TENDENCIAS 2019:

Privacidad e intrusión en la aldea global

ÍNDICE

INTRODUCCIÓN

Desde hace ya varios años, los especialistas de ESET de todo el mundo participan del documento de Tendencias en el que se repasan los principales hitos en materia de seguridad y se plantean cuáles pueden ser los escenarios futuros sobre ataques y las medidas para contrarrestarlos.

Pero más allá de esto, el trasfondo de la cuestión no varía demasiado: se trata de resguardar la privacidad, integridad y confidencialidad de los datos de usuarios y empresas frente a los embates de cibercriminales que intentan acceder a ellos, manipularlos y/o robarlos. Por eso, en esta edición podrán encontrar una sección dedicada a la privacidad de los datos y la preponderancia que tendrá a nivel negocio llevar adelante una correcta gestión de la misma, en particular por todo lo acontecido a partir del caso de Facebook y Cambridge Analytica, así como también con la brecha de Google y su decisión de cerrar su red social Google+.

Este tipo de incidentes comienza a golpear a los grandes de la industria y abre un interrogante sobre cuál puede ser el impacto para otros negocios de menor envergadura que no puedan o no sepan proteger apropiadamente la privacidad de sus usuarios.

En respuesta a esta cuestión, en la que existe un enorme caudal de información personal y privada de los usuarios que estos servicios manejan, suscita que organismos gubernamentales tomen nota de cómo se están procesando y protegiendo los datos, y comiencen a ejercer controles como es el caso de la Unión Europea y el GDPR que entró en vigencia el 25 de mayo de 2018. En la sección correspondiente a esta cuestión no solo se repasarán algunas cuestiones salientes en torno a esta regulación, sino que también se evaluarán cuáles son las implicancias futuras en torno al control gubernamental de la protección de la información de los usuarios en su carácter de ciudadanos.

Y a pesar de que el resto de las secciones se encargan de temas que parecen ser más coyunturales y "de actualidad", los problemas de fondo giran en torno a la protección de los datos y la privacidad. Sucede que, dado que la tecnología avanza constantemente, el impacto sobre las prácticas y usos por parte de los usuarios también va sufriendo cambios y mutaciones, lo que origina a su vez que los cibercriminales se interesen en nuevas formas de aprovecharse de ello. Así es como en el presente documento presentamos una sección sobre los asistentes hogareños y los recaudos que hay que tomar en torno a la tendencia de la Internet de las Cosas y sus implicancias en la seguridad de usuarios y empresas. Otra cuestión relacionada es una amenaza que ha llamado mucho la atención durante este año y que se aprovecha de una tecnología legítima como el blockchain: estamos hablando de los coinminers, una amenaza que busca aprovecharse de los recursos de procesamiento de las víctimas para minar criptomonedas y darle un rédito económico al atacante.

Claro está que todos estos avances tecnológicos y sus consiguientes intentos de aprovechamiento por parte del cibercrimen, también tienen como contraparte el aprovechamiento de la tecnología para proteger a los usuarios y organizaciones. Un ejemplo de este avance es el machine learning, que permite aprovechar al máximo la enorme cantidad de información que se genera a partir de la interacción entre usuarios y sistemas, pudiendo procesarla y haciendo que los sistemas se perfeccionen. Pero la historia nos ha demostrado que toda tecnología puede ser aprovechada con cualquier tipo de fin, por lo que en la sección de machine learning se plantea el siguiente interrogante: ¿esta tecnología podría ser aprovechada con intenciones maliciosas?

Parte de la tarea de proteger la información de usuarios y empresas pasa por conocer el panorama y los desafíos en seguridad de la información, es por esto que los invitamos a que lean todas las secciones de este informe para saber cuáles van a ser las tendencias en seguridad para el año 2019 y también para los años venideros.

1

COINMINERS: EL NUEVO CHICO DEL BARRIO

- ¿Recuerdan el ransomware?
- Enriquecerse minando criptomonedas
- Protegiendo tu sistema

AUTOR

David Harley
ESET Senior Security Researcher

Coinminers: el nuevo chico del barrio

Para muchas personas, su primer encuentro con las monedas virtuales o las criptomonedas puede que haya sido cuando alguien que conocen (o ellos mismos) se convirtió en víctima del ransomware; una amenaza que generalmente exige a la víctima que pague mediante una criptomoneda como Bitcoin, para recuperar sus archivos del cifrado.

Utilizar tal método de pago es ventajoso para el criminal porque las transacciones no son fáciles de asociar con una identidad del mundo real, especialmente si existe un proceso de conversión a otras criptomonedas antes de finalmente ser cambiadas por efectivo o ítems con determinado valor en el mundo real. En consecuencia, muchas víctimas del ransomware se han encontrado a sí mismas teniendo que seguir las instrucciones de un criminal que les explica los pasos que se deben seguir para suscribirse a una billetera de Bitcoin o de algún otro medio, para efectuar el pago por el rescate de su información personal.

Esto no quiere decir, por supuesto, que las víctimas del ransomware están bien familiarizadas con el esoterismo que envuelve a las criptomonedas o que entiendan a qué se refieren por minado de criptomonedas (algunas veces denominado criptominería o minería de monedas), incluso si han utilizado criptomonedas para pagar un rescate. Una exhaustiva descripción sobre cómo trabaja el blockchain, las criptomonedas y la minería de criptomonedas está fuera del alance de este artículo. En resumen, si bien cuando nos referimos a la "minería" de monedas virtuales no es en el mismo sentido en el que los siete enanitos minaban en busca de joyas, sí involucra invertir trabajo en términos de procesamiento y poder eléctrico con el fin de "buscar" algo. Dicho de una manera simplista, la minería de criptomonedas consiste en dedicar poder de procesamiento a un proceso matemático que crea y distribuye monedas virtuales.

La minería de criptomonedas (o de hecho, las criptomonedas) no es en sí misma una práctica ilegal, por más que hay muchos proveedores de aplicaciones y especialistas que podrían ser acusados de manipular el potencial de ganancia del vagón minero. Parte del entusiasmo de los proveedores de apps y de los especialistas, quienes intentan convencer a quienes los escuchan de que se involucren con esta práctica, ha sido comparado con el que genera el Esquema Ponzi o la Burbuja de los mares del Sur.

Si bien Bitcoin es la criptomoneda de la que todos han escuchado hablar, hay muchas otras más. Monero, por ejemplo, es popular entre los cibercriminales porque está centrada en la privacidad, lo cual tiene obvias ventajas para los criminales –incluso más que para el resto de los usuarios.

De hecho, la minería de Bitcoins es un proceso costoso y apenas rentable para cualquiera, menos para quienes lo realizan a gran escala, ya que demanda demasiado poder de procesamiento como para ser realizado por computadoras individuales y dispositivos; aunque existen algunas monedas alternativas que son menos demandantes. Sin embargo, el procesamiento de carga puede ser compartido entre múltiples máquinas y dispositivos, lo cual explica por qué existen aplicaciones legítimas que (generalmente por una comisión) hacen de interfaz con un pool de minería. Pero eso no quiere decir que los propietarios de las máquinas participantes siempre están al tanto de estar ocupando ese rol, y tampoco quiere decir que las ganancias son compartidas. Si bien cada vez se ven más casos donde servicios legítimos se prestan para el intercambio y están dispuestos a prestar poder de procesamiento de un dispositivo individual para propósitos de minería, **c**uando se toma posesión de un dispositivo de manera ilegítima (criptojacking) no se produce tal intercambio. Esto último es más notorio cuando parte del poder de procesamiento del sistema de la víctima es "secuestrado" por un malware en el disco o sin archivos (comúnmente referido como un coinminer) o mediante secuencias de comandos en un sitio web (criptojacking en el navegador).

Las formas de minar criptomonedas y sus demandas

Sistemas individuales dedicados a la minería de criptomonedas tienden a no depender solamente de los ciclos de Unidades de Procesamiento Central (CPU), sino que también se apoyan en el procesamiento de dispositivos auxiliares, como son las Unidades de Procesamiento Gráfico (GPU) y los Circuitos Integrados para Aplicaciones Específicas (ASIC, por sus siglas en inglés). ¿Veremos más malware de minería pensado para aprovecharse de tal hardware? Es probable que individuos u organizaciones que incursionen de manera consciente en el negocio de la minería, con equipamiento dedicado comparativamente más costoso, estén atentos a los ciclos robados (¡incluso podrían estar usando software de seguridad!); pero los usuarios de computadoras equipadas para videojuegos, por ejemplo, probablemente estén menos atentos.

No obstante, es probable que se perciba una disminución si sucede que los sistemas utilizados por aplicaciones demandantes de recursos son reclutados de manera encubierta para minar criptomonedas; sobre todo si son sistemas poco potentes, como consolas de videojuegos antiguas o dispositivos móviles. ¿Esto quiere decir que los criptomineros evitarán tales sistemas? No necesariamente. Los cibercriminales no suelen preocuparse por los recursos de otros, a menos que estén haciendo lo posible por mantenerse bajo el radar. Además, tal como sugiere la frecuente utilización de mineros en el navegador, un dispositivo será de utilidad por más que no tenga alta potencia o que no se sepa si estará disponible durante mucho tiempo.

El evidente y alto uso de ciclos de CPU y GPU perfectamente podrían sugerir la presencia de malware para minería de criptomonedas. Otro posible síntoma incluye el sobrecalentamiento (consecuencia de la permanente actividad del ventilador o el notable calentamiento del dispositivo en el caso de teléfonos y tabletas), congelamientos inesperados, reinicios y volúmenes inexplicablemente altos de tráfico de red. Por supuesto, esto también puede ser síntoma de otro tipo de problemas que puede que estén o no relacionados a un malware u otro problema de seguridad.

Desde el comienzo del 2018 hemos estado viendo que el malware de minería de criptomonedas es descrito como "el nuevo ransomware'.

¿Qué sucedió con el ransomware?

A lo largo de los últimos años, puede que el ransomware haya sido descrito como un suceso extraordinario del cibercrimen. Opiniones y estimaciones sobre la "participación del mercado" y el impacto financiero de tipos específicos de amenazas en un momento dado varían de manera muy amplia como para ser de un valor discutible. Sin embargo, hay pocas dudas que hasta hace poco tiempo, los medios y el público parecían estar más preocupados por el ransomware que por cualquier otra amenaza cibernética actual.

Sin embargo, desde el comienzo del 2018 hemos estado viendo que el malware de minería de criptomonedas es descrito como "el nuevo ransomware", y que los ataques de ransomware

han atraído mucho menos la atención de los medios. Por supuesto que esto no quiere decir que la epidemia de ransomware ha seguido su curso, pero sí vemos una menor cantidad de historias sobre individuos que han perdido sus datos o que han tenido que pagar por un rescate. Es difícil saber si esto se debe a un cambio en el interés por parte de la prensa, que ahora busca temas sobre malware más novedosos, o si se trata de una caída significativa de los ataques de ransomware en individuos.

El hecho de que sí se sigan escuchando historias de grandes organizaciones atacadas por ransomware posiblemente indique un menor interés en epidemias en "mosaico", donde campañas de spam maliciosas generan muchas víctimas, cada una generando una pequeña retribución económica y con la esperanza de que todas esas piezas del mosaico generen una retribución sustancial. En su lugar, parece existir la tendencia de dirigirse hacia un pequeño número de víctimas que sean altamente rentables. Por ejemplo, se estima que quienes están detrás de SamSam han estado obteniendo ganancias cercanas a los USD 330,000 al mes dirigiéndose a empresas y organizaciones del sector público. Además, ha habido una mayor diversificación en los círculos del ransomware, como por ejemplo, en las campañas de sextorsión.

Males que convergen

No existe ninguna ley de la naturaleza que diga que el malware no puede entrar en más de una categoría. XBash es un reciente ejemplo de funcionalidad convergente que, según informes, combina un sorprendente número de atributos.

- Puede ser descrito como un ransomware, aunque quizás pseudo-ransomware sería una mejor descripción, dado que parece no haber manera de que los actores detrás de Xbash puedan restaurar los datos de las víctimas que eligieron pagar. Esto hace que su funcionalidad sea más parecida con la clase de malware destructivo que denominamos wiper; a pesar de demandar el pago de un rescate.
- También es descrito como una amenaza que combina esta funcionalidad con la de botnet, minería de criptomonedas y funcionalidades de autopropagación.
- Es multiplataforma, capaz de variar su payload según si es ejecutado en Linux o Windows, y de acuerdo a qué servicios estén disponibles. Pero también existe, por ejemplo, varios add-ons de terceras partes para Kodi que son utilizados para distribuir mineros para Linux y Windows. Y sí, hay ejemplos de malware para minería de criptomonedas dirigidos a macOS o Android.

Treinta años en el negocio de la seguridad me han hecho pensar que la sofisticación y una funcionalidad versátil no necesariamente son indicadores de una tendencia significativa, pero sí podrían denotar una transición entre clases de amenazas, en el sentido de que, por ejemplo, Melissa fue la máxima referencia de los macro virus y a la vez fue una alerta temprana que anunciaba la llegada de una gran marea de correos masivos. Aun así, es probable que, al menos en el corto plazo, los cibercriminales continúen limitándose a apostar por el malware experimental que obtiene rédito dónde sea y de la manera que sea posible. También podemos esperar ver más software para minar monedas intentando remover mineros "competencia" en sistemas comprometidos, con el objetivo de obtener una porción más grande del procesamiento.

¿Cuánto se puede obtener minando monedas?

Investigadores del Instituto de Seguridad Aplicada de la Universidad Técnica del Brunswick sugieren que el criptojacking con base en la web es común, pero es moderadamente redituable. Sin embargo, las tendencias en cuanto al criptojacking no dan señales de que esté reduciendo. Según un artículo de Tomáš Foltýn publicado re-

"La criptominería incrementó en un 956% en un año y el número de organizaciones afectadas se duplicaron en la primera mitad de 2018, lo que permitió a los cibercriminales ganar aproximadamente 2,500 millones de dólares durante esos meses."

cientemente, una de cada tres organizaciones en Reino Unido fue impactada por el criptojacking en abril de 2018, mientras que dos de cada tres ejecutivos creen que sus sistemas han experimentado el criptojacking en algún punto.

Un reporte que cita Phil Muncaster en un artículo manifiesta que la criptominería incrementó en un 956% en un año y que el número de organizaciones afectadas se duplicaron en la primera mitad de 2018, lo que permitió a los cibercriminales ganar aproximadamente 2.500 millones de dólares durante esos meses. En esta misma línea, otro reporte afirma que en lo que va de 2018, la criptominería ilegal incrementó cerca de un 459%, atribuyendo ese crecimiento al uso de EternalBlue. Pienso que esta tendencia creciente continuará durante un tiempo, aunque no estoy seguro de cuánto de ese crecimiento podemos considerar que es culpa de la NSA.

El uso del minero Coinhive como complemento en sitios web ha sido popular porque permite al sitio "pedir prestado" ciclos del sistema de la víctima con el fin de minar Monero. Sin embargo, rápidamente se volvió popular entre los cibercriminales, quienes lo utilizaron para vulnerar sitios legítimos con el fin de ejecutar scripts de Coinhive, configurados para minar Monero, en beneficio propio. Más recientemente, Crypto-Loot fue adoptado para un propósito similar por el conocido Pirate Bay.

Conclusión: mantén tu sistema protegido

No todas las sugerencias que a continuación detallamos son específicas para el malware de minería de criptomonedas (o el ransomware), pero con suerte contribuirán a reducir el impacto de otras amenazas también.

- Las soluciones de seguridad ayudan a evitar ser infectado con malware para minar criptomonedas y por otro tipo de amenazas. No solo como medio para evitar todo tipo de malware, si no también como medio para detectar malware para minar criptomonedas bajo la forma de archivos ejecutables que puedan comprometer los sistemas, y también para detectar o bloquear scripts de minería en el navegador.
- Este tipo de malware es frecuentemente detectado como "Possibly Unwanted" o "Possibly UnSafe", por lo tanto, asegúrate de que la solución de seguridad que tengas instalada esté configurada para alertar este tipo de aplicaciones.
- A pesar de lo que puedan decir algunos proveedores de tecnología de la competencia, las soluciones de seguridad más conocidas son capaces de detectar varios procesos maliciosos en la memoria principal o desde scripts que corren en el servidor.
- Otra forma recomendada de reducir los riesgos relacionados con el navegador es instalar un ad-blocker, que además presenta otras ventajas. O utilizar un bloqueador de scripts que tenga buena reputación.
- Ten en mente que los coinminers frecuentemente encuentran la manera de entrar a través de vulnerabilidades como EternalBlue, la cual fue parcheada en marzo de 2017. Instala parches con las actualizaciones lo antes posible, cualquiera sea el sistema operativo que estés usando.
- Siempre existe el riesgo de que cibercriminales causen daño, por lo tanto, mantén a salvo tus respaldos.
- Ningún producto puede detectarlo todo. Algunas veces el sentido común y la precaución te salvarán en momentos en los que la tecnología falle.

2

LAS MÁQUINAS APRENDEN, LOS HUMANOS NO TANTO

- Sistema de machine learning
- Tecnología utilizada para propagar malware
- Limitaciones prácticas del machine learning

AUTORA

Lysa Myers
ESET Senior Security Researcher

Las máquinas aprenden, los humanos no tanto

Existe un dicho que propone que las tres virtudes de un gran programador son la pereza, la impaciencia y la arrogancia. Es de especial importancia tener presente esta idea a la hora de discutir sobre el futuro escenario del malware. Otra recomendación práctica al hacer predicciones en ciberseguridad, es recordar que (sin importar de qué lado de la ley este cada uno) la gente está intentando conseguir un buen retorno a su inversión, tanto de tiempo como de esfuerzo. ¿Qué pueden enseñarnos estas reglas acerca del futuro de la ciberseguridad cuando se trata de la adopción de machine learning?

En cuanto a las predicciones sobre cómo podrían comportarse los cibercriminales, podemos asegurar que, salvo casos excepcionales, lo que buscan es robar dinero o bienes valiosos con el menor esfuerzo posible. Para la mayoría de los atacantes, implementar la última tecnología no merece su tiempo o esfuerzo, cuando los ataques más básicos y automatizados les dan lo que buscan. Este es el escenario más frecuente, y se convierte en un problema significativo para la mayoría de las personas a la hora de asegurar sus hogares o negocios.

Probablemente, los atacantes financiados por el Estado comiencen a utilizar herramientas más complejas para lograr sus objetivos. Con un presupuesto mucho más generoso, esa posibilidad no debe ser ignorada o descartada. Las grandes organizaciones, especialmente aquellas que están protegiendo las investigaciones de las industrias o la información personal de millones de clientes, necesitan estar particularmente al tanto de los atacantes bien financiados. Y en cierto punto, estas herramientas más complejas serán integradas, inevitablemente, a las acciones cotidianas de los operadores de malware.

Para quienes están a cargo de la seguridad, obtener el mayor retorno de su inversión significa tratar de proteger cuanto más puedan y de la manera más efectiva bajo un presupuesto asignado, en términos de dinero y de personal. Para los proveedores de seguridad, aun existiendo preocupaciones en cuanto al presupuesto, el factor más importante pasa a ser la necesidad de optimizar las soluciones que ofrecemos a nuestros clientes para que los productos detecten cuanto más puedan al menor costo para los clientes, en términos de poder de procesamiento y de cualquier mantenimiento que deba hacerse por operadores humanos.

En este capítulo discutiremos cómo se utiliza el machine learning – y seguirá siendo adoptado – por quienes están a ambos lados de la ecuación: quienes atacan los sistemas y quienes los defienden. También discutiremos algunas limitaciones prácticas del machine learning, y dónde seguirán siendo cruciales los humanos en el proceso de crear nuevas técnicas para atacar y para defender sistemas.

Aplicando el aprendizaje automático para la defensa

La base de cualquier buen sistema de machine learning es contar con una amplia cantidad de datos útiles. Sin información de la cual aprender, las máquinas no tienen los materiales necesarios para generar reglas efectivas y poder tomar decisiones.

Los lectores regulares de WeLiveSecurity estarán familiarizados con el hecho de que los productos de seguridad llevan usando la automatización y el aprendizaje automático desde hace ya tiempo. Esta ha sido parte importante de nuestra caja de herramientas por más de 20 años, y sin dudas, su prominencia se hará mayor a medida que avance el tiempo.

Los sistemas utilizados para identificar archivos y comportamientos sospechosos tienen hoy un contexto y vocabulario más profundo para describir comportamientos no deseados.

Los investigadores dentro de la industria del malware han estado reuniendo e intercambiando información acerca de amenazas durante varias décadas, para que podamos maximizar nuestra habilidad de proteger clientes contra comportamientos maliciosos. Además, por un período de tiempo apenas menor, hemos estado dialogando con una amplia variedad de proveedores de software para reunir datos acerca del estado actual de los archivos limpios. Esto nos provee de una enorme cantidad de información almacenada, tanto histórica como reciente, con la cual entrenar los sistemas de machine learning acerca de qué archivos y comportamientos se consideran sospechosos, y qué comportamientos son los más adecuados para indicar intentos benignos. Esto nos ayuda a identificar los archivos y comportamientos problemáticos manteniendo un mínimo nivel de falsos positivos.

Cuando la industria anti-malware comenzó, gran parte del trabajo de análisis de amenazas se realizaba manualmente y la cantidad de información almacenada era más bien básica. Los primeros sistemas de machine learning utilizaban rasgos de archivos maliciosos conocidos y limpios para inferir si futuras muestras serían sospechosas.

Dado el crecimiento del flujo de nuevos tipos de malware, una mayor parte del trabajo inicial de análisis es realizado por la automatización, para que los investigadores ocupen menos parte de su tiempo realizando tareas repetitivas y de esta manera puedan aplicar su experiencia en ver y comprender patrones, tanto en muestras individuales como entre sus respectivas variantes y campañas de malware enteras. Este trabajo automatizado ha aumentado considerablemente el volumen y los tipos de información que son almacenados acerca del comportamiento de muestras individuales, y mejoró nuestra comprensión sobre patrones más amplios dentro del panorama de las amenazas. En consecuencia, los sistemas utilizados para identificar archivos y comportamientos sospechosos tienen hoy un contexto y vocabulario más profundo para describir comportamientos no deseados.

La funcionalidad de los productos de seguridad sigue expandiéndose, y los números y tipos de especialistas en seguridad que participan en intercambios de información asciende. Todos estos datos extra continúan mejorando tanto la profundidad como la amplitud de la información que están reuniendo quienes se ocupan de la protección, frente a un panorama de amenazas en constante evolución.

El machine learning tiene una larga historia en la protección contra el malware y otras amenazas de seguridad. El futuro promete un aumento sostenido en las maneras de identificar comportamiento problemático o anómalo, no solo a nivel de archivos, sistemas o de red, sino también a lo largo de Internet como un todo.

Machine learning como herramienta de ataque

Como discutimos previamente, la mayoría de los ataques de malware se implementan de la manera más sencilla posible, no hay motivo para hallar nuevas tecnologías o técnicas si las viejas están logrando un flujo de ingresos ilegítimos estable. Probablemente, este continúe siendo el caso, dado que el bajo costo de entrada al crimen digital sigue invitando a nuevos participantes con una "ética cuestionable". Si no se genera un cambio radical en la manera en que las personas entienden e implementan la seguridad, no podremos ignorar el impacto que tienen los ataques sobre las viejas vulnerabilidades y brechas básicas dentro de la higiene cibernética.

Pero a medida que se amplía el mercado del cibercrimen y más Estados se suman a la lucha, es probable que los criminales se vean impulsados a utilizar la automatización en mayor medida para hacer sus creaciones más eficientes. Los ciberdelincuentes ya utilizan búsquedas automáticas para asistir en el hallazgo de máquinas vulnerables y cuentas en línea, y así reunir grandes cantidades de datos dispersos para el subsecuente reconocimiento dirigido a objetivos. Esta automatización aumentará, sin duda alguna, para hacer de sus esfuerzos algo más redituable y práctico en lo que respecta a los ataques de ingeniería social.

Y a medida que las bases de datos de las organizaciones criminales se vuelven más exhaustivas, pueden ser utilizadas eventualmente para informar al sistema de machine learning y que se creen reglas de ataque que hagan las campañas más efectivas. Existen tres áreas que parecen estar más sujetas a la asistencia del machine learning: la adquisición del objetivo, la explotación de la víctima y la protección de los recursos para evitar su destrucción.

Actualmente, el reconocimiento automático parece estar enfocado en hallar objetivos vulnerables. Al añadir mejor información a la base de datos de objetivos vulnerables, los criminales pueden crear una imagen más detallada que les permitirá obtener un mayor entendimiento del valor de cada target. En lugar de pedir por el equivalente en criptomonedas de algunos cientos o miles de dólares por un rescate a objetivos cuyas bases de datos valen millones – donde los criminales están dejando una cantidad significativa de dinero sobre la mesa –, mejor les resultaría evaluar el máximo lo que un target estaría dispuesto a pagar. Y con mayor reconocimiento, pueden ser más precisos a la hora de exfiltrar todos los activos valiosos dentro de la organización de una víctima, en lugar de solo tomar lo primero que parece interesante.

La ingeniería social siempre ha sido un área bastante problemática para los criminales que buscan explotar a un objetivo específico, dada la naturaleza internacional de sus esfuerzos. Todos podemos pensar en los intentos de phishing o scam que hemos recibido y que contenían grandes errores gramaticales o diferían en gran medida del estilo de mensajes que uno puede esperar de cierta fuente, si no ha sido falsificada. Si bien algunos ataques de phishing y otros tipos de fraude han logrado perfeccionar su habilidad para imitar a las fuentes legítimas, muchos siguen siendo muy evidentemente falsos. Sin embargo, el machine learning puede ayudar a aumentar la efectividad en este campo.

En el ejemplo de publicidad dirigida los criminales tienen un modelo para mejorar la eficiencia de sus comunicaciones. Si bien es poco probable que cuenten con el volumen y la calidad de información que tienen almacenada los proveedores para rastrear las compras hechas regularmente por la gente, los delincuentes podrían emplear rastreadores web para seguir a las víctimas mientras visitan sitios o conseguir información de vendedores de datos, también conocidos como "Data Brokers", para armar perfiles. Esto podría llevar a los intentos de fraude y phishing a ser mucho más personales y convincentes.

Los delincuentes podrían emplear rastreadores web para seguir a las víctimas mientras visitan sitios o conseguir información de vendedores de datos.

El abordaje más complejo, técnicamente hablando – y por ende, el que menos probabilidades tiene de volverse común en el corto plazo –, sería el del machine learning ayudando a los cibercriminales a proteger su infraestructura para evadir la detección con mayor efectividad. Esto requeriría, en un principio, hacer de su estructura de comando y control una más resistente, y crear nuevas variantes de malware.

Cómo podría afectar el machine learning la "carrera armamentista"

Desde el descubrimiento de los primeros archivos creados con objetivos maliciosos, existe una carrera armamentista entre los creadores y los detectores de malware. El machine learning no pondrá fin a ella. Existen – y siempre existirán – límites a la utilidad de las computadoras para reemplazar a los humanos como los encargados de tomar decisiones. Debería existir siempre una relación de mutua colaboración constante, en lugar de una delegación de nuestra responsabilidad en las máquinas.

La creatividad de los desarrolladores humanos (tanto con fines benéficos como malignos) siempre necesitará de la presencia de expertos que puedan ver cuando algo caiga fuera de los patrones existentes. Omitir a las personas de los procesos de análisis para la defensa permitirá a los individuos maliciosos ganar ventaja.

Muchos cibercriminales con motivaciones económicas cuentan actualmente con un proceso de obtención de datos que favorece al rápido procesamiento de la información, ya que ciertos datos, como detalles de las tarjetas de crédito y credenciales de acceso, tienden a volverse viejos rápidamente. Pero han estado moviendo su foco hacia otra clase de datos más estable, como la de seguros o información médica, que conserva su valor por más tiempo. Es probable que las bases de datos que tengan una presencia más permanente con el tiempo se vuelvan más detalladas y, en consecuencia, más útiles para los fines ilícitos de estos actores. A medida que sus propios recursos se vuelven más estables y valiosos, podrían necesitar métodos de protección más avanzados.

Irónicamente, esto haría que la carrera armamentista deje de ser una batalla entre un lado centrado en atacar y otro enfocado en defender, y se acerque más a una cuestión de ataque-contraataque.

Al final, pareciera que estamos cerca de ver un aumento gradual de las tendencias que ya existen; machine learning mejorado y ampliado para defender máquinas, y un aumento de los atacantes financiados llevando sus herramientas y sus técnicas hacia el uso cotidiano del malware. Si bien el poder y la importancia de los sistemas de machine learning no debería ser ignorada por quienes están del lado de la defensa (probablemente no lo sea por los atacantes), la realidad es que no es una solución mágica para ninguno de los dos bandos.

El cibercrimen es sumamente lucrativo para la mayoría de sus integrantes sin la necesidad de desarrollar nuevas herramientas, aunque deberíamos prepararnos como si estuvieran por lanzar sus armas más sofisticadas. Y la seguridad para la defensa es tan compleja que no solo los humanos necesitarán de las computadoras para poder identificar archivos y comportamientos sospechosos, sino que las computadoras siempre necesitarán de los humanos para identificar nuevos tipos de armas.

3

GDPR: ¿EL PRIMER PASO HACIA UNA LEY DE PRIVACIDAD GLOBAL?

- El valor de la privacidad de los datos
- UE vs. EUA
- Aumento de las regulaciones a la privacidad

AUTOR

Stephen Cobb
ESET Senior Security Researcher

GDPR: ¿El primer paso hacia una ley de privacidad global?

Para cualquier compañía o consumidor preocupado por la privacidad de su información personal en la era digital, 2018 se destacará por ser el año en el que entró en efecto el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) dentro de la Unión Europea (UE). La legislación ya está teniendo un gran impacto en la privacidad digital, no solo dentro de la UE, sino también en Estados Unidos, así como en otros países; una tendencia que afectará el panorama de la ciberseguridad desde 2019 en adelante.

¿Es inevitable?

En su mayoría, los responsables de asegurar la privacidad corporativa han oído sobre el GDPR mucho antes de que se hiciera efectivo. En 2015 se dio a conocer el contenido de la regulación y en 2016 fue adoptado, aunque con un posterior período de gracia de dos años. El día al que todos estaban atentos – 25 de mayo de 2018 – marcaba el fin de ese período de gracia y la entrada en vigencia definitiva de la normativa en la Unión Europea.

Para ese entonces, la mayoría de los negocios norteamericanos habían al menos pensado en el GDPR. Si has asistido a algún seminario o conferencia en relación al tema dentro de Estados Unidos durante 2017, habrás notado que la pregunta más frecuente de las compañías era: ¿nos afecta a nosotros el GDPR? "Sí", solía ser la respuesta, por motivos resumidos en un artículo publicado en WeLiveSecurity en 2016.

Las compañías deben adecuarse al GDPR si:

- Monitorean el comportamiento de datos de sujetos que están localizados en la UE
- Están asentados fuera de la UE pero proveen servicios o bienes a la UE (incluyendo servicios gratuitos)
- Tienen un "establecimiento" en la UE, independientemente de dónde procesen datos personales (por ejemplo, procesamientos basados en la nube fuera de la UE para una compañía basada en la UE).

Entonces, la pregunta más común que siguió en la discusión estadounidense sobre el GDPR fue: ¿Cómo podemos evitarlo? Las respuestas dadas por consultores de firmas como Deloitte, PwC, y KPMG, pueden resumirse de la siguiente manera: no pierdan el tiempo con maniobras técnicas para evadir el GDPR y planeen cómo alinear las estrategias de su organización en lo que concierne a datos con esta regulación, ya que es inevitable algún tipo de equivalente al GDPR donde sea que hagan negocios.

La privacidad de los datos llega alto

La predicción de una regulación de privacidad al "estilo GDPR universal" fue recibida con escepticismo, hasta que salió a escena el California Consumer Privacy Act (CCPA) de 2018. De hecho, el CCPA se convirtió en ley menos de 40 días antes de que entre en efecto el GDPR, y afirma que, cuando se trata de negocios que manejan su información personal, los residentes de California tienen derecho a:

- Conocer qué información ha recolectado, obtenido o derivado un negocio acerca de ellos;

Planeen cómo alinear las estrategias de su organización en lo que concierne a datos con esta regulación, ya que es inevitable algún tipo de equivalente al GDPR donde sea que hagan negocios.

- Eliminar, transferir o tener acceso a información personal almacenada por la compañía;
- Saber si su información personal es vendida o revelada por la compañía, y en caso de serlo, a quién;
- Prohibir la venta de su información personal por la compañía;
- Recibir iguales servicios y precios de la compañía, incluso si se ejercen sus derechos de privacidad.

Si bien la manera en que estos derechos están presentados en el CCPA incluyen numerosas excepciones y limitaciones, no hay duda de que marcan un enorme cambio en lo que respecta a la privacidad en Estados Unidos. Y si bien California solo es uno de los Estados que conforman los Estados Unidos de Norteamérica, representaría la quinta mayor economía del mundo si fuera un país independiente (justo detrás de Alemania, Japón, China y el resto de Estados Unidos). Eso hace a California una enrome influencia, tanto en términos de leyes como prácticas de negocios.

La privacidad divide

Para comprender cómo la adopción de protecciones al estilo GDPR para datos personales en California podría impactar sobre el panorama de la privacidad en 2019, deberíamos echar un vistazo a la forma en que la UE y los Estados Unidos han manejado la privacidad hasta ahora. La Carta de Derechos Fundamentales de la UE contiene un derecho explícito para la protección de datos personales y prohíbe la recolección o el uso de información personal acerca de residentes de la UE sin su conocimiento o permiso.

En los Estados Unidos no existe un derecho constitucional explícito para la privacidad, por lo que las compañías pueden recolectar y utilizar información sensible acerca de ti, excepto que haya una ley o demanda que no lo permita. Aquí hay un ejemplo de lo que esto significa:

> **Imagina que comienzas un negocio que ofrece un servicio de viajes compartidos basado en una app, similar a Uber. Tu compañía reúne datos sobre personas que utilizan el servicio, incluyendo nombres y detalles de sus viajes. Si tu servicio se usa en la UE existen leyes que restringen lo que la app puede hacer con esos datos, incluso sin haber leyes específicas sobre la privacidad para esta clase de servicios de transporte.**

En Estados Unidos, la respuesta a la pregunta "¿qué puede hacer mi negocio de viajes con la información personal que reúne de viajeros?" suele ser "depende". Las variables incluyen dónde está incorporado el servicio y dónde opera, pero la respues-

ta suele reducirse a... "lo que sea que quieras y puedas hacer con ella". Y esa puede seguir siendo la situación hasta que se realice una demanda o se aprueba una ley de privacidad para regular el uso de datos personales recolectados por las firmas de viajes compartidos.En otras palabras, los Estados Unidos tienen protecciones distintas para diferentes tipos de datos personales, creados de diversas maneras, en tiempos variados. Por ejemplo, el Video Privacy Protection Act de 1988, fue un proyecto redactado y promulgado unos pocos días después de filtrarse a un periódico los registros de videos alquilados por un nominado a la Corte Suprema.

Las protecciones para la privacidad existentes en Estados Unidos vienen de leyes federales, legislaciones estatales o decisiones de la corte, ya sea a nivel estatal o federal. (Para más detalles sobre la ley de privacidad en Estados Unidos puedes ver el White Paper de ESET: Data privacy and data protection: US law and legislation.

En la UE, los datos que te pertenecen a ti, como individuo identificado; están protegidos por defecto, desde el primer momento. Ese es el significado práctico del término "protección de datos" en el uso europeo. Todo aquel que quiera reunir datos que te pertenecen tiene la obligación legal de obtener tu permiso para hacerlo, y cuando obtienen tus datos deben ejercer un control riguroso sobre quién puede acceder a ellos y con qué propósito. Esto aplica a nuevas formas de datos personales tan pronto como se hagan efectivos, por lo que no tienes que esperar que se haga una demanda o que ocurra un incidente político vergonzoso.

La creciente ola de regulaciones de privacidad

Entonces, ¿cómo, sin una ley fundacional de privacidad de datos en Estados Unidos, puede un único Estado hacer una diferencia en la protección de la privacidad? Todo tiene que ver con la afluencia, la influencia y la envidia. California es el estado más rico del país americano, y puede permitirse ser pionero en derechos que resultan difíciles de establecer en otros estados. Eso prepara el camino para otros estados cuyos residentes probablemente sientan envidia hacia los californianos si tienen mejores protecciones para su privacidad de la que proveen sus propios estados, de la misma manera en que los estadounidenses sienten cada vez más envidia de los europeos y sus derechos bajo el GDPR.

La historia también juega su rol: el primer paso hacia el CCPA de 2018 se llevó adelante en 1972. Fue ahí cuando los votantes de California reformaron la constitución para incluir la privacidad entre los derechos personales de todas las personas (cada estado de Estados Unidos puede tener su propia constitución, además de la constitución federal). Solo cinco años después, el estado hizo efectivo el Information Practices Act de 1977, para limitar la recolección, el manejo y la diseminación de información personal en manos de agencias estatales; un movimiento estimulado por el aumento del procesamiento de datos entre los departamentos gubernamentales.

25 años después, en 2002, cuando los modelos de negocios digitales comenzaron a expandir la recolección de datos personales y aumentaron el riesgo de la divulgación desautorizada, California implementó la primera ley estatal exigiendo el envío de notificaciones ante brechas de seguridad. 16 años más tarde llegamos a 2018, y los 50 estados de los Estados Unidos poseen su ley de notificación de brechas, sugiriendo que otras protecciones, como los derechos de privacidad de datos del estilo GDPR englobados en el CCPA, también serán difundidas a lo largo de Estados Unidos.

Hay argumentos contrarios ante esta predicción, y no menor es la continua discusión para modificar el CCPA antes que se haga efectiva en 2020. En oposición a esto, los defensores de la privacidad están manteniendo activa la presión sobre los legisladores (el movimiento a favor del CCPA tiene su propio sitio web, una estrategia que podría ser fácilmente adoptada en otros estados).

Desestimar los derechos a la privacidad y protección de datos como "solo una anomalía europea" se vuelve difícil cuando esa anomalía está por convertirse en ley en el estado norteamericano que alberga a los gigantes digitales, como Google, Facebook, Apple, HP y Oracle.

El desafío para las compañías que creen que el CCPA será negativo para los negocios es el siguiente: ¿cómo convences a los consumidores/votantes de que su privacidad necesita menos protección que quienes habitan otros países? Desestimar los derechos a la privacidad y protección de datos como "solo una anomalía europea" se vuelve difícil cuando esa anomalía está por convertirse en ley en el estado norteamericano que alberga a los gigantes digitales, como Google, Facebook, Apple, HP y Oracle. Estas compañías operan globalmente, y la tendencia global se dirige de manera clara hacia la privacidad de estilo GDPR.

El país más grande de América Latina – Brasil – adoptó una nueva Ley de Protección General de Datos (LPGD) en 2018, para reemplazar un modelo de privacidad sectorial que se acercaba a lo que Estados Unidos tiene hoy. De acuerdo a analistas legales globales, "la Ley brasileña replica muchos de los componentes del GDPR". Además, el LPGD puede ayudar a Brasil a alcanzar "un acuerdo de adecuación recíproca de la Comisión Europea, similar al que recibió Japón". Por lo tanto, sí; otra potencia económica – Japón – se dirige hacia los niveles de protección de la privacidad de la UE. También así lo hace China, y si bien el control interno de Internet de China es un factor complejo, el hecho de que uno de los mayores procesadores de datos esté desarrollando las herramientas y la tecnología para manejar los datos de manera que se adecúe con el GDPR es significativo.

Resumen

Un objetivo clave en la ciberseguridad es controlar el acceso a la información para evitar que sea expuesta sin autorización. Un objetivo de la regulación de la privacidad es influenciar la manera en que se define la "exposición desautorizada" en lo que respecta a información personal, y luego explicitar las consecuencias que pueden tener las organizaciones si permiten que ocurra dicha exposición.

En consecuencia, una brecha de datos podría hacer más que dañar la confianza que la gente deposita en las organizaciones – como se plantea en "Tendencias 2019: Privacidad recargada " –, ya que podría también resultar costoso si la brecha, y/o el manejo de la misma, viola las regulaciones de privacidad.

En octubre de 2018, el Supervisor Europeo de Protección de Datos anunció que el mundo puede esperar las primeras multas del GDPR "para ciertos casos hacia fines de este año". Cerca del momento del anuncio, la Comisión Irlandesa de Protección de Datos comenzó a investigar a Facebook por una brecha que "podría resultar en una multa de hasta 1.630 millones de dólares". A medida que se hizo más evidente el impacto del GDPR – y más real – en 2019, predecimos que muchas compañías estarán ocupadas preparándose para cumplir con el CCPA y cualquier otra legislación similar alrededor del mundo.

4

PRIVACIDAD RECARGADA: ¿SERÁ ELLA QUIEN DECIDA QUÉ NEGOCIOS SIGUEN EN PIE?

- Vulnerabilidades y fallos expusieron a millones
- El test de Facebook
- Nuevos modelos de privacidad

AUTORES

Lysa Myers & Stephen Cobb

ESET Senior Security Researcher

Privacidad recargada: ¿Será ella quien decida qué negocios siguen en pie?

El número de personas cuya privacidad digital estuvo en riesgo durante 2018 por algún problema en relación a la seguridad de los datos, probablemente haya superado los 2,000 mil millones antes de que finalice el tercer trimestre del año. Si ese número parece exagerado, recuerda que solo cinco organizaciones han expuesto cerca de 1,800 millones de registros antes de alcanzar la mitad del año: Aadhaar, Exactis, Under Armour, MyHeritage, y Facebook. De hecho, 2018 podría no alcanzar el record de exposiciones de 7,800 millones en 2017, o incluso el anterior de 6,300 millones de 2016.

Lo que más interesante podría resultar de 2018 es que varios de los problemas de seguridad del año no encajan dentro de la clásica percepción de "brecha". Mientras muchos de nosotros pensamos en una brecha como la irrupción en un sistema por un grupo de atacantes con el objetivo de robar información, no es del todo claro si los problemas de seguridad de 2018 fueron completamente producto de atacantes. Algunos de ellos fueron el resultado de vulnerabilidades o bugs que permitieron un acceso no intencionado, como los casos de Facebook que pusieron en riesgo las cuentas de 90 millones de usuarios, o el bug en Google+, que expuso las cuentas de más de medio millón de usuarios (y contribuyó al cierre de la plataforma).

En ocasiones, los problemas de privacidad surgen de productos o servicios que se comportan de acuerdo a como fueron diseñados, tal como se los describe en los acuerdos de licencia; pero terminan convirtiéndose en absolutas pesadillas para la privacidad. Dos ejemplos de esta clase de problemas son el escándalo de Cambridge Analytica con Facebook, y su recolector de datos Onavo VPN. Las consecuencia inintencionadas de compartir información extra han ocupado los titulares desde comienzos de 2018, con el revuelo de la app Strava.

¿Cuáles son entonces las implicancias para 2019? Mucho quedará en manos de dos grandes jugadores: Facebook y Google. Entre las dos, estas compañías han acumulado bases de usuarios gigantescas, junto con cantidades abrumadoras de datos personales acerca de ellos, que deben ser protegidos del acceso no autorizado. La gente se pregunta ahora si esas compañías, en un sentido social, se han vuelto "demasiado grandes para fallar".

Facebook y Google han desarrollado plataformas muy poderosas, que tienen el potencial de conectar grandes cantidades de personas con el propósito de compartir y difundir información, ya sea para bien o para mal. Como resultado, son muchos los que han llegado a depender de los productos de Facebook y Google. Pero cualquiera sea la acción llevada a cabo por estas plataformas que represente un riesgo o peligro para ciertos individuos al usarlas, seguramente tenderá a alejarlos.

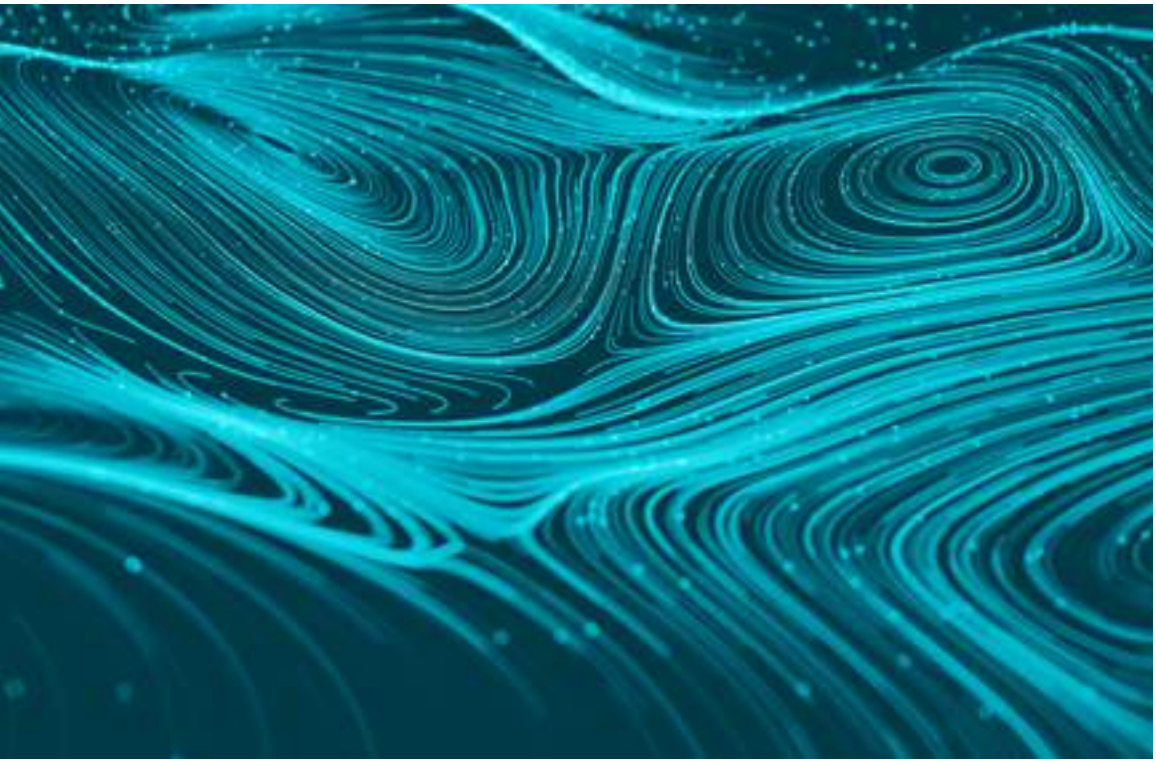
En otras palabras, desde una perspectiva social, esperar que la gente elija no ser parte de ninguna de las funcionalidades que ofrecen Google o Facebook, sería similar a elegir no participar de la vida moderna. Si bien, teóricamente, sería posible evitar el uso de ambas, hacerlo sería, hoy en día, un obstáculo para llevar a cabo las tareas diarias relacionadas con los negocios o la vida personal, lo que para muchos representaría una dificultad innecesaria.

¿Ir más allá o ir demasiado lejos?

Es claro que la gente no ha dejado de usar Facebook, a pesar de los dos grandes conflictos de seguridad que protagonizó en 2018; pero el sentimiento de muchos usuarios se ha visto afectado, en formas difíciles de representar con estadísticas. En lugar de ser un sitio al cual la gente quiere conectarse y donde busca compartir sus historias con familia y amigos, para algunos Facebook se ha convertido en un lugar difícil de abandonar si no se quiere perder el contacto con familia y amigos.

cebook, como Instagram, Messenger y WhatsApp. Si bien muchos pueden estar abandonando el sitio de Facebook con un sabor amargo, no están saliendo de su ecosistema por completo.

Considera el dispositivo Facebook Portal para realizar videollamadas, cuyo lanzamiento está programado para fines de 2018. Esto podría servir como prueba para conocer el sentimiento del público en torno a la compañía en 2019. Mientras esté la privacidad de por medio, los dispositivos de asistencia virtual pueden describirse como un beneficio con pros y contras, lo que es de esperar cuando se trata de dispositivos con micrófonos



Algunos estudios recientes han mostrado una caída en el uso de Facebook, así como en el engagement de las audiencias y de las ganancias, algo que se ha estado acelerando en los últimos años. Pero al profundizar en esta información, se ven algunas señales de alerta. Por ejemplo, si bien son menos los que usan el servicio a través de un buscador web de escritorio, son más los que lo hacen desde una app móvil. Menos personas gastan su dinero y su tiempo en Facebook, pero más lo están haciendo en aplicaciones que son propiedad de Facebook, como Instagram, Messenger y WhatsApp.

incorporados y encendidos constantemente dentro de nuestro hogar.

Los asistentes virtuales que contienen a los altavoces inteligentes más populares – Alexa, el Asistente de Google, Siri y Cortana – han estado disponibles durante varios años. Eso significa que han sido probados, y son probablemente confiables. El desafío que enfrentará el Facebook Portal en 2019 será que los propios problemas de seguridad que enfrentó Facebook pueden dificultar la generación de un nivel de confianza similar entre

Menos personas gastan su dinero y su tiempo en Facebook, pero más lo están haciendo en aplicaciones que son propiedad de Facebook, como Instagram, Messenger y WhatsApp.

el público. Y varios analistas han notado que lanzar un dispositivo de vigilancia a pocos días de haber sido expuestas millones de cuentas de usuarios sugiere que Facebook está, en cierto modo, haciendo oídos sordos a las preocupaciones de privacidad de sus usuarios.

Si Facebook realmente comienza a decaer, quizás podría deberse a que pareciera continuar destinando recursos para aprovecharse de la dependencia de la gente con su plataforma; aparentemente sin notar que solo están perdiendo la confianza de sus usuarios.

Hace tiempo que se sabe cuál es el impacto que pueden tener las brechas y otros problemas de seguridad en el ámbito financiero, incluso en compañías de gran tamaño. Alcanza con mirar lo que sucede con el valor de las acciones en empresas que cotizan en la bolsa cuando se hace pública una brecha de privacidad. El stock de Equifax, la agencia de informes de crédito – otro gran repositorio de información personal – cayó un 30% tras la brecha que generó el desastre de 2017, e incluso 12 meses después no ha podido recuperarse por completo. Facebook ocupa una posición algo distinta porque sus clientes no son sus usuarios, sino sus anunciantes. Dicho esto, la desconfianza del usuario puede tener un efecto dominó si los anunciantes de Facebook ven una pérdida de valor en la plataforma como medio para promocionar sus productos.

Diversidad defensiva y nuevos modelos de privacidad

Las compañías que están tan inmersas en nuestra vida diaria es porque tienen a parte de la audiencia captiva. ¿Será 2019 el año en que las grandes compañías demuestren, finalmente, que han tomado a la privacidad con la suficiente seriedad para que no haya brechas de privacidad significantes? No está claro, pero no hay dudas que 2018 fue el año en el que muchos se vieron forzados a considerar los peligros de tener a un gran negocio como el portal hacia toda su existencia en Internet.

Lo que podremos ver convertirse en tendencia hacia 2019 es un aumento en el número de gente buscando alternativas a las plataformas que dominan actualmente el panorama en línea, en un esfuerzo por diversificar su propio mundo digital. Esta diversificación conlleva dos beneficios iniciales: la "biodiversidad" digital y el mantenimiento de "zonas" digitales segregadas. Alcanzar un flujo de información sin fricciones entre cada persona y entidad conectada suena bien, también la idea de utilizar las credenciales de una plataforma para acceder a todas tus cuentas en línea. Sin embargo, las desventajas son difíciles de predecir y son también potencialmente enormes.

A modo de ejemplo biológico, considera una banana. La banana Cavendish es tan popular, que si dices "banana", la imagen que inmediatamente viene a la mente de la gran mayoría de la personas es la clásica especie clonada amarilla. Las bananas que obtengas en Finlandia serán genéticamente idénticas a las de Florida, pero ¿por cuánto tiempo?

Las bananas Cavendish han estado al borde del desastre de infección fungal que también acabó con sus predecesoras, las Gros Michel. Gran parte del motivo por el cual las bananas que compramos en supermercado son un cultivo tan precario se debe a que no existe una diversidad genética que permita ayudar al fruto a resistir ante infecciones u otros desastres. Una vez que se ha infectado un área con el hongo patógeno, éste permanece en el suelo por más de tres décadas, por lo que las bananas ya no pueden crecer allí. Lo único que nos ha permitido mantener a las bananas Cavendish como un cultivo viable es establecer procedimientos de bioseguridad para mantener distintas plantaciones separadas – no solo en términos geográficos, sino a nivel microbiano.

Para hacer una comparación, consideremos la crisis que afectó a sapos y ranas que fueron infectados por el hongo chytrid; el mismo que afectó a distintas poblaciones anfibias alrededor del mundo y que solía ser transportado por los humanos. Hubo una gran preocupación por el temor de que este patógeno pueda causar la desaparición total de una especie a nivel mundial, si no se frenaba la

Lo que podremos ver convertirse en tendencia hacia 2019 es un aumento en el número de gente buscando alternativas a las plataformas que dominan actualmente el panorama en línea, en un esfuerzo por diversificar su propio mundo digital.

expansión de la amenaza. Sin embargo, dado que estas ranas no son clones, sino diferentes genéticamente, poseen una variedad de genes que les permiten adaptarse a las amenazas. Y fue por esta razón que las poblaciones de sapos y ranas han comenzado a desarrollar resistencia a esta amenaza, y han comenzado a sobrevivir; a pesar de ser infectadas.

Una población o ecosistema homogéneo – ya sea en el mundo de las moléculas y microbios o en el reino de los dígitos y los datos – crea el potencial para un riesgo extensivo cuando surge una amenaza. Si diversificamos nuestro ecosistema digital, tanto individualmente como a nivel de población, reduciremos el riesgo y haremos que sea más sencilla la recuperación ante los problemas que surjan. Por ejemplo, tener una única instancia de identificación que conecte muchas de nuestras cuentas en línea significaría que cuando una amenaza aparece dentro del sistema se convertirá en un riesgo para todas esas cuentas. Aun siendo potencialmente menos conveniente tener que poner todos nuestros huevos en canastas diferentes, metafóricamente, también nos enfrentamos a perder menos si una de esas canastas es derribada.

Resumen

En 2019 podríamos ver una mayor diversidad de plataformas a medida que la gente se aleja de los sitios que han demostrado ser inseguros, y un continuo descenso en la confianza y el compromiso con plataformas existentes. Podríamos incluso ver como ciertas compañías y/o productos van desapareciendo debido a las preocupaciones en torno a la privacidad. Además, a medida que se desarrolla el año, ten en mente que los miedos de los consumidores no son los únicos que impulsan la privacidad en el trabajo. Considera los escenarios de riesgo regulatorio descriptos en la sección "Tendencias 2019: GDPR". El GDPR puede no ser la única fuente de sanciones que afecte a las compañías en 2019 si no toman en serio a la privacidad. Otras localidades – como Brasil y California, recientemente – ya han aprobado legislaciones similares, y no parecieran ser las últimas.

5

ASISTENTES DE VOZ PARA EL HOGAR: CUANDO TUS DISPOSITIVOS NUNCA SE APAGAN

- Ataques que continuarán
- Usabilidad y seguridad alineados
- Avance de la seguridad de los datos

AUTHOR

Camilo Gutiérrez Amaya

ESET Senior Security Researcher

Asistentes de voz para el hogar: cuando tus dispositivos nunca se apagan

Si pensaras en los dispositivos electrónicos que usas a diario, ¿cuáles dirías que son los más importantes? ¿Pensaste en el router? Ese dispositivo, que no suele ser más que una caja negra en un rincón de la casa, se ha convertido en crucial; incluso más que la computadora o el dispositivo móvil.

Esto es así porque además de darle acceso a Internet a los usuarios, por este dispositivo pasa toda la información sensible de los usuarios, y en caso de no estar correctamente actualizado puede ser aprovechado por un cibercriminal para comprometer todos los dispositivos conectados. Por lo tanto, un router vulnerado puede convertirse en una plataforma de ataque que sirva como puente para acceder a otros dispositivos en la misma red.

Pero en la actualidad no es el único dispositivo que agrupa información de otros aparatos. De hecho, en el último tiempo empezaron a popularizarse los asistentes personales o asistentes de voz; que además de estar comunicados con varios dispositivos tienen la capacidad de controlarlos, como es el caso de luces inteligentes, sensores, cámaras e incluso electrodomésticos. Y de la mano de este incremento en la variedad de dispositivos interconectados también crece la superficie de ataque.

Con la creciente cantidad de dispositivos inteligentes conectados, que según un informe de IDC se estima que para 2020 serán 80,000 millones, veremos durante el próximo año un incremento en la cantidad de ataques, en los que se utilizarán desde scripts automatizados de vulnerabilidades en dispositivos IoT hasta ataques dirigidos utilizando exploits diseñados para tomar el control de los mismos. Asimismo, al ser los routers y los asistentes personales los que más interactúan con otros dispositivos inteligentes serán los puntos preferidos por los atacantes.

Crecimiento de ataques

Desafortunadamente, determinar cuánto van a incrementarse los ataques durante el próximo año no es posible, pero sin lugar a dudas veremos con más frecuencia casos de amenazas desarrolladas específicamente para estos dispositivos. También podemos esperar más diversidad de amenazas dirigidas a dispositivos que funcionan como concentradores, como son routers o asistentes, ya que son estos los que pueden darle a un atacante el acceso a toda una red junto con los dispositivos conectados, y lo más importante: a la información que manejan.

No se puede perder de vista que durante los últimos años hemos sido testigos de diferentes tipos de ataques sobre routers, como fue el caso de la "botnet Carna" y su "Censo de Internet en 2012", así como de otros eventos de menor escala que ocurrieron previo a Mirai. De hecho, podría decirse que Carna fue la precursora de la botnet Mirai, y si bien no tenía la intención maliciosa de esta última, Carna logró comprometer varios y diversos dispositivos como routers tipo SOHO. El caso de la botnet Mirai fue uno de los más populares. Compuesta principalmente por dispositivos IoT comprometidos (llegó a infectar 600.000 dispositivos alrededor del mundo), ha sido utilizada para realizar decenas de miles de ataques DDoS; entre ellos uno de los más grandes de la historia, cuando en octubre de 2016 atacaron los servidores

de Dyn y provocaron la caída de populares servicios como Netflix, Twitter, Spotify, PayPal, así como varios medios de comunicación de Estados Unidos y Europa. Asimismo, también se realizaron investigaciones sobre los asistentes de voz, en las que una de las más recientes demostró que es posible enviar comandos ocultos, que no son detectables para el oído humano, a asistentes como Siri de Apple, Alexa de Amazon y al Asistente de Google; logrando activar los sistemas dispositivo, sin que el usuario se percate, y hacer llamadas o abrir sitios web.

Y si bien muchas de estas investigaciones partieron de pruebas de conceptos, demuestran que es posible para un atacante desbloquear dispositivos, hacer transferencias bancarias o realizar compras en línea simplemente encubriendo mensajes maliciosos en una reproducción de audio normal.

Por lo tanto, hay un desafío de cara al futuro, ya que proteger estos puntos concentradores en todo nuestro mundo conectado no será fácil. Por ejemplo, un mal funcionamiento en estos componentes o un ataque que los use como plataforma puede llevar a comprometer la información de una gran variedad de dispositivos.

Si bien la usabilidad y facilidad que los dispositivos inteligentes ofrecen al usuario están muy bien valoradas, también pueden representar una puerta abierta para el ingreso de amenazas. La realidad es que a medida que se avanza hacia una mayor adopción en el uso de dispositivos IoT agrupados bajo un asistente doméstico, los riesgos para la seguridad y privacidad aumentan. No se puede perder de vista que con la evolución de la tecnología también evoluciona la forma en que piensan y actúan los cibercriminales.

El equilibrio entre usabilidad y seguridad

Si ya tienes dispositivos inteligentes en tu hogar o estás pensando en uno nuevo, deberías tener en consideración la seguridad que puede proveer. A principios de este año, investigadores de ESET publicaron un informe sobre el análisis de doce dispositivos IoT populares en el mercado y además de encontrar varias vulnerabilidades (en algunos casos incluso severas), cada uno de los dispositivos analizados presentó algún problema en materia de privacidad, siendo el desempeño de los asistentes inteligentes de voz lo que generó mayor preocupación. Por lo tanto, es importante investigar las características que el dispositivo como el fabricante ofrecen y a partir de esa información determinar si existe un balance entre comodidad y seguridad.

Así que si para el próximo año piensas comprar un Alexa, Google Home, Amazon Echo, Apple HomePod u otro asistente similar, ante todo debes estar al tanto de cuáles son los datos personales que capturan y comparten, y de esta manera determinar cuál es el más conveniente y el que mejor se adapte a tus necesidades de seguridad y tu expectativa de privacidad.

Los mismos ataques que hemos visto hasta hoy en Internet van a migrar hacia los dispositivos con menos características de seguridad. Así que es necesario considerar desde el lugar físico en los que se ubiquen estos dispositivos hasta pensar en adquirir aquellos dispositivos que ofrezcan mejores características de cifrado o con una autenticación robusta. Son medidas que hay que tener en cuenta porque aún estamos lejos de estándares de seguridad para IoT.

Si bien la usabilidad y facilidad que los dispositivos inteligentes ofrecen al usuario están muy bien valoradas, también pueden representar una puerta abierta para el ingreso de amenazas.

Así que 2019 nos presenta un panorama complejo en cuanto a las amenazas que podamos ver para estas tecnologías, y si bien las preocupaciones de seguridad y privacidad pueden ser muchas, es momento de que como usuarios tomemos medidas de protección y no dejemos estas decisiones a la deriva o únicamente en manos de los fabricantes.

El foco de seguridad en los datos

Así que, ¿hacía donde debería estar el foco de la seguridad para el próximo año cuando hablamos de dispositivos como los asistentes personales? Lo más importante sobre la seguridad en este caso es precisamente saber cuáles son los datos que intercambian y recolectan estos dispositivos: información de identificación, datos que permitan acceder a perfiles online, información financiera y en general datos que pudieran resultar sensibles. La amplia variedad de dispositivos, tecnologías, protocolos y proveedores hace complejo pensar en llegar fácilmente a una estandarización que permita definir las medidas de seguridad que se puedan adoptar. Este es un proceso que llevará tiempo y no será el próximo año cuando veamos estos estándares implementados.

Así que mientras llegamos a ese punto, los fabricantes deberán ocuparse de establecer políticas de seguridad en la capa de aplicación de sus productos que permitan proteger la integridad y la confidencialidad de los datos. De lo contrario, será posible encontrar ataques en los que a partir de la inyección de código logren explotar vulnerabilidades que permitan llegar hasta la información almacenada en los servidores.

¿Qué depara el futuro?

Al día de hoy hemos visto un incremento en la superficie de ataque, con casos en los que se llegó a sistemas que utilizan una amplia gama de tecnologías y protocolos de comunicación. Y junto a este crecimiento veremos cómo durante el próximo año las amenazas tendrán diferentes vectores de ataque que aprovecharán la amplia variedad de opciones.

Ya vimos como los cibercriminales utilizaron dispositivos IoT para hacer amplios ataques de denegación de servicio, pero en la medida que se conectan más dispositivos y se integran en la vida de todos, los atacantes continuarán explorando sus características para detectar otras vulnerabilidades (ya lo han hecho con termostatos, sistemas de cámaras de seguridad, juguetes para niños, vehículos, etc) y así llevar amenazas como los fraudes, el ransomware o la minería de criptomonedas a estos dispositivos de manera generalizada. Con el crecimiento en la adopción de criptomonedas y la gran cantidad de dispositivos conectados a Internet, los dispositivos inteligentes pueden convertirse en el punto de entrada para que un atacante obtenga grandes granjas de criptominería.

Hay quienes se muestran preocupados ante esta realidad y ya están tomando medidas. Un ejemplo es la aprobación de una nueva ley en el estado de California, Estados Unidos, que para el año 2020 exigirá que todos los dispositivos IoT comercializados en el mercado deberán venir configurados con contraseñas únicas.

Por lo tanto, dado este panorama que pareciera no muy alentador, como usuario es necesario que conozcas sobre los dispositivos que adquieres, las características ofrecidas por los fabricantes y sobre todo hacer un uso seguro de la tecnología. La realidad es que la amplia variedad de fabricantes en su carrera desenfrenada por vender sus productos puede dejar muchos de ellos con vulnerabilidades que los dejen más expuestos. Por lo tanto, ser consciente de que existen riesgos es la mejor manera de estar preparado para mantener seguros tus dispositivos y la información que se maneja a través de ellos.

Los mismos ataques que hemos visto hasta hoy en Internet van a migrar hacia los dispositivos con menos características de seguridad.

CONCLUSIÓN

2018 fue un año en el que los datos y la privacidad tuvieron un protagonismo especial. Casos específicos como el incidente de Facebook y Cambridge Analytica o la entrada en vigencia del Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) fueron, en gran medida, responsables de que la privacidad y la seguridad de los datos diera tanto de qué hablar.

Las secciones de este informe muestran la importancia que tienen los datos, tanto para las empresas, los usuarios, para quienes se encargan de brindar protección y también para los cibercriminales.

Tal como hemos visto, la evolución de las amenazas no es ajena a la evolución de la tecnología ni del comportamiento de los usuarios. Así como los mercados buscan conocer más de cerca el comportamiento de los usuarios en Internet para establecer una comunicación personalizada, lo mismo sucede en el caso de los atacantes, quienes seguramente comenzarán a adoptar el uso de tecnologías como el Machine Learning en su afán de recopilar datos que luego puedan ser utilizados para realizar campañas de ingeniería social personalizadas y más convincentes.

Por lo tanto, en este contexto en el que toda actividad que realizamos en la era digital deja una huella, y en el que seguirán existiendo incidentes que afectarán a empresas y a usuarios, la entrada en vigencia del GDPR representa un faro para el mundo que seguramente comenzará a replicarse en distintos países y regiones a través de distintas iniciativas para la protección de datos. Y si bien el GDPR despertó muchas interrogantes en el sector empresarial, fundamentalmente en aquellos países que no estaban ubicados dentro de la Unión Europea, los hechos ocurridos este año parecen haber provocado un cambio de consciencia que hasta ahora no se había logrado. ¿Será esto suficiente? Probablemente no lo sea.

Este escenario marcado por el surgimiento de reglamentaciones para la protección de datos plantea un desafío: cómo se complementarán y articularán las nuevas normativas que vayan surgiendo en cada región o país con el resto de los países, siendo que la propia naturaleza de Internet es el desconocimiento de las fronteras geográficas. También plantea otro tipo de interrogantes, como saber qué sucederá cuando dos normas se contradigan o se detecten vacíos legales ante casos no previstos. Porque aparte de establecer normas, se requiere de un sistema que acompañe las necesidades que vayan surgiendo y que contemple los avances naturales para actualizar las normas a cada tiempo. En este sentido, es el momento donde las empresas y los gobiernos deben demostrar su compromiso y no dejar todo librado a las empresas de seguridad o a los usuarios, ya que la situación así lo requiere.

A medida que se desarrollan los avances tecnológicos, la superficie de ataques se amplía cada vez más y por eso el desafío pasa por llevar adelante educación en varios planos y públicos. En un mundo actual atravesado por la interconectividad, donde todos los servicios están vinculados entre sí en la nube, en el que los asistentes virtuales, los routers y demás dispositivos inteligentes pueden ser la puerta de entrada para el robo de información o en el que un sitio web puede haber sido infectado por un código malicioso para minar criptomonedas, se hace cada vez más necesario un perfil de usuario más atento, con más herramientas para hacer un uso responsable y consciente de la tecnología, que sepa, no solo cómo protegerse, sino además conocer acerca de la responsabilidad y los riesgos que conlleva subir información personal a la nube, así como también ser consciente de qué tipo de información está subiendo y compartiendo con servicios de Internet legítimos.

Y las organizaciones, empresas y fabricantes deberán hacer su parte si no quieren verse afectadas por usuarios que perdieron la confianza como consecuencia de haberse visto perjudicados a raíz de un incidente de seguridad. Incluso compañías como Facebook, cuyo principal valor es el servicio que ofrece a partir de la manipulación de grandes volúmenes de información personal, ya no tiene la misma percepción que antes por parte de los usuarios. Pero la realidad es que no todas las empresas tienen una segunda oportunidad para demostrar que consideran prioritario el resguardo de dicha información, y puede llegar a ser suficiente un solo un incidente donde se vean comprometidos los datos privados de las personas para que se pierda definitivamente la confianza y que eso derive en la desaparición de un servicio o el quiebre de una empresa.

2019 comenzará y seguirán existiendo casos de brechas de seguridad, dispositivos que salen de fábrica sin haber tenido suficientes controles de seguridad y campañas sofisticadas que afecten a entidades críticas. Paralelamente, seguirán llegando a la bandeja de entrada los usuarios campañas de phishing clásicas que intenten aprovecharse de individuos sin las aptitudes suficientes para hacer un uso seguro de la tecnología. Ante esta diversidad de ataques y complejidades de los mismos, existen múltiples responsabilidades de los diversos actores de la sociedad (empresas, usuarios, fabricantes, gobiernos, organizaciones de la sociedad civil) para asegurarse que la privacidad y confidencialidad de los datos se mantendrán.

Esperemos que este informe sea de utilidad para aquellos que tienen injerencia en la toma de decisiones y que entre todos podamos colaborar para hacer de la tecnología un entorno más seguro.