EFECTIVA PROTECCIÓN DE IDENTIDAD: BUENA GESTIÓN DE CLAVE DE ACCESO + DETECCIÓN DE FILTRACIONES

Las herramientas de protección de la identidad digital ofrecen a los proveedores de servicios maneras hasta ahora impensadas de alcanzar a nuevos posibles clientes. Sin embrago, los interesados deben elegir cuidadosamente un producto que no sólo rapidamente detecte una filtración de datos, sino que impida que ésta ocurra.

F-Secure

CONTENIDO

INTRODUCCIÓN

El área de la protección de la identidad digital , la cual ya es un negocio consolidado en América del Norte, está actualmente en áuge en América Latina como una nueva modalidad de seguridad. Asimismo, los nuevos informes del tema indican que las actual crisis de salud mundial está propiciando el aumento del robo de identidad y otros delitos en línea. Más que nunca los usuarios necesitan contar con una de protección de identidad efectiva.

De acuerdo con un reciente estudio de Finanso.se, el robo de identidad, ya muy generalizado en los países europeos, se ha convertido en el segundo tipo de fraude más común en Europa. Dada la pandemia y la crisis economica mundial, Javelin Research pronostica un alza en las estafas y los fraudes de apropiación de cuentas para el 2020. Hecho debido a que los hackers son más activos durante los periodos de adversidad monetaria. Incluso la comisaria de la unión europea, Ylva Johanson, advertió recientemente acerca del áuge del robo de identidad y otros fraudes online a medida que la gente se va quedando más tiempo en sus hogares.

Según lo reveló una encuesta efectuada por F-Secure el 2019, el problema ya es una preocupación muy concreta entre los usuarios. El 56% de ellos estánpreocupados ante la posible filtración de sus datos personales; el 55% está preocupado por ser víctima de fraude en compras en línea y al 58% le causa dolor de cabeza que su cuenta bancaria pueda ser vaciada.

Las cifras demuestran que la gente está lo preocupada como para evaluar adquirir una herramienta de protección: 52% dice que un sistema de alerta para cuando se han filtrado de datos privados sería un servicio atractivo. El 26% estaría dispuesto a pagar por él y al 34% le gustaría adquirirlo a través de su proveedor de telefonía móvil o de banda ancha.

EL “ESCENARIO” ESTÁ PREPARADO

Al parecer el momento actual nunca ha sido más propicio para los proveedores de servicios que piensan en incorporarse al emergente negocio de las soluciones de protección de identidad. Éstas les permiten adoptar perspectivas de marketing muy novedosas y llegar a un nuevo publico. Los servicios en cuestión apuntan al "público premium", es decir, a la Generación X, ya que, por ejemplo, el 46% de las víctimas de robo de identidad tienen entre 30 y 49 años.

Pero antes de que los proveedores de servicios se dediquen a ofrecer esta nuevo tipo de productos, es conveniente considerar la forma en que estos funcionan, ya que no todas las ofertas de PID son idénticas. Se debe tener precaución de elegir una solución que proporcione a sus clientes el equilibrio adecuado entre la detección efectiva del robo de identidad y la prevención del abuso.

Las actuales ofertas en esta materia en el mercado, tanto en el ámbito de los usuarios como en el de los proveedores de servicios, suelen ofrecer una vigilancia de reacción. Es decir, apuntando a las informaciones ya filtradas con alertas para cuando se encuentran esos datos y para que las víctimas puedan tomar medidas para disminuír el daño. Sin embargo, en orden de ofrecer a los clientes un servicio más completo y eficaz de protección de identidad, una herramienta debe incluir también medidas proactivas que pongan a los usuarios en mejores condiciones para así evitar que se produzca el ciberdelito.

Para determinar qué herramienta debe ser empleada, es útil comprender cómo se produce el robo de indentidad y cómo opera el mundo de la delincuencia en la web.

CÓMO OCURRE EL ROBO DE IDENTIDAD

Cuando pensamos en el robo de identidad, a menudo pensamos en cosas terribles: un número de seguridad social robado y una hipoteca solicitada a nombre de la víctima o también en cuentas bancarias vacías. Esos casos son devastadores, pero la gran mayoría de los robos de identidad actuales se producen en el ámbito de la apropiación de cuentas, que, según Javelin, ha crecido un 72% en 2019.

Perder su acceso a Netflix porque se ha sido hackeado es un ejemplo de apoderamiento de cuenta. Por supuesto que eso suena menos intimidante, sin embargo, esta forma de robo de identidad puede extenderse rápidamente desde, por ejemplo, la cuenta de streaming a otras tantas en línea de una misma persona. Con cada una de ellas, el hacker obtiene un mayor acceso a los detalles confidenciales y a la vida online de la víctima y, por ende, más oportunidades de hacerle daño económico o de otro tipo.

¿Pero cómo se extiende la apropiación de cuentas? La respuesta está en lo que se supone que nos protegería: en las claves de acceso. Como la mayoría de nosotros tenemos tantas cuentas online, está fuera de nuestro alcance recordar fácilmente un password único y fuerte para cada una de ellas.

Demasiados usuarios reutilizan la misma clave en todas dándole la "llave maestra"a cualquier criminal que la descifre.

Esto no sería un hábito tan arriesgado si no fuera por el hecho que los delincuentes utilizan constantemente diversos métodos para robar credenciales de acceso, desde el empleo de malware y campañas de phishing, hasta el robo de información en servicios en línea. En el caso de las filtraciones de datos, una vez que los piratas extraen los datos, los comparten en la web con otros otros delincuentes. Ellos utilizan herramientas automatizadas para descifrar claves codificadas. Mientras más cortas y más más débiles, más rápidas y fáciles son de descifrar, razón por la cual los criminales se enfocan en ellas.

Una vez que se logra descifrar un conjunto de claves, los hackers comienzan a ingresar a las cuentas con herramientas automáticas. Éstas les permiten comparar las claves obtenidas con un gran número de cuentas en línea para encontrar combinaciones que sirvan. Si una funciona en un sitio, puede ser utilizada para ingresar a otros servicios empleados por el usuario.

LA PROTECCIÓN PROACTIVA IMPLICA LA GESTIÓN DE CLAVES DE ACCESO

Si volvemos a la idea de un servicio de monitorización de ID, no hay duda de que tal es útil. Pero debido a la tendencia de los humanos a usar y reutilizar claves débiles, la monitorización de la ID por sí sola no combate la fuente del problema.

Lo que sirve para dar con la raíz de él es la administración claves de acceso. Los administradores de passwords ayudan a los usuarios a generar una clave fuerte y única para todas y cada una de las cuentas. Los de calidad son tan simples en su manejo que entrar a un programa de esos es incluso más fácil que reutilizar una clave débil.

F-Secure, líder en la alianza con proveedores de servicios para ofrecer soluciones de seguridad con valor agregado, incluye como parte de su herramienta de protección de ID un administrador de claves poderoso y simple de usar. F-Secure ID Protection incorpora la funcionalidad de la popular aplicación para consumidores F-Secure KEY, ofreciendo los beneficios de la gestión de passwords a los clientes de los proveedores de servicios.

El resultado: Una solución única de protección contra el robo de identidad enfocada en reducir el riesgo de convertirse en víctima de robo de identidad o de apropiación de cuentas. F-Secure ID, con su administración de claves incluída, ofrece algo verdaderamente único en el mercado.

"Los administradores de passwords ayudan a los usuarios a generar una clave fuerte y única para todas y cada una de las cuentas"

Desde luego que no existe un 100% de seguridad y aunque el riesgo puede ser reducido, nunca llega a ser cero. ¿Entonces qué pasa si un usuario está haciendo todo lo correcto, usando un administrador de claves para crear sólo aquellas fuertes y únicas y sin embargo su información confidencial sigue viéndose amenazada? sigue viéndose amenazada?

Es entonces cuando, como dice el refrán, el tiempo es crucial.

LA NECESIDAD DE ACTUAR RÁPIDAMENTE

Cuando los piratas ingresan a un sitio y extraen las claves, ellos por lo general sólo tardan unos días en descrifrarlas. Una vez que la información ha sido desencriptada y está lista para su uso en ataques, los criminales pueden empezar a hacerse cargo de las cuentas.

Eventualmente, la información traspasada llega hasta la dark web, lugar en internet inaccesible para los browsers y donde los piaratas compran, venden, comercian y bajan los datos robados.

La decodificación es a menudo efectuada con la ayuda de otros cibercriminales. Entre ellos se comunican a a través de lo que se conoce como la underground web, la parte más escondida, donde los hackers "sombrero negro" y otros delincuentes interactúan directamente. Es este el lugar donde la información pasa de mano en mano. Primero se reparte en un pequeño grupo, pero a medida que los datos circulan, se produce una distribución más amplia, entre los amigos y conocidos del atacante.

Eventualmente, la información traspasada llega hasta la dark web, lugar en internet inaccesible para los browsers y donde los piratas compran, venden, comercian y bajan alos datos robados. . Allí, en la dark web, la información información queda a disposición de cientos o incluso miles de potenciales hackers.

LA LÍNEA DE TIEMPO DE LA FILTRACIÓN

El criminal
descubre la debilidad

LA INTELIGENCIA HUMANA CONMIENZA AQUÍ

Día 0

LAS CREDENCIALES ROBADAS SON RECURSOS DE DATOS DE ALTO VALOR

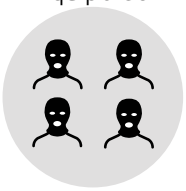
Un

Atacante

Día 2

El criminal
roba datos

Equipo de



Atacantes

Día 3

Los datos obtenidos
se comparten con el equipo

Amigos de

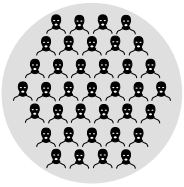
los atacantes

¡COMIENZA la toma de posesión de la cuenta!

LOS ESCÁNERES DE DARK WEB EMPIEZAN A ACTUAR

LOS DATOS ROBADOS SE FILTRANA A LA DARK WEB

Cientos de

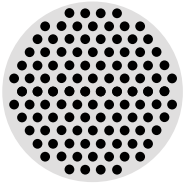


Atacantes

Día 200

Los escáneres de la Dark Web
empiezan a detectar datos

Miles de



Atacantes

Día 500

Los datos robados
terminan en listas compuestas

Los datos robados
son filtrados a la web pública

La mayoría de los servicios de protección de identidad funcionan vigilando la dark web y alertando a sus usuarios cuando se detectan allí sus datos. El problema es que, en esta etapa, lo más probable es que ellos ya hayan sido utilizados indebidamente con fines de lucro. Si bien nunca es perjudicial para las víctimas saber que sus informaciones han sido afectadas, en esta etapa puede ser demasiado tarde para prevenir daños a su expediente en línea o a sus cuentas bancarias.

La velocidad es muy importante: cuanto antes se puedan encontrar los datos de una víctima después de una filtración, mejor podrá ésta detener el abuso y la manipulación de sus cuentas online y evitar el robo de identidad. Detectar el problema incluso antes de que los datos lleguen a la dark web permite al usuario retomar el control, eso antes de que ellos sean puestos al alcance de grupos enteros de ciberdelincuentes.

INTELIGENCIA HUMANA

A diferencia de otros productos que no son capaces de detectar la información robada hasta que llega a la dark web, F-Secure ID Protection logra descubrir datos filtrados mucho antes. En promedio 6 a 9 meses antes que otras herramientas existentes en el mercado. Frecuentemente incluso a los pocos días de una filtración inicial.

Esto no significa que F-Secure no realice el monitoreo de dark web, porque sí lo hace. Pero la verdadera razón por la que es capaz de identificar información robada tan tan rápidamente es porque también incluye la inteligencia humana, proveniente de equipos de investigadores especializados. Estos expertos, a lo largo del tiempo, han establecido múltiples perfiles en la underground web, la parte más profunda, donde los hackers se comunican directamente. Allí, los investigadores utilizan estos perfiles para hacerles ingeniería social, aprovechando la confianza brindada para acceder a los datos filtrados en las primeras etapas de un delito.

> "F-Secure ID Protection es capaz de descubrir datos robados en un promedio de 6 a 9 meses antes que otras herramientas existentes en el en el mercado. Incluso a los pocos días de una filtración inicial "

Como los piratas son por naturaleza muy desconfiados respecto a cada nuevo contacto, la formación de una cadena en la underground web es algo que sólo es posible trás años de trabajo dedicado. Pero este esfuezo ha dado frutos: F-Secure goza de las mejores tasas de éxito y de tiempos de de descubrimiento del mercado. "Hit Rate" se refiere a la probabilidad de detectar y vincular los datos filtrados a una dirección específica de correo electrónico monitoreada. Mientras los competidores suelen hablar de una cifra de aciertos del 30%, la F-Secure alcanza el 55%.

ATRACTIVO MODELO DE LICENCIAS, NUEVAS FORMAS DE PARTICIPAR

Los mejores niveles de éxito en el área, los tiempos de detección más cortos y la excelente capacidad preventiva en la gestión de claves, son sólo algunas de las razones por las cuales los clientes estarán mejor protegidos. A parte de ello, F-Secure ID Protection también cuenta con un modelo simple de licencia familiar. Con sólo una suscripción, la cual incluye múltiples correos electrónicos, todo el hogar podrá podrá gozar de la protección de identidad.

El enfoque basado en aplicaciones, proporciona a los proveedores una manera más eficiente de relacionarse con los clientes que a través del correo electrónico. Con alertas, notificaciones y guía de reacción, se alcanza alcanza a los usuarios a tiempo y dondequiera se encuentren sus dispositivos electrónicos. Con F-Secure los proveedores son capaces de aumentar sus ventas al poder ofrecer productos adicionales de la cartera completa de seguridad, como por ejemplo: seguridad de internet, seguridad de hogar conectado, VPN, gestión de claves y mucho más.

En la unión europea el mercado de protección de la identidad está en pleno auge, por lo cual, éste es el momento propicio para que los proveedores de servicios saquen al mercado sus propias ofertas. F-Secure les proporciona una nueva línea de ingresos, la oportunidad de aumentar el ARPU, el cual incluye el canal adecuado, con procesos, servicios y herramientas de apoyo para para lograr el mayor éxito posible.

Pero, por sobre todo, es la expertise en inteligencia humana la que hace de F-Secure ID Protection la forma más eficaz de protección y con el mayor beneficio para los clientes de los proveedores. Tanto para reacionar en caso de que informaciones confidenciales se vean afectadas, como además para evitar que lleguen a correr peligro.

Nadie más cuenta con los vastos conocimientos sobre ataques cibernéticos que posee F-Secure. Durante las últimas tres décadas F-Secure ha liderado las innovaciones en seguridad cibernética, defendiendo decenas de miles de oficinas, hogares y millones de personas. F-Secure protege a las empresas y a los rconsumidores contra todo tipo de peligros, desde ciberataques avanzados, filtraciones de información, hasta el complejo malware de rescate. Los productos de F-Secure, basados en la inteligencia artificial, también ayudan a proteger los dispositivos electrónicos inteligentes y a los hogares conectados de sus clientes.

La combinación única de tecnología de punta y de servicios a la más alta calidad cubren todo el ciclo de vida de las operaciones del cliente, lo que convierte a F-Secure en un acierto para el canal de proveedores de servicios. Los productos de F-Secure son vendidos en todo el mundo por más de 200 proveedores de servicios y miles de partners.

www.f-secure.com/identity-protection

F-Secure