

# EL FACTOR HUMANO 2016



## 1. LAS PERSONAS ESTÁN REEMPLAZANDO A LAS VULNERABILIDADES AUTOMATIZADAS COMO TÁCTICA DE ACCESO PREFERIDA POR LOS ATACANTES

Un incontestable 99,7 % de los documentos usados en campañas basadas en adjuntos utilizaron ingeniería social y macros. Al mismo tiempo, el 98 % de las URL en mensajes malintencionados dirigen a malware alojado, bien como un ejecutable, bien como un ejecutable dentro de un archivo.

## 2. LAS CAMPAÑAS DEL TROYANO BANCARIO DRIDEX FUERON EL VECTOR DE ATAQUE QUE COLOCÓ A MÁS PERSONAS EN LA CADENA DE INFECCIÓN

Los troyanos bancarios son el tipo más habitual de carga dañina de adjuntos de documentos malintencionados, responsables del 74 % de todas las cargas dañinas. El volumen de correos electrónicos basados en Dridex fue casi 10 veces mayor que la siguiente carga dañina más usada en dichos ataques. Los atacantes usan ingeniería social e imitan procesos habituales como facturas y extractos con el fin de engañar al usuario para que haga clic en los mensajes de su correo electrónico.

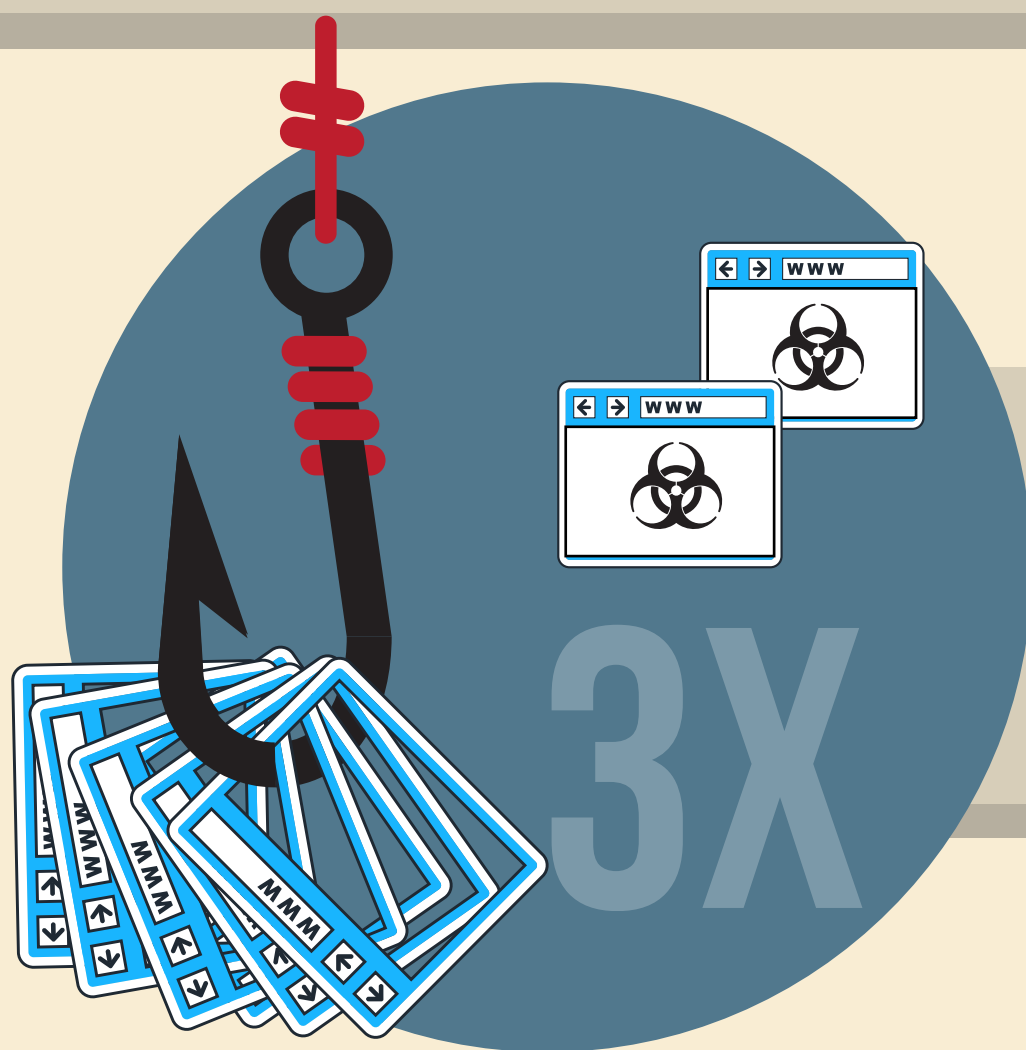


## 3. LOS ATACANTES PROGRAMARON LAS CAMPAÑAS DE CORREO ELECTRÓNICO Y REDES SOCIALES PARA AJUSTARLAS A LAS HORAS CON MÁS ACTIVIDAD DE USUARIOS

Al cambiar de las vulnerabilidades de malware a los clics humanos, los atacantes optimizaron las horas de actividad de la campaña para que coincidieran con las horas en las que hacen clic los usuarios. Los mensajes de correo electrónico se entregan al comienzo de la jornada laboral (9-10 a.m.) en las regiones objetivo. Del mismo modo, las horas de publicación de spam en las redes sociales coinciden con las horas de mayor uso legítimo de las redes sociales.

## 4. LOS USUARIOS SE DESCARGARON VOLUNTARIAMENTE MÁS DE 2000 MILLONES DE APLICACIONES MÓVILES QUE ROBARON SUS DATOS PERSONALES

Los atacantes usaron amenazas de redes sociales y aplicaciones móviles, no solo correo electrónico, para engañar a los usuarios y hacer que infectaran sus propios sistemas. Uno de cada cinco clics en URL malintencionadas se produjeron fuera de la red, muchos de ellos en redes sociales y dispositivos móviles. Estos clics fuera de la red ya no son casos aislados: son amenazas reales. Realizamos un análisis de las tiendas de aplicaciones de Android y descubrimos más de 12.000 dispositivos móviles malintencionados (capaces de robar información, crear puertas traseras y otras funciones) que lograron más de 2000 millones de descargas.



## 5. EL NÚMERO DE URL QUE ENLAZAN A PÁGINAS DE PHISHING DE CREDENCIALES FUE CASI 3 VECES SUPERIOR AL DE ENLACES A PÁGINAS QUE ALBERGAN MALWARE

Hemos observado que, de media, el 74 % de las URL usadas en campañas de phishing enlazaban a páginas de phishing de credenciales, en lugar de a sitios que albergan malware.

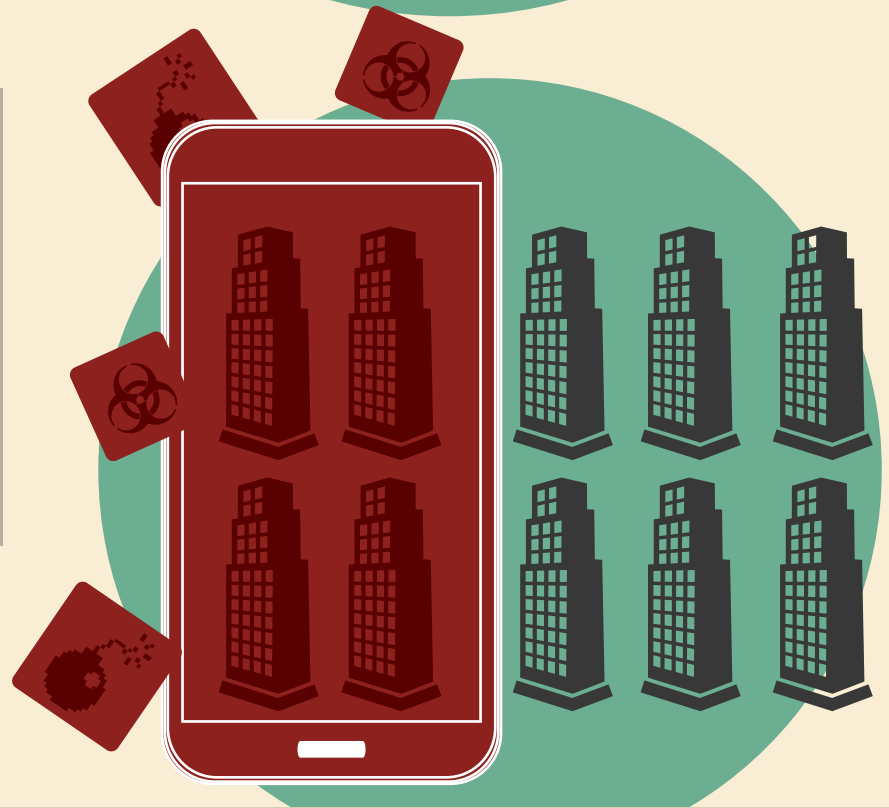
## 6. LAS CUENTAS USADAS PARA COMPARTIR ARCHIVOS E IMÁGENES, TALES COMO GOOGLE DRIVE, ADOBE Y DROPBOX, SON LAS TRAMPAS MÁS EFICACES PARA EL ROBO DE CREDENCIALES

Los enlaces de Google Drive son los señuelos de phishing de credenciales en los que más se hace clic. A través de estas marcas pueden engañar a los usuarios para que hagan clic, especialmente si el mensaje que recibe la víctima procede de un contacto de su lista.



## 7. EL PHISHING ES 10 VECES MÁS HABITUAL QUE EL MALWARE EN LAS PUBLICACIONES EN LAS REDES SOCIALES

Crear una cuenta falsa de una marca conocida en las redes sociales es muy sencillo, y por eso la mayoría de ataques que utilizan las redes sociales se decantan por el phishing.



## 8. LAS APLICACIONES MÓVILES PELIGROSAS DE TIENDAS NO AUTORIZADAS AFECTAN A 2 DE CADA 5 EMPRESAS

Estas aplicaciones pueden robar información personal, contraseñas y datos. De las grandes empresas analizadas con Proofpoint TAP Mobile Defense, aproximadamente el 40 % tenía aplicaciones malintencionadas de tiendas DarkSideLoader, es decir, tiendas de aplicaciones no autorizadas.

## 9. CAMPAÑAS A PEQUEÑA ESCALA QUE ENVÍAN CORREOS ELECTRÓNICOS ESPECÍFICAMENTE A UNA O DOS PERSONAS DENTRO DE UNA ORGANIZACIÓN PARA QUE TRANSFERIRAN FONDOS A LOS ATACANTES

Para llevar a cabo estas estafas, también llamadas "phishing de transferencias" o "phishing para CEO", los atacantes tienen que realizar una investigación a fondo. Estos correos electrónicos han falsificado los remitentes, de modo que parezcan enviados por CEO, CFO u otros cargos ejecutivos; rara vez incluyen enlaces o adjuntos, y suelen incluir instrucciones urgentes para que el destinatario transfiera fondos a una cuenta indicada.

