por completo al sistema de voto Diebold en el Condado de León, Florida, usando una tarjeta de memoria. Así pudo cambiar todos los votos sin ser detectado, pero el software, con algunas variaciones, nuevo nombre y nuevo dueño, sigue siendo usado en Estados Unidos para contar votos.

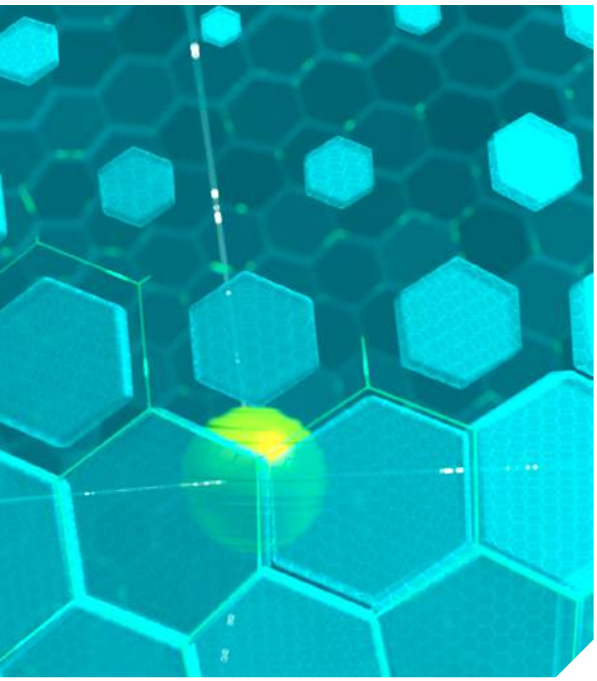
Han pasado más de 10 años y poco cambió, excepto la aparición de más evidencia. La urna electrónica de Brasil está rodeada de polémica desde 2012, cuando se descubrió que era posible quebrar completamente el carácter secreto de los votos. Luego de años en donde se demostraron muchas vulnerabilidades en este sistema, el Tribunal Superior Electoral volverá a adoptar (de manera híbrida) el registro en papel de los votos, en el 5% de las urnas de las elecciones de 2018.

En tanto, en Argentina y Alemania también se han demostrado vulnerabilidades en la transmisión de votos.

Entonces, la tendencia indica que no podemos depender de la tecnología en algo tan sensible como un proceso electoral: debemos usarla como herramienta complementaria. Si la idea es mitigar el fraude en cualquiera de sus formas, contemplemos sistemas híbridos, con registro de votos tanto electrónico como en papel.

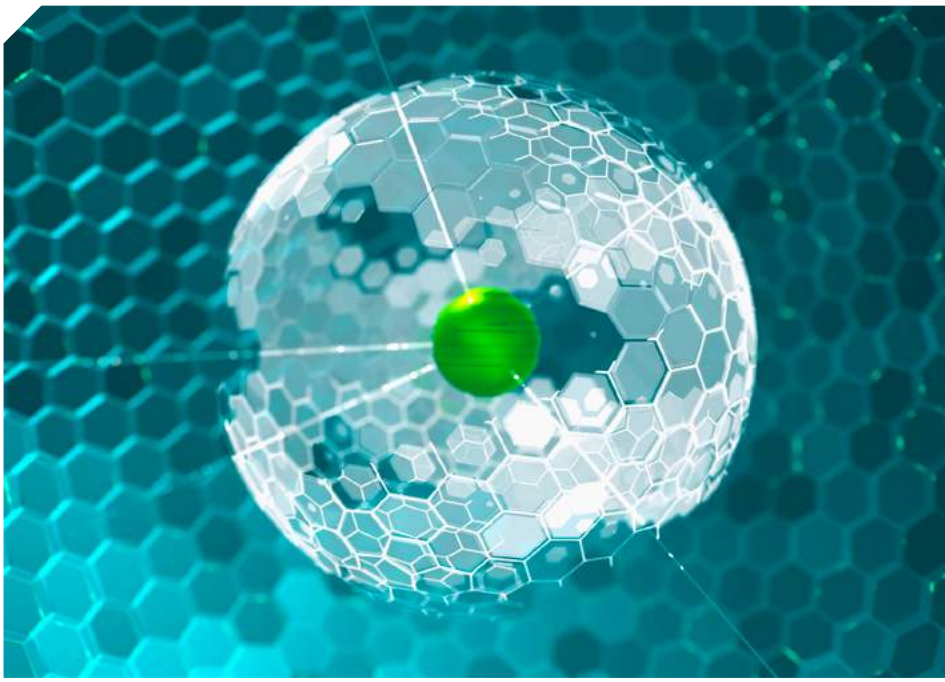
Hacktivismo para cambiar la opinión pública

Las interacciones de carácter político no han escapado del alcance del fenómeno que son las redes sociales. Se usan como plataformas de campaña para llegar a una mayor cantidad de personas, y también fuimos testigos de su uso para desestabilizar campañas electorales a través del esparcimiento de rumores, la creación de falsas noticias y, por supuesto, los ataques masivos y los dirigidos a personajes públicos.



El detalle es que muchos de estos ataques se hacen utilizando bots, amenazas informáticas u otro tipo de herramientas maliciosas que, con una adecuada gestión de la seguridad en campañas electorales, podrían evadirse. De lo contrario, lo que parecería la expresión popular termina siendo la manifestación de un grupo de atacantes.

Que esto permita manipular o sesgar la opinión pública no significa el apocalipsis de la democracia, pero sí implica retos de seguridad para garantizar una participación política sana.



Ya durante el pasado mes de julio fue anunciado el programa "Defending Digital Democracy", que cuenta con la participación y el patrocinio de empresas como Facebook y Google. Esto es un reflejo de la importancia de considerar la protección de este tipo de mecanismos.

En la medida en que las partes involucradas no tomen cartas en el asunto, seguiremos viendo estos incidentes en el futuro.

Ciberseguridad nacional

Si la tecnología forma parte de nuestras vidas, entonces dentro de las responsabilidades de un Gobierno está garantizar que los usuarios puedan interactuar con ella de la forma más segura posible, a través de un programa de ciberseguridad a nivel nacional y la incorporación de figuras como CISOs y auditores.

Y si los funcionarios, como por ejemplo las autoridades de tribunales o comisiones electorales, tienen que tomar decisiones sobre implementación de tecnologías, entonces deben tener una formación en ciberseguridad a la altura de las circunstancias para elegir con precisión.

Hay que considerar que con nuevos avances aparecen nuevos riesgos, y si queremos usar la tecnología para mejorar nuestras vidas, no dejemos que cree nuevos problemas. Todo lo que tiene que ver con el sistema electoral debería empezar a considerarse parte de la infraestructura crítica de cada país (y ser cuidado como tal).

Los desafíos están planteados. Es momento de ejecutar las acciones de prevención pensando en la seguridad digital de la información y que todos los actores involucrados aporten las soluciones para garantizar la correcta ejecución de los procesos democráticos.

Las redes sociales también han sido utilizadas para socavar campañas electorales al difundir falsedades y promocionar noticias falsas. Esto sin mencionar los ataques a la reputación de figuras públicas.

4

Condena para el cibercrimen: La policía y la investigación contra el malware se unen en la lucha

- Interrupciones, prisión y cómo ESET combate la actividad cibercriminal
- Caso de éxito: cómo Windigo ayudó a encarcelar a un atacante
- ¿Por qué nos debería importar?

AUTOR

Alexis Dorais-Joncas
ESET Senior Security Researcher

Condena para el cibercrimen: La policía y la investigación contra el malware se unen en la lucha

El objetivo primordial del análisis de malware es determinar cómo funciona una muestra del mismo, extraer IOCs (Indicadores de Compromiso) y determinar el potencial de las contramedidas. Este trabajo es de naturaleza técnica casi en su totalidad: se focaliza en archivos binarios y sus propiedades. Los resultados del análisis de malware son cruciales para las organizaciones, para permitirles defenderse ante un brote o remediar una infiltración del momento. También son cruciales para los proveedores de software de seguridad, permitiéndoles construir mejores sistemas de detección y medidas de protección para sus clientes.

Pero a veces, otro tipo de preguntas requiere de respuestas. ¿Está este archivo relacionado con este otro? ¿Cómo está construida la infraestructura de C&C (comando y control) y cómo funciona el protocolo de comunicación? ¿Cómo monetiza la botnet sus actividades, con pago por instalación, spam, redirección de tráfico?

Responder preguntas como estas es de lo que se encarga la investigación de malware. Permite una mejor comprensión del cuadro general que hay detrás de una muestra de malware aislada, para conectar los puntos y entender qué es lo que está sucediendo.

Por supuesto, esto también ayuda al software de seguridad, en otras palabras, a los proveedores de Antivirus a diseñar una mejor protección. Pero la información que se obtiene de la investigación de malware también puede ser útil para reforzar la ley en la lucha contra el cibercrimen. ¿Cómo? Tomemos algunos ejemplos de los trabajos hechos por ESET que han contribuido a desmontar operaciones maliciosas.

Campaña contra Dorkbot

En 2015, ESET fue invitado a participar de la campaña de Erradicación Coordinada de Malware (CME) organizada por Microsoft contra la familia de malware Win32/Dorkbot. Dorkbot era un kit que estaba a la venta disponible en foros clandestinos, que infectó más de un millón de computadoras, abarcando múltiples botnets independientes. El objetivo de esta campaña de CME era discontinuar de manera masiva la mayor cantidad posible de estas botnets al dar de baja de manera simultánea las infraestructuras C&C relacionadas.
Para apoyar esta operación, los investigadores de malware de ESET automatizaron el proceso de extracción de información C&C de los binarios de Dorkbot. Aplicamos este proceso a nuestro flujo de muestras de Dorkbot, tanto nuevas como ya existentes. Luego "limpiamos" manualmente los resultados al borrar sinkholes conocidos y dominios/IPs limpias para mitigar el riesgo de dar de baja recursos legítimos. Microsoft fusionó esa información con la propia para crear una lista exhaustiva de todos los nodos C&C activos a los cuales apuntar. Esta lista completa fue luego compartida con las agencias de fuerzas de seguridad alrededor del mundo como la Canadian Radio-television and Telecommunications Commission (CRTC), el Computer Emergency Readiness Team del Departmento de Seguridad Nacional de los Estados Unidos (DHS/US CERT), Eu-

ropol, el Federal Bureau of investigation (FBI), Interpol y el Royal Canadian Mounted Police (RCMP). El día de la operación, las notificaciones y órdenes judiciales fueron ejecutadas de manera coordinada.
A partir de entonces, ha habido un marcado declive en la actividad de Dorkbot alrededor del mundo, indicando que la campaña de CME fue un éxito.

Nuestra contribución fue compartir información técnica proveniente de nuestra investigación, tal como las IPs infectadas, información obtenida de los mensajes de spam enviados por la botnet y otra información relevante y disponible de manera pública, como la información del registro de dominio.

Equipado con esa información, el FBI fue capaz de hacer su parte, lento pero seguro. A comienzos de 2015, un ciudadano ruso llamado Maxim Senakh fue identificado como

Windigo y la botnet Ebury

ESET publicó por primera vez un exhaustivo análisis técnico de lo que bautizamos Operación Windigo en 2014. En resumen, Windigo estaba soportado por un backdoor que robaba credenciales que infectó a miles de servidores Linux, en los cuales eran instalados uno o más componentes maliciosos adicionales para monetizar la botnet con actividades como el envío de spam o el redireccionamiento de tráfico HTTP. Luego de la publicación, comenzamos a colaborar con el FBI en su investigación sobre los cibercriminales detrás de Operación Windigo.

uno de los co-conspiradores detrás de Operación Windigo y fue formalmente acusado en los Estados Unidos. Senakh fue luego arrestado por las autoridades finlandesas en la frontera con Rusia mientras volvía a su país luego de unas vacaciones, para ser extraditado a los Estados Unidos en febrero de 2016. Senakh terminó declarándose culpable de conspirar para cometer fraude electrónico y de violar la Computer Fraud and Abuse Act, por lo que fue sentenciado a 46 meses de prisión.

Más detalles de esta historia pueden encontrarse en este post: https://www.welivesecurity.com/la-es/2017/10/30/eset-ayudo-fbi-caso-windigo-prision/

¿Por qué debería importarnos?

Dedicarle tiempo y energía a hacer que la vida de los cibercriminales sea más dura, es algo que vale la pena. Creemos que es una de las mejores maneras de ayudar a prevenir la actividad cibercriminal y hacer que la Internet sea un lugar más seguro. Además pensamos que es hacer lo correcto.

Existen varias teorías detrás de la prevención del crimen clásico y definitivamente no pretendemos ser criminólogos. De todas maneras, hay una diferencia clara entre lo que nosotros hacemos para combatir el cibercrimen y la teoría de la "prevención del crimen situacional", que es definida como:

"*La prevención del crimen situacional se basa en la premisa de que el crimen es frecuentemente oportunista y apunta a modificar los factores contextuales para limitar las oportunidades de que los delincuentes lleven adelante una conducta criminal.*"

Las técnicas de prevención del crimen situacional pueden ser agrupadas en varias categorías amplias, tres de las cuales se conectan con lo que nosotros hacemos.

1. Aumentar el esfuerzo dedicado a campañas coordinadas de ruptura, tal como fue la dirigida contra Dorkbot, forzando a que los atacantes se reagrupen y deban desarrollar nuevas estrategias y técnicas, como por ejemplo crear nuevo malware o cambiar los protocolos de comunicación, lo que representa un aumento en el esfuerzo necesario para mantener su operación criminal.

2. Reducir las recompensas que provienen de cometer un crimen. Al desmantelar operaciones maliciosas necesariamente aumenta el costo de cometer el crimen, reduciendo proporcionalmente la ganancia.

3. Aumentar el riesgo asociado a cometer el crimen.

Brindar información técnica a los oficiales de las fuerzas de seguridad les permite avanzar en sus investigaciones en la dirección correcta y construir casos más fuertes. Más investigaciones de cibercriminales con mayor cooperación de investigadores de malware conducirán a más arrestos y condenas, y por consiguiente aumentará el riesgo para los cibercriminales de ser apresados.

Algunas personas piensan que la razón por la cual tan pocos cibercrímenes son castigados tiene que ver con que es sencillo realizar actividades criminales en Internet de manera anónima, sin demasiadas chances de ser rastreado. La realidad es lo opuesto: mantener una seguridad operacional (OPSEC) perfecta de manera consistente es bastante difícil. Tan solo piensen en todo lo que se debe haber para sacarle provecho a una operación maliciosa: lanzar campañas de infección, monitorear el estado de la botnet, actualizar los componentes maliciosos, registrar nombres de dominio o servicios de alojamiento, monetizar la operación en sí misma, y mucho más. Para poder ejecutar el cibercrimen perfecto, cada uno de los pasos debe ser realizado de manera perfecta, todo el tiempo. Los cibercriminales son humanos y los humanos cometen errores. Todo lo que hace falta es un mal día en el que el atacante se conecta al servidor erróneo antes de habilitar la conexión VPN o TOR y una flecha gigante apuntándole será guardada en un archivo log en algún lado, esperando a que alguien la encuentre.

Algunas personas también abandonan la persecución a los cibercriminales porque aunque hayan sido identificados, a veces se mantienen fuera de alcance. Quizás viven en una jurisdicción que no tiene leyes efectivas contra el cibercrimen, o que no cuentan con un acuerdo mutuo de extradición con los paí-

Para poder ejecutar el cibercrimen perfecto, cada uno de los pasos debe ser realizado de manera perfecta, todo el tiempo. Los cibercriminales son humanos y los humanos cometen errores.

ses que realizan la investigación. Pero nuevamente, los humanos cometen errores. Todo lo que se necesitaría es que un cibercriminal conocido deje su país para tomarse vacaciones en el extranjero.

2017 fue un año marcado por una gran cantidad de arrestos realizados en operaciones contra el cibercrimen, tal como ha marcado Stephen Cobb en su excelente resumen. En la medida en la que las entidades de fuerza de seguridad ganen experiencia en trabajar con entidades privadas como ESET con el objetivo de rastrear cibercriminales, podemos predecir con confianza que 2018 nos traerá más investigaciones exitosas que contribuirán en hacer de Internet un lugar más seguro para todos. Excepto para los cibercriminales.

5

La información personal en la nueva era de la tecnología y la legislación

- Cómo la IoT nos está llevando a un mundo 'público' en términos de información personal
- Armado de perfiles en redes sociales
- Comportamiento de usuarios utilizados en la industria AV (Microsoft, Kaspersky) en relación a los antivirus gratuitos.

AUTOR

Tony Anscombe
ESET Global Security Evangelist and Industry Partnerships Ambassador

La información personal en la nueva era de la tecnología y la legislación

La privacidad es, o debería ser, un derecho humano fundamental. Sin embargo, a los consumidores y a las empresas cada vez les resulta más difícil mantener una posición neutral sobre los datos. Aunque existen partidarios extremistas de la privacidad tecnológica que nunca dejan sus datos en ninguna parte, la gran mayoría de nosotros dejamos huellas por todos lados, como si fueran pisadas sobre la arena en un día de playa muy concurrido.

Los datos están impulsando la próxima revolución tecnológica y alimentando los vastos sistemas de inteligencia artificial en construcción. Una vez que los datos ingresan al proceso de toma de decisiones de las máquinas, ¿podremos eliminarlos realmente? ¿Serán en algún momento olvidados? Las compañías que recopilan datos ¿comprenderán alguna vez dónde y cómo los utilizan los sistemas de inteligencia artificial?

Si bien la mayoría de nosotros entendemos que al completar formularios o usar aplicaciones les estamos dando nuestros datos a las redes sociales o a las empresas, hay muchos otros servicios de recopilación de datos que pueden no ser tan obvios.

Software y servicios gratuitos

Como los consumidores esperan disfrutar del software en forma gratuita o a un precio muy bajo, algunos proveedores decidieron ingresar al mercado de recopilación y distribución de datos. Los productos de software gratuitos cuentan con muy pocos métodos para monetizarse, y uno de los menos intrusivos (o al menos desde la perspectiva de lo que el usuario realmente ve) es la recopilación y venta de datos a terceros.

El año pasado descubrimos que proveedores de seguridad confiables habían decidido ofrecer productos antivirus gratuitos. Aunque es posible que no hayan declarado abiertamente sus intenciones sobre cómo piensan monetizar sus nuevos productos gratuitos, seguramente los veremos usar métodos indirectos de monetización, como la recopilación de datos.

La estrategia de ofrecer productos gratis y monetizarlos a través de medios indirectos parece haberse acelerado luego de que Microsoft comenzara a ofrecer su antivirus Windows Defender como opción gratuita predeterminada. Dado que un porcentaje de usuarios empezaron a usar la opción predeterminada de Microsoft, hay menos oportunidades de venta para los proveedores existentes; de ahí la necesidad de buscar una monetización alternativa y de competir con un software gratuito propio.

La tendencia de ofrecer software gratuito o de bajo costo aumentará durante el próximo año. El riesgo para la privacidad radica en la falta de métodos tradicionales de monetización y la divulgación compleja, diseñada para ocultar la intención con la que se recopilan los datos y si se pueden vender. Muchas empresas ofrecen políticas de privacidad largas e ilegibles que solo pueden entender los abogados.

Con cualquier producto gratuito, es importante que el usuario sepa de qué forma la empresa gana dinero; por ejemplo, un juego para dispositivos móviles puede mostrar anuncios u ofrecer los niveles superiores pagos. Si la manera de monetizar el producto no es evidente, es muy probable que estén usando tus datos y tu privacidad con dicho objetivo.

La Internet de las cosas (IoT)

Si bien todos los productos y aplicaciones gratuitas conocen nuestros hábitos online, la adopción de los dispositivos conectados a la IoT por parte de los consumidores y las empresas implica que los datos sobre la forma en que vivimos ahora también están disponibles para su recopilación y explotación.

Cada vez que vuelves manejando a tu casa del trabajo, tu teléfono transmite las condiciones del tráfico para compartirlas con otros conductores, lo que te permite desviarte o tomar buenas decisiones para llegar más temprano. El sistema de climatización conectado de tu hogar se comunica con tu teléfono, ya que tu ubicación y la hora del día le indican que estás por llegar. Al acercarte a tu cuadra, la puerta del garaje se abre automáticamente utilizando tu proximidad para tomar una decisión. Las luces se encienden y la música se transfiere automáticamente de tu automóvil a tu casa. Los dispositivos de la IoT están diseñados para funcionar juntos y así simplificar nuestra existencia.

Cada dispositivo puede contar una historia a través de los datos que recopila. La combinación de esos datos brindará una imagen completa de nuestra vida: dónde trabajamos, dónde comemos, cuándo vamos al gimnasio, qué cine visitamos, dónde hacemos las compras, etc. Todos estos datos combinados y la inteligencia artificial podrían convertirnos en un títere de la tecnología, ya que ésta tomará las decisiones por nosotros.

La compañía analista Gartner pronostica que en 2018 habrá 11.200 millones de dispositivos conectados en el mundo, que llegarán a 20.400 millones en 2020. Cuidado: el auge de los dispositivos está llegando. Cada vez que un dispositivo solicita una conexión, debemos educar al cliente o a la empresa para que lea la política de privacidad y tome decisiones informadas antes de aceptar los términos de recopilación de datos, tal como allí se establece.

Legislación

En 2018, el Reglamento General de Protección de Datos (GDPR) de la Comisión Europea le dará a los ciudadanos el control sobre cómo se procesa y utiliza su información. La ley afecta a todas las empresas que procesen o recopilen los datos de un ciudadano de la Unión Europea, independientemente del país donde operen.

El incumplimiento podría dar lugar a elevadas multas, pero aún no hay una respuesta clara sobre cómo se impondrán a empresas fuera de la Unión Europea. La Comisión deberá sentar ejemplo con una empresa ubicada fuera de sus fronteras territoriales, lo que seguramente sucederá muy poco después de la fecha de implementación en mayo. Al no tener un ejemplo concreto de aplicación de la ley, muchas empresas internacionales pueden correr el riesgo de incumplimiento, por lo que probablemente veremos a la Comisión Europea intensificando sus medidas y sancionando a alguna compañía internacional en el transcurso de 2018.
La privacidad en los Estados Unidos mostró un retroceso en 2017 cuando la nueva administración revocó la legislación pendiente que les impediría a los proveedo-

Cada dispositivo cuenta una historia mediante toda la información que recolecta. Al combinar las diferentes fuentes de información, podría permitirle a cualquier atacante armar un panorama completo de tu vida.

res de servicios de Internet (ISP) recopilar datos de clientes sin su permiso. Mientras que algunos ISP han hecho una promesa voluntaria de no permitir el marketing de terceros, no significa que no lo utilicen para su propio beneficio comercial

es un concepto relativamente nuevo para muchos proveedores de software, ya que se ha convertido en una tarea menos costosa. El ecosistema de big data implica que ahora muchas más empresas cuentan con la capacidad de recopilar y vender datos.

El gran nivel de detalle de los datos recopilados sobre nuestros hábitos online podría permitir la creación de perfiles y mostrar lo que consideramos intereses extremadamente personales, que ni siquiera nos damos cuenta de que alguien está recopilando.

Los perfiles de los clientes se están convirtiendo en el objetivo de los cibercriminales. Ya hemos visto filtraciones de datos de individuos en sitios que almacenan sus perfiles, en tiendas en línea y otros, pero la máxima recompensa para un cibercriminal podría ser llegar a robar el conjunto de datos completo de todo lo que hacemos online. Esto le daría la oportunidad de extorsionar a los usuarios en función de sus hábitos online.

La capacidad de manipular grandes cantidades de datos como recién explicamos y luego usarlos con un objetivo significativo

Dada la facilidad con que pueden hacerlo, y nuestra disposición a aceptar la configuración predeterminada y no leer la política de privacidad, nuestra identidad, nuestra forma de vida y nuestros datos personales se están convirtiendo en un activo corporativo.

Espero que en 2018 mejore la toma de conciencia del usuario; pero para ser realistas, sospecho que veremos una mayor cantidad de datos recopilados con poca conciencia por parte del usuario. Con cada dispositivo que se conecta sin el respaldo de una decisión o elección informada, nuestra privacidad se erosiona aún más, hasta que en algún momento se convertirá en un lujo del que solo disfrutaban nuestros antepasados.

CONCLUSIÓN

Conclusión

El espectro de ciberataques seguirá expandiéndose, como queda de manifiesto tras analizar la evolución del ransomware o los ataques a la infraestructura crítica, por ejemplo. Pero no perdamos de vista que estos complejos escenarios son apenas una parte del panorama de cibercrimen, y no la más preponderante: los ataques avanzados llaman más la atención, pero solo representan un pequeño porcentaje de lo que vemos en el laboratorio de análisis de malware a diario.

Lo cierto es que la gran mayoría de las amenazas que logran su cometido a diario son las más simples, las que se distribuyen por campañas maliciosas de correo no deseado, phishing y descargas directas, por lo que podrían mitigarse mejorando la concientización de los usuarios. El problema es que todavía no se destinan los recursos para hacerlo.

Los acontecimientos de (in)seguridad informática de 2017 demostraron que, dado el avance de la tecnología y su rápida adopción por parte de usuarios y empresas, varios escenarios que hace algunos años parecían impensados hoy se encuentran en el terreno de lo posible. Más allá de las particularidades de cada caso, el denominador común de todas estas situaciones es el mismo: la información privada y sensible. No importa si es de una empresa, un gobierno o un usuario particular que cree no tener ningún dato atractivo. Hoy en día, la información se entrecruza entre varios actores. Se usa como divisa para acceder a aplicaciones y contenido gratuitos, la usan los organismos gubernamentales para llevar sus registros y ordenar sus operaciones, y la usan las empresas que operan en Internet para monetizar a costa de perfiles de usuarios.

En la mayoría de los casos es una actividad legítima y transparente, a menudo descrita en términos y condiciones que pocos se toman el trabajo de leer. Pero ¿qué pasa cuando hay tantas manos involucradas en el cuidado de esta información? Se multiplican las instancias en las que algo puede fallar, por lo que el riesgo se potencia.

La información personal de un usuario puede verse comprometida por un incidente particular, a saber, una infección de malware o una campaña de phishing, o bien a través de una brecha en los sistemas de una compañía en la que confió como cliente, o incluso a través de un ciberataque que afecte a una entidad gubernamental o crediticia, por ejemplo.

Entonces, si hay tantos frentes que proteger, ¿qué esperamos para instar a todos los actores involucrados a hacer su parte? No se trata de una misión que corresponda solo a las compañías de ciberseguridad, ni tampoco puede exigírseles que acaben con el problema. Sería como exigirle a la medicina que erradique la enfermedad, o a la policía que erradique el crimen.

Las estafas digitales y las amenazas informáticas seguirán existiendo mientras en nuestra sociedad sigan existiendo personas dispuestas a dañar a otras solo porque pueden hacerlo o porque ven un rédito ilícito en ello.

Es hora de que todos los niveles de usuarios y, en definitiva, ciudadanos, comprendan que su seguridad depende tanto de los proveedores que eligen como de sí mismos, y de que falta mucho por hacer. El primer paso es comprender el valor de la información en esta era y el motivo por el que cada actor la necesita para cumplir sus objetivos. No es posible proteger algo sin saber primero de qué y por qué lo estamos protegiendo.

El conocimiento de las amenazas y las medidas para evitarlas son a esta altura indispensables para proteger la disponibilidad, confidencialidad e integridad de la información de los diferentes actores de la sociedad, información que se ha convertido en la base de muchas actividades (legítimas y no legítimas).

Pareciera que el panorama es alentador: desde que WannaCryptor tomó por sorpresa al mundo entero, la seguridad ha empezado a estar presente en más ámbitos y en más titulares. Los ataques a las cuentas de redes sociales de celebridades y clubes de fútbol, como el Real Madrid y el Barcelona, así como a los sistemas internos de compañías de alto perfil, como HBO, Disney y Equifax, también causaron impacto en el público general, parte del cual empieza ahora a comprender lo que está ocurriendo.

Esperamos que este informe ayude a poner de manifiesto los temas clave que hace falta atender para avanzar hacia un entorno más seguro.

ENJOY SAFER TECHNOLOGY™