Ocultos a plena vista
Cisco Talos está trabajando continuamente para garantizar que nuestra inteligencia de amenazas no solo explique los ataques más recientes, sino también las nuevas versiones de amenazas antiguas, como el spam.

- Cisco Talos está trabajando continuamente para garantizar que nuestra inteligencia de amenazas no solo explique los ataques más recientes, sino también las nuevas versiones de amenazas antiguas, como el spam.

READ FULL ARTICLE

Ocultos a plena vista

Back

Ghassan Dreibi
Cisco Latinoamérica
Director de Seguridad
April 09, 2019

Cisco Talos está trabajando continuamente para garantizar que nuestra inteligencia de amenazas no solo explique los ataques más recientes, sino también las nuevas versiones de amenazas antiguas, como el spam. Esto a menudo significa perseguir a los delincuentes cibernéticos a dondequiera que se congregan. Sin embargo, en lugar de manejar y tratar con servidores ocultos en alguna misteriosa dirección de la misteriosa web, un número sorprendentemente grande de cibercriminales cibernéticos prefieren operar directamente a través de las redes sociales. Por ejemplo, Facebook es el hogar de docenas de grupos que sirven como mercados en línea e intercambios de ciberdelincuentes. Talos vio el spam de los servicios anunciados en estos grupos de Facebook en nuestros propios datos de telemetría, lo que indica un impacto potencial para los clientes de Cisco de estos grupos.

Durante los últimos meses, Cisco Talos ha rastreado a varios grupos en Facebook en los que frecuentemente se realizan actividades sospechosas (en el mejor de los casos) e ilegales (en el peor de los casos). La mayoría de estos grupos usan nombres de grupo bastante obvios, como "Spam Professional", "Spammer & Hacker Professional", "Compre Cvv en esta tienda. PAGO POR BTC ” y "Facebook hack (Phishing)". A pesar de los nombres bastante obvios, algunos de estos grupos han logrado permanecer en Facebook por hasta 8 años, y en el proceso han adquirido decenas de miles de miembros.

En total, Talos ha compilado una lista de 74 grupos en Facebook cuyos miembros prometieron llevar a cabo una serie de cuestionables acciones cibernéticas, incluida la venta y el intercambio de información robada de tarjetas de crédito/bancos, el robo y la venta de credenciales de cuenta de una variedad de sitios, y herramientas y servicios de correo no deseado. En total, estos grupos tenían aproximadamente 385.000 miembros.

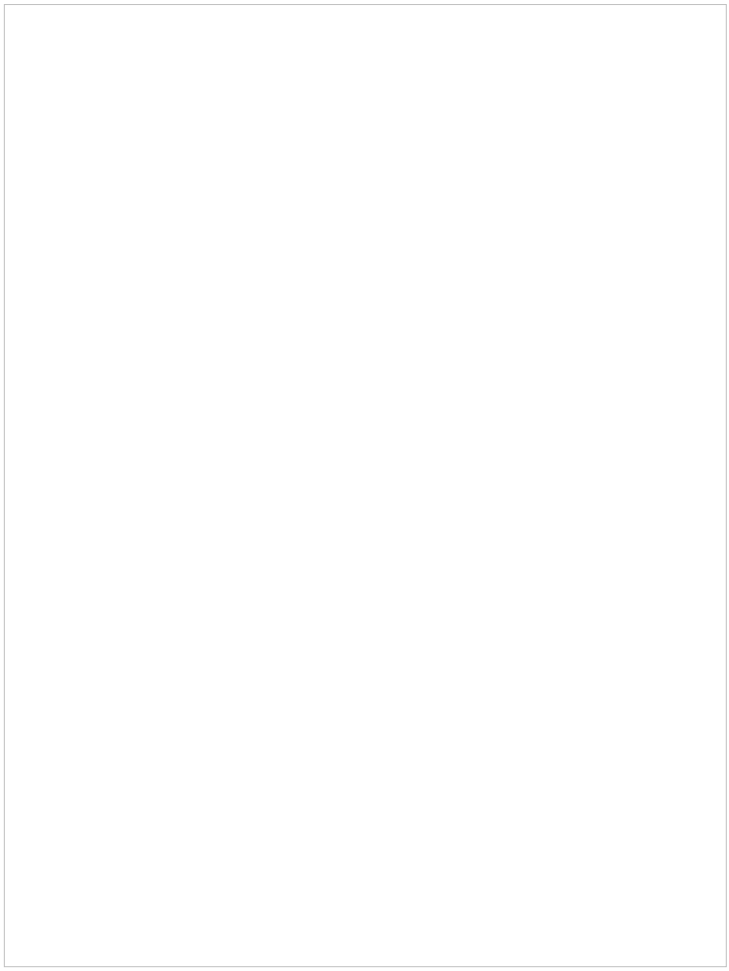
Estos grupos de Facebook son fáciles de identificar para cualquier persona que posea una cuenta en esta red social. Una búsqueda simple de grupos que contengan palabras clave como "spam", "carding" o "CVV" generalmente arrojará múltiples resultados. Por supuesto, una vez que uno o más de estos grupos se han unido, los propios algoritmos de Facebook a menudo sugieren grupos similares, lo que hace que sea más fácil encontrar nuevos lugares de reunión de delincuentes. Facebook parece depender de los usuarios para informar a estos grupos de actividades ilegales e ilícitas para frenar cualquier abuso.

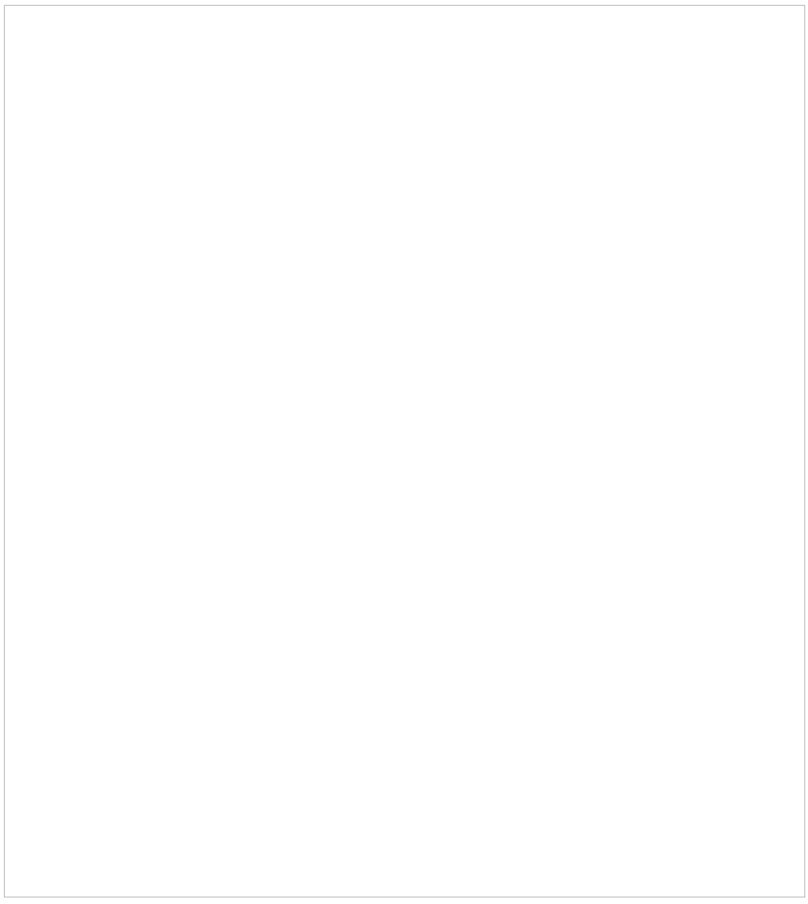
Inicialmente, Talos intentó eliminar a estos grupos individualmente a través de la funcionalidad de informes de abuso de Facebook. Si bien algunos grupos se eliminaron de inmediato, en otros grupos solo se eliminaron las publicaciones individuales. Finalmente, a través del contacto con el equipo de seguridad de Facebook, la mayoría de los grupos malintencionados fueron eliminados rápidamente, aunque nuevos grupos siguen apareciendo y algunos todavía están activos a partir de la fecha de publicación. Talos continúa cooperando con Facebook para identificar y eliminar la mayor cantidad posible de estos grupos.

Este no es un problema nuevo para Facebook. En abril de 2018, el reportero de seguridad Brian Krebs alertó al sitio de redes sociales para que docenas de grupos de Facebook en los que los piratas informáticos ofrecían de forma rutinaria una variedad de servicios, que incluían el robo de información de tarjetas de crédito, el fraude electrónico, el fraude de devolución de impuestos y los ataques de denegación de servicio distribuido (DDoS). Meses después, aunque los grupos específicos identificados por Krebs habían sido deshabilitados permanentemente, Talos descubrió un nuevo conjunto de grupos, algunos con nombres muy similares, si no idénticos, a los grupos informados por Krebs.

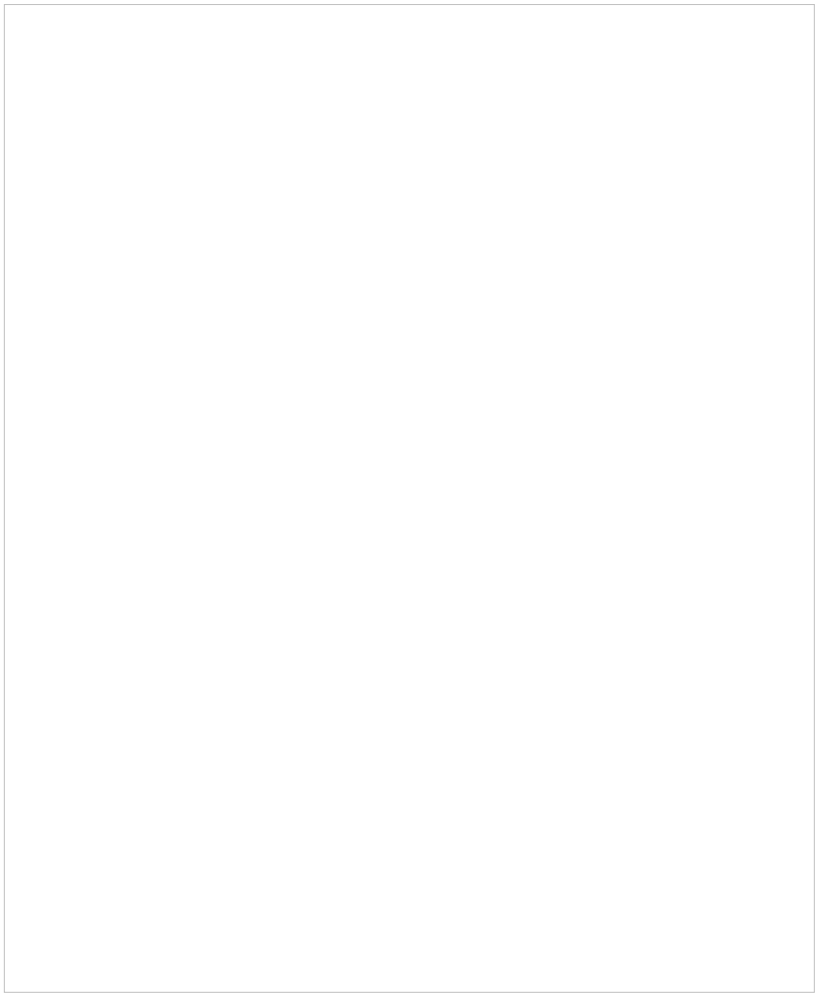
Dentro del mercado de pulgas criminal en línea

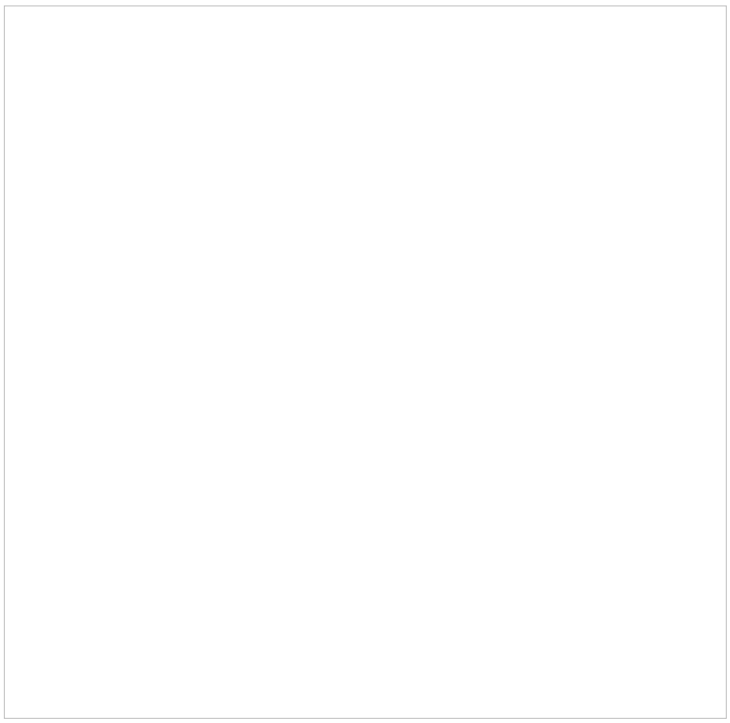
Muchas de las actividades en estas páginas son totalmente ilegales. Por ejemplo, descubrimos varias publicaciones en las que los usuarios vendían números de tarjetas de crédito y los CVV que los acompañaban, a veces con documentos de identificación o fotos pertenecientes a las víctimas.

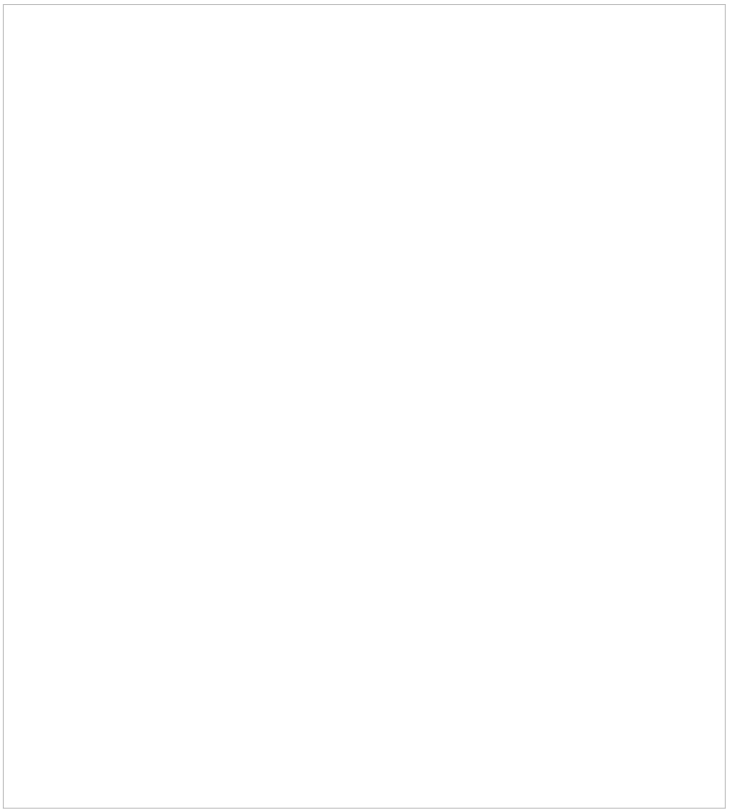




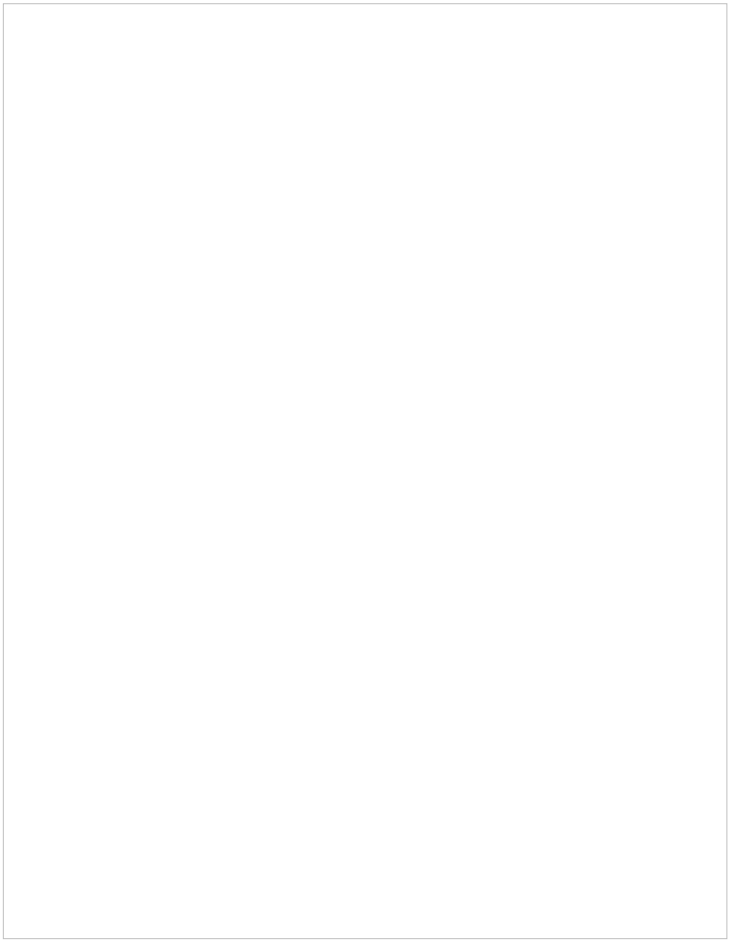
También se promocionaron otros productos y servicios. Vimos spammers que ofrecían acceso a grandes listas de correo electrónico, delincuentes que ofrecían asistencia para mover grandes cantidades de efectivo y ventas de cuentas ficticias en varias organizaciones, incluido el gobierno.







Incluso vimos a los usuarios ofrecer la capacidad de falsificar/editar documentos de identificación.



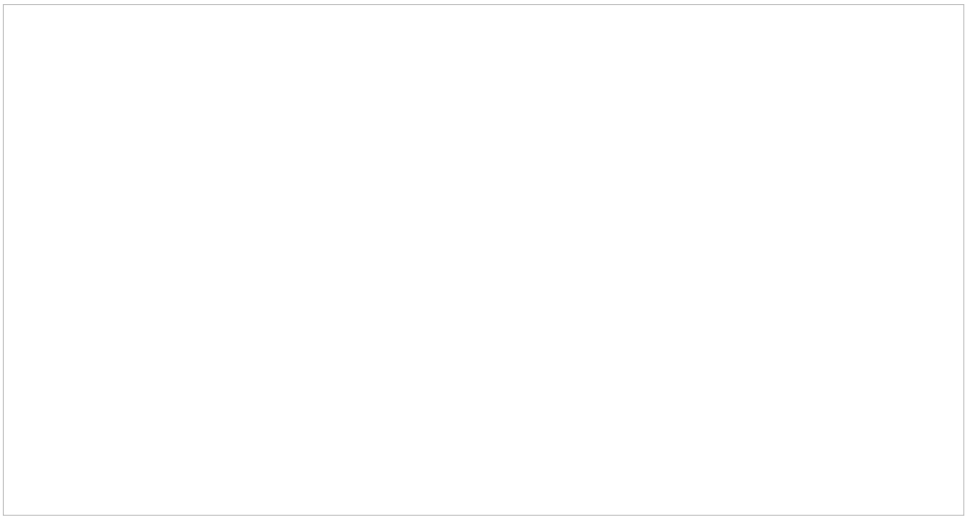
En la mayoría de las ocasiones, estos vendedores solicitaron el pago en forma de criptomonedas. Otros emplean el uso de los llamados

"intermediarios" que actúan como puente entre el comprador y el vendedor de la información y obtienen un recorte de las ganancias. Estos usuarios generalmente promovían el uso de cuentas de PayPal para completar la transacción.

No está claro, según estos grupos, qué tan exitosos o legítimos son algunos de los usuarios. A menudo hay quejas publicadas por miembros del grupo que han sido estafados por otros miembros del grupo. En la mayoría de los grupos, hay una etiqueta y una forma particulares a las publicaciones. Normalmente los vendedores describirán lo que tienen frente a lo que quieren. Casi todas las transacciones son "usted primero" (escrito como "U_f", "uf", por sus siglas en inglés), lo que significa que la persona interesada en realizar la compra u operación tiene que pagar o proporcionar su servicio o producto por adelantado. Como muchos otros grupos de Facebook, estos montones de estafadores también existen como foros para que los delincuentes compartan chistes sobre algunas de sus campañas menos exitosas.

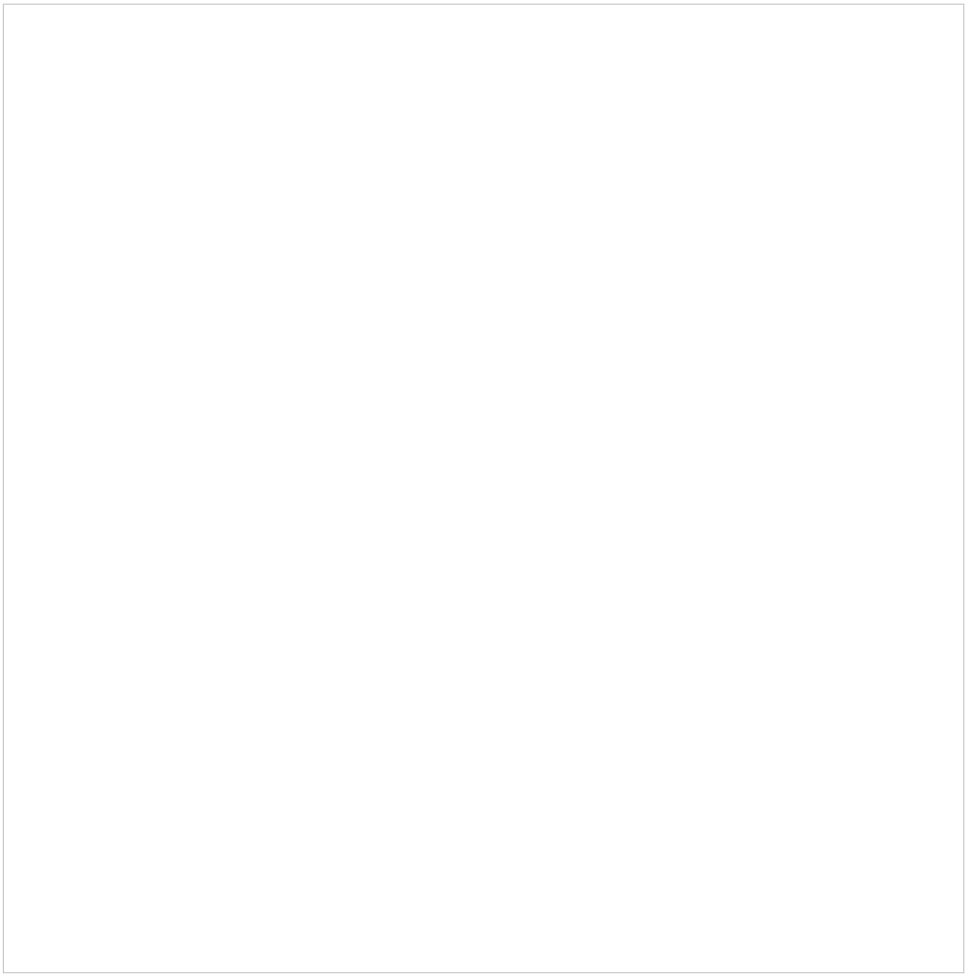
Estafadores en la naturaleza

Una cosa es segura, a pesar de que algunos miembros del grupo solo parecen estar dispuestos a estafar a otros miembros, otros están en libertad cometiendo crímenes que aparecen en los datos de Talos. A continuación encontrarán como ejemplo una publicación de uno de los grupos de Facebook que Talos estaba monitoreando. En la publicación, el spammer está anunciando servicios de spamming, que prometen llevar su phish con el tema de Apple a la carpeta de la bandeja de entrada de Hotmail y Yahoo. Ellos incluyeron una captura de pantalla que muestra el spam que recibieron en su bandeja de entrada.



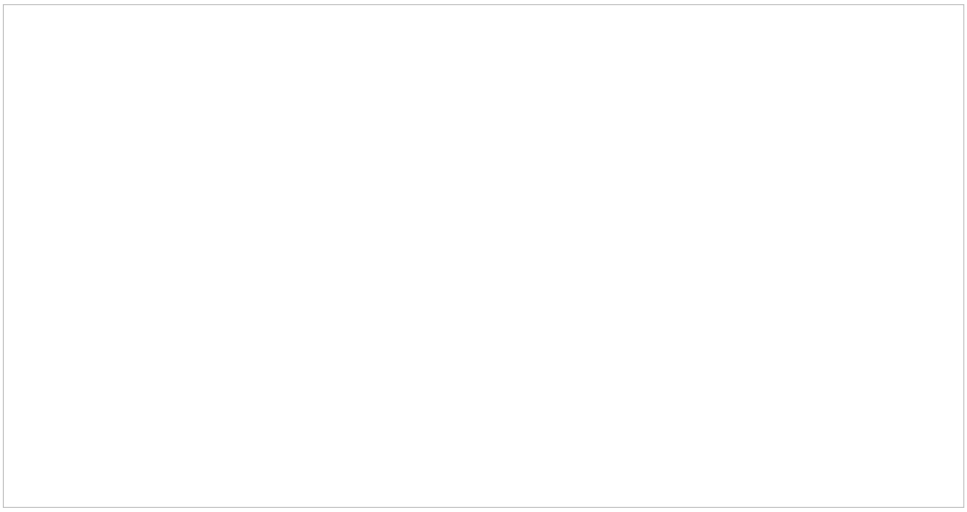
Talos pudo localizar ejemplos de este mismo phish en nuestros datos de telemetría. Basados en las muestras de correo electrónico que Talos recuperó para su análisis, los atacantes habían adjuntado un archivo PDF que decía ser una factura por una compra en Apple. El PDF incluye

enlaces para ver o cancelar su pedido.

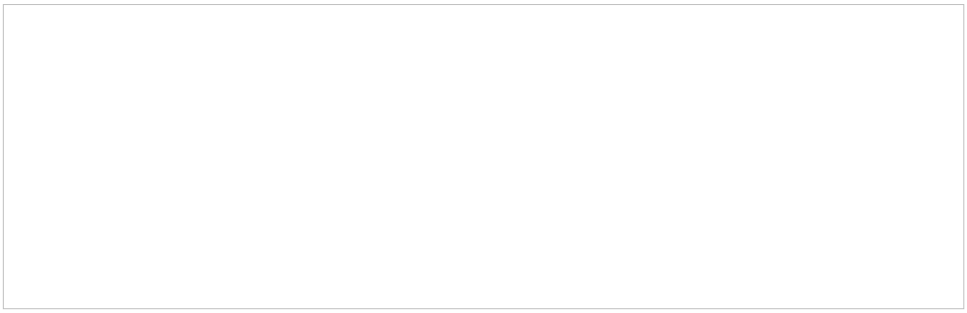


Un análisis dentro de la zona de pruebas de malware de ThreatGrid indica que cuando el usuario selecciona ver o cancelar el pedido, el enlace dirige a la víctima a un sitio web de phishing ubicado en un dominio registrado recientemente: appleid[.]Apple.com.verifysecureinfomanage.info

El sitio web de suplantación de identidad (phishing) en sí mismo se creó con "16Shop", un infame kit de suplantación de identidad que se conoce que está dirigido a usuarios de Apple.



La investigación de Cisco Umbrella indica que la dirección IP utilizada para alojar el dominio de phishing, también alberga muchos otros nombres de dominio de apariencia sospechosa, que probablemente se hayan utilizado para estafas similares en el pasado.



Este no es el único ejemplo en nuestros datos que encontramos con respecto a este tipo de actividad ilícita, que fueron seguidas por publicaciones en grupos de Facebook que venden las mismas herramientas, técnicas o servicios utilizados por el estafador. Algunos miembros del grupo, de hecho, cumplen con su palabra cuando se trata de cometer este tipo de delitos en línea.

Conclusión

Las redes sociales han proporcionado herramientas que permiten a personas de todo el mundo reunirse y compartir ideas. Esta es una de las características definitorias de las redes sociales. Sin embargo, los algoritmos informáticos subyacentes que nos ayudan a conectarnos, lo que sugiere nuevos amigos o redes, no son lo suficientemente inteligentes para distinguir las actividades benignas de las no éticas o totalmente ilegales.

Hasta ahora, al parecer, Facebook se ha basado en las comunidades para controlar las amenazas, con lo cual, por razones obvias, estas comunidades delictivas se muestran reticentes. Como consecuencia de esto, un número considerable de estafadores cibernéticos han continuado proliferando y beneficiándose de actividades ilegales. Operando con impunidad, estos atacantes sondean implacablemente las ciber-defensas de empresas en todo el mundo. Este es un esfuerzo de alto riesgo porque un atacante con incluso el punto de apoyo más pequeño dentro de una organización puede causar un daño considerable.

Para combatir a estos adversarios motivados, tenemos que trabajar juntos. Las plataformas de medios sociales deben continuar sus esfuerzos, tanto manuales como automatizados, dirigidos a identificar y eliminar grupos maliciosos. Los equipos de seguridad y los proveedores deben trabajar en equipo para compartir activamente la información, tomar medidas e informar a nuestros clientes. Las empresas deben ser diligentes en cuanto a su protección y esfuerzos de higiene cibernética. Y, por último, los consumidores deben estar lo más informados y escépticos posible. Ataques como el spam atacan al individuo como punto de entrada.

Nota: Si los usuarios se encuentran con grupos maliciosos en Facebook, pueden denunciar a través de la pestaña de "informe" de Facebook, que se encuentra en la parte superior de la página del grupo en el menú desplegable debajo del botón "... Más".

-
-
-
-
-

Cancel

- All Contents
- Filtered
- Social
- My Library
- Notifications

  11

- Follow