NAVEGACIÓN SEGURA:

su transformación digital no estará segura sin ella

El año 2017 estuvo repleto de titulares sobre apropiaciones fraudulentas de cuentas a manos del malware financiero. En retrospectiva, la llegada del troyano Trickbot puede haber sido el punto de inflexión en una nueva era de ataques de malware. Nunca antes el alcance de un troyano había sido tan global: los bancos de los Estados Unidos, América Latina y Europa fueron su blanco, y sus sofisticadas técnicas de redirección dificultaron la detención de su propagación. Sus ataques tampoco hicieron diferencia; entre los objetivos figuraban los 20 bancos más importantes, bancos medianos e incluso instituciones locales pequeñas. Pero Trickbot fue solo el comienzo de la embestida.

El troyano Marcher, diseñado para atacar móviles Android, también evolucionó para mantenerse al día. Las versiones anteriores utilizaban mensajes de texto SMS de phising como vector de ataque, pero las nuevas interacciones del malware también han agregado esquemas de phishing que se envían a través de aplicaciones móviles y correo electrónico no autorizados, así como malversación en sitios web pornográficos. Al igual que Trickbot, Marcher se basa en una combinación de phishing, superposiciones maliciosas en una aplicación legítima y un toque de ingeniería social con el fin de engañar a las víctimas para que les entreguen los datos de su cuenta bancaria y tarjeta de crédito.

Estos tipos de malware siguen expandiéndose, mientras que otros se desarrollan y cobran vida a un ritmo sin precedentes. Los directores de TI de los bancos de todo el mundo tienen buenas razones para ser cautelosos. De todas las industrias, el sector financiero es el principal objetivo de los ciberdelincuentes, ya que los frutos de un ataque exitoso son, en promedio, los más rentables, según un informe del analista de ciberseguridad Flashpoint. Y, mientras las aguas vuelven a su cauce después de la caída de estos troyanos bancarios, hay otra cifra que las instituciones financieras deben conocer: en todo el mundo, las pérdidas por apropiación fraudulenta de cuentas ascienden a un valor aproximado de $7 mil millones de dólares por año[1].

Los periodistas y analistas de ciberseguridad hablan cada vez más de miseria y desolación, y por razones alimentarias: están surgiendo nuevas estrategias y técnicas de ataques fraudulentos con una constancia aterradora. En un informe publicado recientemente, 26 destacados expertos en seguridad advirtieron que la Inteligencia Artificial (IA) es una presa fácil de aprovechar para los estados deshonestos, ciberdelincuentes y terroristas. El uso malintencionado de la IA para fines fraudulentos es algo que, sin duda, veremos en 2018. Este tipo de amenaza vanguardista aumenta la eficacia de los ataques de phishing de siete a 20 veces, según nuestra última investigación académica sobre el tema[2].

Si bien el futuro es incierto y hay motivos de preocupación, no todo está perdido. La gran mayoría de los ciberataques presenta vulnerabilidades propias; a pesar de las técnicas de infección inteligentes, el malware en dispositivos aún necesita comunicarse con el atacante para que este pueda obtener información robada, y el malware en páginas necesita cambiar los campos de los formularios de los sitios web para capturar las credenciales de inicio de sesión. Sin embargo, incluso si surgen nuevos ejemplares de malware, con la protección adecuada, los ciberdelincuentes encontrarán cada vez más difícil detectar una vulnerabilidad en el dispositivo o durante las transacciones.

La detección de malware heredado ya no es confiable por sí sola

Los ataques dirigidos contra las instituciones financieras están en aumento, y los tipos de ataques han evolucionado. Considere lo siguiente: en los últimos dos años, los troyanos bancarios y otros ataques financieros de malware han alcanzado niveles sin precedentes. Cada mes, se crean 1,4 millones de sitios de phishing nuevos; en 2016, los ataques de troyanos bancarios en todo el mundo aumentaron un 30 %; entre 2015 y 2016, los ataques de phishing aumentaron un 65 %.

$7 mil millones de dólares

Pérdidas totales en todo el mundo debido a la apropiación fraudulenta de cuentas cada año.

Esto significa que las formas en que las instituciones financieras garantizan que los clientes se conecten de manera segura a sus plataformas en línea y realicen transacciones deben evolucionar para estar al día respecto de las últimas tendencias de fraude. Hasta hace poco, una estrategia de navegación segura efectiva consistía en implementar productos que detectaran malware en dispositivos de usuario final y que eliminaran esos ejemplares específicos. Lamentablemente, esta estrategia no basta si se aplica sola contra el avance incesante de la ciberdelincuencia. La búsqueda y mitigación del malware, a pesar de seguir siendo una práctica recomendada sensata, ya no se puede considerar una panacea por sí sola porque el malware siempre está evolucionando, y hay muchos tipos que están diseñados específicamente para evadir ese método de detección. Por citar solo un ejemplo: las nuevas variantes de malware producen infecciones web no detectables hasta que el ataque se implementa por completo y se comunica a los proveedores de productos antimalware.

Otro motivo por el que es necesario reforzar las estrategias de seguridad de los puntos de conexión es que los grandes desarrolladores de sistemas operativos y los fabricantes de teléfonos inteligentes y tablets son conscientes de la amenaza, y han reforzado la seguridad de los dispositivos y tiendas de aplicaciones en el proceso. Google, por ejemplo, sigue restringiendo el acceso de las aplicaciones al sistema operativo Android, al hardware y a los permisos para que las aplicaciones se vean entre sí.

El resultado es un menor riesgo de seguridad para los usuarios y menos oportunidades para quienes afirman proporcionar protección independiente para puntos de conexión móviles.

1. "Apropiación fraudulenta de cuentas: qué necesita saber sobre esta artimaña de $7 mil millones". http://blog.easysol.net/account-takeover/
2. "DeepPhish: Simulación de la IA maliciosa", Alejandro Correa Bahnsen, Iván Torroladlo, Luis David Camacho, Sergio Villegas, febrero de 2018, página 7.

Apple ha ido aún más lejos, al prohibir directamente cualquier aplicación que ofrezca a los usuarios de teléfonos inteligentes/tablets protección antivirus o antimalware en su App Store. Su política establece: "No incluya ninguna función oculta o no documentada en la aplicación; la funcionalidad de la aplicación debe ser clara para los usuarios finales y para App Review. Del mismo modo, no debe comercializar su aplicación en la App Store ni fuera de línea, como contenido o servicios que no ofrece realmente (p. ej., detectores de virus y malware basados en iOS). El comportamiento atroz o reiterado es motivo para la eliminación del Developer Program"[3].

Sin embargo, estas restricciones contra las aplicaciones de protección antivirus o antifraude solo se aplican en el ámbito móvil y no en computadoras portátiles o de escritorio. Las soluciones tradicionales de protección de puntos de conexión tampoco sirven como defensa contra las amenazas dirigidas a los inicios de sesión y transacciones bancarias móviles, como las aplicaciones móviles con acceso remoto falsas que engañan a los usuarios para que las descarguen; los ataques superpuestos que colocan una pantalla de inicio de sesión falsa sobre una aplicación bancaria cuando esta se activa y la manipulación de aplicaciones legítimas que permite a los hackers acceder a datos confidenciales de inicio de sesión.

Por otra parte, las computadoras portátiles y de escritorio pueden beneficiarse de la protección de los puntos de conexión. Dado que los hackers suelen depender de vectores de ataque más tradicionales en el caso de las computadoras personales (en lugar de aplicaciones móviles falsas), la protección de los puntos de conexión de las computadoras portátiles y de escritorio sigue siendo una opción de seguridad adecuada para esos tipos de dispositivos.

Sin importar si los ataques están dirigidos a dispositivos móviles o computadoras personales, es necesario pensar qué debería incluir una estrategia de navegación segura y completa; en parte para sustituir la detección de malware en puntos de conexión como el principal mecanismo de seguridad. Un nuevo enfoque ante este problema implica alejarse de los intentos de detección y mitigación del malware presente en los dispositivos de usuario final, y acercarse a una gestión más prudente de esos dispositivos. La idea es bloquear la comunicación entre el malware y el atacante al crear una conexión muy segura entre el cliente y el banco.

El enfoque de seguridad contra el fraude multicapa se considera una buena práctica: factores de protección superpuestos e integrados que no funcionan de manera independiente. Sin embargo, muchos siguen teniendo estrategias de seguridad que funcionan en un silo: soluciones antifraude que tratan cada ataque como distinto según el canal y que carecen de la interconectividad y el intercambio de inteligencia necesarios para tener un panorama general del fraude.

Cuando las organizaciones implementan una estrategia antifraude basada en silos en lugar de un enfoque más holístico, es posible que creen, sin saberlo, un punto ciego y expongan sus sistemas a las formas en que el malware y otras amenazas aprovechan las vulnerabilidades de los dispositivos y las sesiones. "Hoy vemos a los ciberdelincuentes usar software avanzado y ataques sofisticados y de múltiples enfoques contra instituciones financieras y otras empresas para hacer uso de su infraestructura contra ellos", advierte Leo Taddeo, director de Seguridad de la Información de Appgate y exdirector de la División de Operaciones y Cibernética. Si una empresa analiza cada uno de ellos en un silo, se ubican en una clara posición de desventaja. Debemos pensar más en las estrategias que las fuerzas del orden público despliegan, es decir, analizar una organización (de ciberdelincuencia) en todas las diferentes fases que utiliza para ejecutar y completar el fraude", afirmó.

Con esta perspectiva en mente, una estrategia de seguridad debe considerar la protección de todas las vías de amenaza que los ciberdelincuentes tienen en cuenta para que cualquier marco de navegación segura sea realmente inaccesible.

Abordar las causas fundamentales del fraude

A esta altura, todos deberíamos saber que cualquier estrategia de ciberseguridad es tan fuerte como su eslabón más débil, y el eslabón más débil fue, es y seguirá siendo el ser humano. Esto se evidencia por el gran número de personas que todavía son engañadas por estafas de phishing. Solo en los Estados Unidos, el phishing y, en particular, las estafas que comprometen los correos electrónicos corporativos (también conocidas como spear phishing) cuestan a las empresas alrededor de 500 millones de dólares al año.

Para reducir la tasa de éxito del phishing, muchos departamentos universitarios de informática, bancos y compañías de comercio electrónico lanzaron una serie de campañas de concienciación para enseñar a los empleados y clientes a detectar con precisión la diferencia entre un correo electrónico legítimo y una estafa de phishing. Estas campañas demuestran un impacto positivo constante, con un promedio de alrededor de 10 por ciento menos de clics en los correos electrónicos de phishing durante los ejercicios de simulación. Sin embargo, con un promedio de 156 millones de correos electrónicos de phishing enviados todos los días, un 10 por ciento menos de personas engañadas en estas estafas no es suficiente.

Las protecciones tradicionales tampoco ayudan mucho. En términos globales, alrededor del 10 por ciento de todos los correos electrónicos de phishing pasan los filtros de spam y, de ellos, 8 millones son abiertos por los destinatarios. 800 000 personas hacen clic en los enlaces maliciosos contenidos en esos correos electrónicos, y alrededor de 80 000 caen en la estafa todos los días, lo que da lugar al robo de identidad, fraudes de tarjeta de crédito y pérdidas financieras por la apropiación fraudulenta de cuentas[4]. Como es de esperar, hay igual espacio para contratar software malintencionado en dispositivos móviles que para computadoras portátiles y de escritorio.

156 millones

Número promedio de correos electrónicos de phishing Se envían cada día

Como ya se ha mencionado, Apple y Android han hecho grandes avances en la búsqueda de la seguridad de sus sistemas operativos, pero los estafadores son implacables en la eliminación de malware nuevo y más difícil de detectar. Esto significa que las aplicaciones móviles falsas que ofrecen gran cantidad de programas maliciosos a través de troyanos siguen siendo un problema. También lo son los riesgos que supone liberar los teléfonos inteligentes de las limitaciones impuestas por el fabricante, una práctica conocida como jailbreaking (desbloqueo de iOS) o rooting (desbloqueo de Android). Los usuarios pueden elegir entre jailbreaking o rooting para sus teléfonos por varias razones (p. ej., utilizarlos con diferentes operadores de telefonía móvil), pero el inconveniente es que el teléfono, ya sea Android o iOS, se vuelve inseguro por naturaleza. Los atacantes son incluso conocidos por desarrollar malware dirigido específicamente a los teléfonos con jailbreaking o rooting, ya que son mucho más fáciles de infectar.

3. "Pautas de revisión de App Store". https://developer.apple.com/app-store/review/guidelines
4. "Phishing: ¿Cuántos muerden el anzuelo?". Seguridad Pública de Canadá: http://www.getcybersafe.gv.ca/cnt/rsrcs/nfgrphcs-2012-10-11-en.aspx

No se puede depender de los clientes y empleados para evitar por completo las muy convincentes estafas de phishing o las descargas de aplicaciones móviles sospechosas. Corresponde a las instituciones financieras proteger a los usuarios de ellos mismos. Estas organizaciones no pueden controlar lo que hace su base de clientes en sus computadoras portátiles o teléfonos, y tampoco pueden despreocuparse de su negocio principal para dedicar tiempo y recursos a detectar y neutralizar el malware en forma constante. Por lo tanto, una estrategia que aborde el panorama general debe hacer mayor hincapié en la gestión de amenazas, en lugar de su detección y eliminación. Esto no quiere decir que la detección de amenazas no sea importante: la detección de amenazas en vectores de ataques siempre será un pilar esencial para la prevención del fraude. Sin embargo, resulta aún más esencial la protección contra las causas fundamentales del fraude, o la capacidad del malware en un dispositivo para comunicar al hacker la información que ha recopilado y que puede utilizar para rastrear y robar fondos.

Interrumpir la estructura de mando y control del ciberataque y obstruir el vínculo entre el actor malintencionado y el dispositivo infectado es negar al malware la capacidad de hacer su trabajo, lo que lo hace inofensivo. Esto se puede lograr al crear una conexión hermética entre el cliente y el banco mientras la actividad transaccional está en curso.

No todas las soluciones de navegación seguras se crean iguales

Algunas soluciones de seguridad populares no consideran la prevención de amenazas de manera holística, sino que (y esto es aún peor) proporcionan solo un tipo de protección y se enfocan en un solo vector de amenazas. Otros productos antifraude amplían la protección independiente y no están diseñados para funcionar junto con otras soluciones a fin de proporcionar un marco de seguridad más sólido y de enfoques múltiples. Por ejemplo, algunas soluciones proporcionan una conexión segura entre la institución financiera y sus clientes, y buscan y neutralizan en forma activa el malware que se encuentra en computadoras y dispositivos móviles. La protección que administra es buena, suponiendo que todos los ataques se envíen y se lancen a través del navegador web de un dispositivo. Sin embargo, para el malware más avanzado que existe hoy en día, los navegadores web son solo uno de los numerosos vectores de ataque que aprovechan los ciberdelincuentes para hacer llegar su malware a tantos dispositivos como sea posible. Los proveedores de seguridad que ofrecen una solución antifraude basada en navegador no pueden proteger contra ataques Man-in-the-Middle (con intermediarios) sofisticados y otros tipos de ataques. Por esta razón, una solución de seguridad dinámica y orientada al cliente no debería "vivir" en el navegador, por así decirlo, sino ser "agnóstica" respecto del navegador web; es decir, que pueda detectar malware independientemente de cómo se envíe a un dispositivo.

Otras soluciones sin cliente, o las que ofrecen protección a los dispositivos móviles y no requieren acción alguna del usuario final, identifican el malware de manera activa, pero, lamentablemente, muchas adoptan un enfoque reactivo. Algunos de estos tipos de soluciones funcionan enfocándose en la identificación de amenazas de malware conocidos. Como tales, no son buenos para detectar ataques nuevos y previamente desconocidos. Las soluciones heredadas como estas tienden a arrojar una red demasiado amplia, consideran las conexiones legítimas de los clientes como amenazas potenciales y, como resultado, generan gran volumen de alertas, lo que exige que el departamento de TI de la organización analice cada una en forma manual para determinar cuáles son amenazas reales y cuáles son falsos positivos.

La debilidad presente en los sistemas heredados que muchos proveedores de ciberseguridad venden demuestra dos cosas: que las soluciones manuales realizan un trabajo adecuado al detectar y mitigar la mayoría de los ataques de fraude, pero que no pueden neutralizarlos a todos. También revela otra deficiencia: que las soluciones antifraude "independientes" en silos son menos efectivas porque sus productos no están diseñados para integrarse, comunicarse o complementarse entre sí. En otras palabras, no pueden proporcionar verdadera seguridad contra el fraude de múltiples enfoques y, como resultado, las instituciones financieras que implementan estas soluciones, así como su base de clientes, podrían ser vulneradas.

Práctica recomendada: proteger las sesiones bancarias en línea y móviles

Dada la variedad de dispositivos, los vectores de amenazas y los riesgos asociados con un personal que se encuentra cada vez más fuera de los perímetros de seguridad convencionales, la posibilidad de que los dispositivos de los usuarios se infecten es mayor que nunca. La interconectividad de los dispositivos en una red cada vez más nebular requiere la protección específica de los dispositivos en torno a la actividad transaccional, ya que cada tipo de dispositivo tiene su propio conjunto de necesidades de seguridad.

Las tres principales áreas de preocupación son: las computadoras portátiles y de escritorio, los dispositivos móviles y la página web transaccional de la institución financiera. Estos son los puntos de contacto a los que quieren acceder todos los ciberdelincuentes. No importa cómo los clientes se conecten al sistema de una institución financiera, la protección de la sesión es fundamental. Cada una de las tres categorías merece una solución. Las empresas e instituciones financieras inteligentes buscan proveedores que ofrezcan soluciones de seguridad que cubran todos los posibles vectores de ataque, con ventajas y componentes que la empresa elija para satisfacer sus necesidades individuales de ciberprotección.

BANCA MÓVIL

La forma ideal de protegerse contra las ciberamenazas en una computadora de escritorio será diferente de la forma ideal de proteger un teléfono inteligente. Por ejemplo, en el caso de los clientes que desean conectarse a sus cuentas en línea a través de una computadora portátil, la institución financiera haría bien si proporcionara un producto antifraude práctico que el cliente pueda descargar e instalar en su equipo. Además, una solución integral y completa protegería al cliente al detectar cualquier proceso malicioso que se ejecute en el equipo, al bloquear cualquier malware que intente comunicarse con su creador mientras el cliente está en sesión y al impedir que el usuario explore cualquier sitio de phishing o clonado conocido.

Para los clientes de una institución financiera que desean realizar sus operaciones bancarias a través de su teléfono inteligente o tablet, toda la protección que necesitan se puede integrar o "crear" en la propia aplicación móvil del banco. La protección de la conexión móvil entre el cliente y el banco con un software antifraude versátil puede ser casi invisible para el usuario final, y debe proteger contra ataques peligrosos, como la falsificación de aplicaciones, intercepciones Man-in-the-Middle, phishing, pharming y aplicaciones reempaquetadas. Pero no solo eso; una solución de protección contra el fraude móvil realmente exhaustiva debe poder analizar si un dispositivo está en riesgo (por ejemplo, si se lo desbloquea) y, por lo tanto, si se le debe denegar acceso a los sistemas.

Sin importar si la amenaza es móvil o basada en computadora, siempre habrá una parte considerable de los usuarios finales que se negará a descargar e instalar la protección antifraude que se les ofrece. Es posible que se sientan más cómodos al iniciar sesión en su cuenta en línea a través del sitio web, o que simplemente no quieran agregar otra aplicación a su dispositivo. Cualquiera sea la razón, este tipo de clientes no consideran los peligros y las trampas de las amenazas de fraude con la seriedad que merecen. Sin embargo, los bancos y otras organizaciones también deben proteger a estas personas. Por esta razón, una solución que detecte cualquier modificación maliciosa que se haya insertado en el portal transaccional del banco es siempre una medida prudente.

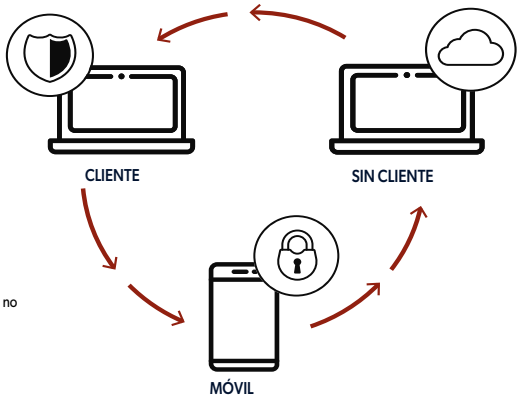
Marco de Detect Safe Browsing (DSB) de AppGate

Por suerte, existe un conjunto de productos que pueden ayudar a evitar que cualquier dispositivo sea víctima del fraude de identidad digital y mitigar la mayor variedad de riesgos para los puntos de conexión: Detect Safe Browsing de AppGate. El marco de DSB adopta un enfoque por capas para la detección y prevención de ataques de malware a través de diferentes factores de forma que pueden funcionar de manera conjunta.

- DSB Client: Una aplicación que se descarga en la computadora portátil o de escritorio del usuario final que detecta y analiza el malware financiero en los dispositivos del usuario. La aplicación puede bloquear las conexiones de comando y control de cualquier malware dirigido a una institución financiera, y proporcionar visibilidad en el entorno de navegación del usuario final y obstruir las amenazas en tiempo real.
- DSB Clientless: Una solución transparente que detecta inyecciones de malware en páginas transaccionales de sitios web, sin que sea necesaria la acción del usuario final. Clientless utiliza una tecnología patentada que toma una Malware SnapshotTM o una captura de pantalla que proporciona pruebas concretas del malware en acción.
- DSB Mobile: El Software Development Kit (SDK) móvil de Detect Safe Browsing es una biblioteca que se puede integrar en cualquier aplicación de banca móvil personalizada para sistemas operativos iOS o Android. La solución, que proporciona una conexión extremadamente segura entre la plataforma de banca móvil y el dispositivo del cliente, puede detectar y hacer que las amenazas pierdan poder sin inconvenientes para el usuario final.

Con estas tres tecnologías funcionando en conjunto, Detect Safe Browsing evita la actividad maliciosa que da lugar a la apropiación fraudulenta de cuentas y otros ciberataques sofisticados, proporciona pruebas procesables de que se está llevando a cabo un ataque y protege la conexión entre el banco y el cliente con un nivel tan alto que se garantizan transacciones seguras, incluso en dispositivos infectados por malware o en peligro de otro tipo.

Cada factor de forma de DSB tiene su propia especialización, de modo que cuando los tres se despliegan juntos en un conjunto de productos que denominamos el marco de DSB, proporcionan una solución contra el fraude realmente sólida y de múltiples enfoques que le ofrecerá a usted y a su cliente tranquilidad respecto a la realización segura de las transacciones bancarias en línea. Los sólidos sistemas de protección, detección y prevención multicapa que conforman el marco de DSB garantizan que su organización evite convertirse en uno de los llamados "hitos de la ciberdelincuencia" de 2018 y demás.



Detecte la navegación segura con cliente

Una solución que se puede descargar y protege las PC y Mac de los ataques de phishing y malware

- Software ligero de escritorio para PC
- Backend en la nube
- Arquitectura abierta de API
- Independiente del navegador
- Protección incluso cuando se actualiza el navegador
- Se enfoca en el comportamiento malicioso, no en las firmas

Detecte la navegación segura sin cliente

- Detección de ataques de phishing, MitM, MitB, de día cero y malware enfocado
- Identifica inyección de código HTML en páginas
- Malware Snapshot® registra la evidencia de ataques
- Detección de datos de ingreso comprometidos

Detecte la navegación segura con un SDK móvil

Protege tanto la aplicación bancaria como la navegación móvil, detectando malware y otros riesgos móviles.

- Visibilidad total
- Implementación simple
- Protección contra ataques Mit, de superposición, pharming y repackaging enfocados de aplicaciones
- Evaluación de riesgo de dispositivos y autenticación basada en riesgos

appgate