La verdad sobre la ingeniería social

Deje atrás las ideas erróneas

Cuanto más sepa sobre sus empleados, sus vulnerabilidades y privilegios, así como sobre quienes desean hacerles daño, mejor podrá mantener a raya los ataques de ingeniería social. Sin embargo, a medida que nosotros mejoramos nuestras herramientas para identificar las amenazas potenciales, los ciberdelincuentes perfeccionan sus métodos y se comportan de forma imprevisible.

Para ayudarle a ir siempre un paso por delante, le presentamos las últimas tendencias, comportamientos e ideas erróneas sobre los ciberdelincuentes y sus métodos de ataque.

Idea errónea n.º 1

Los ciberdelincuentes prefieren los ataques súbitos

La realidad:

Antes de lanzar un ataque, los ciberdelincuentes normalmente dedican tiempo a investigar y a ganarse la confianza de la víctima.

TA453

El grupo TA453, un atacante vinculado con Irán, suele utilizar conversaciones legítimas en sus campañas para solicitar información a sus objetivos.

TA406

TA406, un grupo relacionado con el régimen norcoreano, intenta recopilar credenciales y otros datos de las víctimas antes de enviar enlaces o adjuntos maliciosos.

TA499

El grupo TA499, respaldado por el Estado ruso, envió mensajes de correo electrónico aparentemente inofensivos para obtener información de personas destacadas antes de iniciar sus ataques.

Idea errónea n.º 2

Los servicios legítimos, como Google y Microsoft, pueden utilizarse sin riesgo

La realidad:

Los ciberdelincuentes se aprovechan con regularidad de los servicios legítimos para recopilar credenciales, así como para alojar y distribuir malware.

14 %

El 14 % de todas las campañas maliciosas observadas utilizan servicios legítimos.

Las URL relacionadas con Google son las más empleadas con fines maliciosos…

Pero las URL relacionadas con Microsoft generan el doble de clics que las alojadas por Google.

Idea errónea n.º 3

Los ciberdelincuentes se limitan al correo electrónico

La realidad:

La inteligencia sobre amenazas de Proofpoint, líder del sector, ha identificado un número creciente de ataques basados en mensajes de correo electrónico que remiten a un centro de llamadas (TOAD).

250 000

Proofpoint ha observado más de 250 000 ataques TOAD al día.

Los mensajes de correo electrónico TOAD no contienen enlaces ni adjuntos, sino que incitan a las víctimas a llamar a un centro de llamadas falso.

50 000 USD

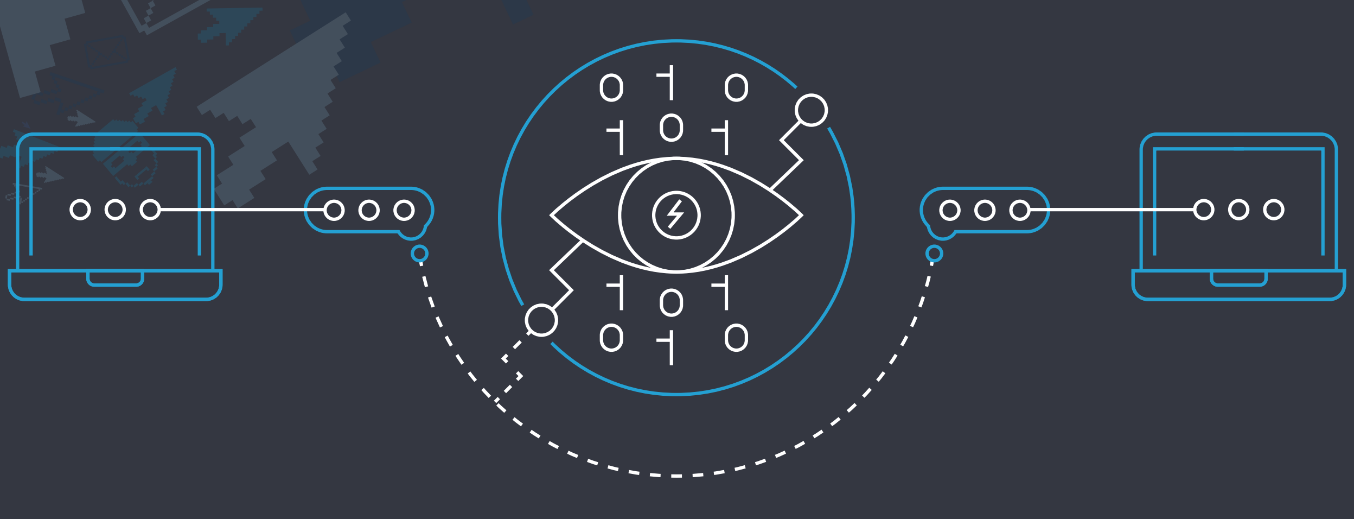
En un caso, una víctima perdió casi 50 000 dólares en un ataque TOAD.

Idea errónea n.º 4

Los hilos de conversaciones internas son seguros

La realidad:

El secuestro de conversaciones o hilos es una técnica popular entre numerosos atacantes de gran volumen con motivaciones económicas.



500

Proofpoint ha observado más de 500 campañas basadas en el secuestro de hilos de discusión.

16

…que distribuyen 16 familias de malware diferentes…

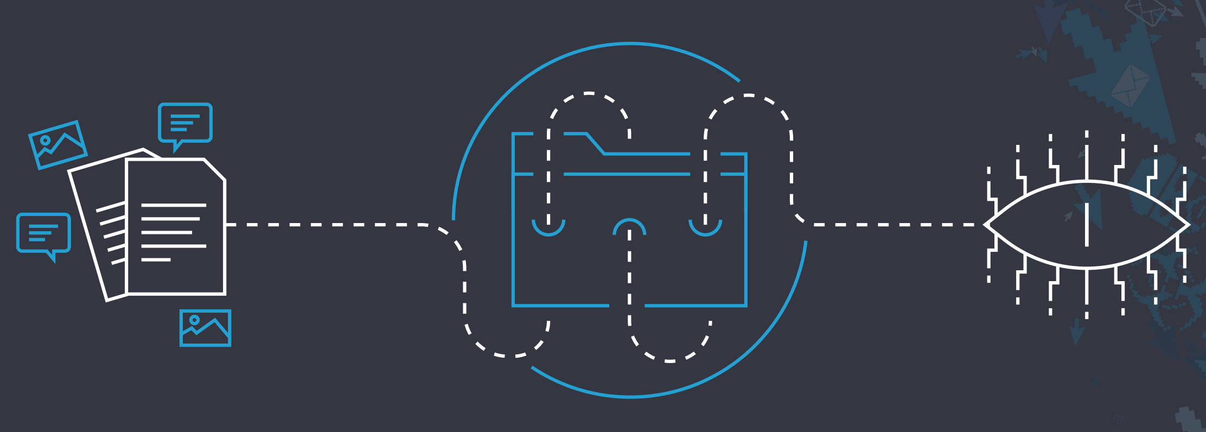
…incluidas Qbot, Emotet, IcedID y Racoon Stealer.

Idea errónea n.º 5

Los ciberdelincuentes solo utilizan contenido estándar de carácter comercial

La realidad:

Los ciberdelincuentes sacan partido de los acontecimientos actuales, las noticias, la cultura popular y de cualquier otra cosa que les permita incitar a sus víctimas a interaccionar con el contenido malicioso.



En 2021, Proofpoint observó cientos de millones de timos relacionados con la COVID-19 al mes.

Las estafas vinculadas con temas fiscales son uno de los fraudes favoritos de los ciberdelincuentes, que ofrecen descuentos a cambio de una amplia variedad de datos confidenciales.

Entre otros señuelos observados figuran el Día de San Valentín, el Juego del calamar, la guerra en Ucrania y la ayuda para los refugiados.

Más información

proofpoint | Threat Research

2022 Social Engineering Report

JUNE 2022

Descargar el informe de Proofpoint sobre ingeniería social

Otros recursos

LEER EL BLOG

Descubra las tácticas de ingeniería social más extrañas utilizadas el año pasado en este artículo del blog de los investigadores de amenazas de Proofpoint.

OÍR EL PODCAST

Ingeniería social: cómo manipulan a sus víctimas los ciberdelincuentes. En este podcast, Proofpoint explica cómo explotan los ciberdelincuentes el factor humano para atacarnos.

PONERSE EN CONTACTO →

Programe una reunión con Proofpoint para averiguar cómo podemos proteger su organización. Pregúntenos sobre nuestras evaluaciones de riesgo gratuitas.

Para obtener más información, visite proofpoint.com/es

PROTEGIENDO A LAS PERSONAS. PROTEGIENDO LOS DATOS.

Los ciberdelincuentes saben que los usuarios son la forma más fácil de entrar en su organización. Defiéndalos. Protéjalos. Empodérelos con Proofpoint. Cada día protegemos a más empleados de las empresas Fortune 500 y Global 2000 que ningún otro proveedor del mercado.

Analizamos...

Más de 2600 millones **de mensajes de correo**

Más de 49 000 millones **de URL**

Más de 1900 millones **de adjuntos**

Más de 28,2 millones **de cuentas cloud**

Más de 1700 millones **de mensajes de móvil**

...cada día