Correo electrónico: pulse con precaución

Cómo protegerse contra el phishing, el fraude y otras estafas

cisco

Contenido

Introducción 3

Remitente vs. destinatario 3

Implicaciones para las empresas 3

Respuesta necesaria 4

Panorama actual del e-mail y el phishing 6

Ataques de correo electrónico más comunes 7

Phishing en Office 365 7

Sabotaje del correo electrónico profesional 8

Extorsión digital 9

Spam de paquetes y facturas 10

Estafa de pago por adelantado 11

Malware en el correo electrónico 12

Infraestructura de envío de e-mails 13

Botnets 13

Toolkits para el envío masivo de mensajes de correo electrónico 14

El fraude como método 15

Cómo protegerse de los ataques de correo electrónico 17

Signos que indican la presencia de un correo electrónico fraudulent 17

Estrategias de prevención de ataque 19

Esté preparado 20

Cómo proteger su correo electrónico 21

Cómo puede ayudarle Cisco 23

Acerca de Cisco Cybersecurity Series 25

Introducción

El año pasado, el spam cumplió 40 años. Sí, en 1978, Gary Thuerk, director de marketing de Digital Equipment Corporation, envió el primer mensaje de spam a 393 personas a través de la ARPANET original para comercializar un nuevo producto. No es de extrañar que este mensaje fuera tan bien recibido como lo es gran parte del spam actual. Thuerk recibió una dura reprimenda y fue advertido para que no lo volviera a hacer.

Ojala fuera tan sencillo hoy en día Transcurridos 40 años, la prevalencia del spam ha crecido exponencialmente, inundando nuestras bandejas de entrada con ofertas no deseadas de productos farmacéuticos y dietéticos y oportunidades de trabajo. Pero ahí no queda la cosa: se le han sumado unos primos mucho más peligrosos: la suplantación de identidad (phishing) y el software malicioso (malware). El primero nació hace más de 30 años, y el segundo también tiene un historial de varias décadas en la distribución de correo electrónico. Hoy por hoy, lo triste es que muchos de los mensajes de correo electrónico son spam y cosas peores. El volumen es asombroso. En abril de 2019, se enviaron 41 678 millones de mensajes de correo electrónico desde España como spam, y en todo el mundo, el 85% de todo el correo electrónico en abril de 2019 fue spam, según Talos Intelligence. El volumen de correo electrónico no deseado también está en aumento: el spam alcanzó su máximo nivel de los últimos 15 meses en abril.

El Instituto Español de Ciberseguridad, Incibe, también informo' de que ya en mayo de 2019 se realizaron cuatros campañas de phishing en España suplantando a empresas Españolas.

Remitente vs. destinatario

Se podría aducir que el correo electrónico está estructurado en un formato casi ideal para los estafadores: obliga al usuario a leer y evaluar lo que recibe y luego tomar decisiones sobre lo que abre o en lo que pulsa. Solo con la cantidad adecuada de ingeniería social, explotando la buena naturaleza de las personas, es posible empujar al usuario a la acción.

Es esta ingeniería social la que no solo lo convierte en un atractivo vector de envío, sino también en todo un reto para protegerlo sistemáticamente. Rara vez, o nunca, un ataque transmitido por correo electrónico sortea al usuario. Si bien son comunes las URL que llevan a sitios web afectados o maliciosos y usan exploit kits, siguen dependiendo de la coerción del usuario para pulsar primero en el enlace de un e-mail

Implicaciones para las empresas

No es de extrañar que el correo electrónico sea uno de los principales desafíos que mantienen en vela a los responsables de seguridad informática (CISO). En nuestro informe anual Estudio comparativo sobre CISO (CISO Benchmark Study), descubrimos que el 55% de los CISO españoles encuestados consideran que defenderse de los comportamientos de los usuarios, como pulsar sobre un enlace malicioso en un e-mail, es muy o extremadamente desafiante. Esta preocupación es la mayor, por encima de cualquier otro problema de seguridad analizado, como los datos en la nube pública y el uso de dispositivos móviles.

La frecuencia de estos intentos de ataque también llama la atención de los CISO. De hecho, España tiene el porcentaje más alto de Europa de incidentes de seguridad

como resultado de la apertura de mensajes no deseados maliciosos en el seno de la empresa: el 54% frente a la media europea del 41%. Si comparamos España con el resto de países analizados por el Estudio comparativo sobre CISO, es el segundo país con más spam malicioso justo por detrás de México (61%). El 37% de los CISO españoles se enfrentaron a un incidente similar como resultado del robo de datos por medio de un ataque de phishing, dato acorde con la media global del 36%. Según datos del citado Estudio, los CISO de España consideran que las amenazas al correo electrónico son el riesgo de seguridad número uno para sus empresas.

En un estudio aparte encargado por Cisco a ESG en 2018, el 70% de los encuestados refirió que cada vez es más difícil protegerse de las amenazas del correo electrónico. En cuanto a las consecuencias de los ataques por correo electrónico, el 75% de los encuestados refirió impactos operativos significativos y el 47%, impactos económicos significativos.

Respuesta necesaria

¿Cómo proteger algo que es a la vez una necesidad y un riesgo? Para muchas empresas, el salto a la nube ha sido visto como una solución. Sin embargo, la nube no es una fórmula mágica contra los peligros del correo electrónico. En la mayoría de los casos, no hace sino postergar el problema. Los problemas de seguridad no desaparecen, más bien persisten.

Existen varias formas de minimizar el impacto general de las amenazas de correo electrónico. En este documento, analizaremos el panorama actual de las amenazas, proporcionando una visión general de los tipos de ataque más comunes en la actualidad. Explicaremos cómo se materializan, sus objetivos y la infraestructura subyacente. Discutiremos lo que puede hacer para proteger su negocio y cómo identificar las amenazas transmitidas por correo electrónico cuando llegan a sus usuarios.

"Gracias a la tecnología de seguridad de Cisco, 29 millones de mensajes de correo electrónico maliciosos han sido detenidos en el último año, incluidos ataques de ransomware, phishing y otros."

Maria de la Peña, Directora de Tecnología Aplicada de Ibermutuamur

“Las empresas necesitan encontrar el equilibrio entre la seguridad y el riesgo empresarial, y la experiencia del usuario. Una vez que se alcanza ese equilibrio, se necesita un programa que aplique la defensa con una respuesta activa para cuando las cosas vayan mal. El error humano es una realidad y hoy en día hay una industria de ciberdelincuencia multimillonaria que apuesta por él. Debe prever ese error y ser capaz de responder rápidamente cuando ocurra. Cada día nos topamos con intentos fructíferos de sortear nuestras defensas de seguridad debido a errores humanos o malhechores especializados que apuntan a nuestros activos o a vulnerabilidades del software; y cada día confirmamos que nuestra detección y respuesta activas están detectando y conteniendo esos ataques. Así es como sé que tenemos un programa de seguridad totalmente funcional.”

Steve Martino, SVP y CISO, Cisco

Panorama actual del e-mail y el phishing

Los riesgos presentados por correo electrónico son numerosos. De acuerdo con el informe de Verizon 2018 Data Breach Investigation Report, al que Cisco contribuyó, el correo electrónico es el vector número uno tanto para la distribución de malware (92,4%) como para la suplantación de identidad (96%). Interactúe con correo electrónico indebido y podría ser víctima de criptominería, sufrir un robo de credenciales o, en caso de caer en una estafa de ingeniería social inoportuna, perder grandes sumas de dinero. Escale esto a nivel empresarial, y un mensaje de correo electrónico inoportuno puede causar estragos.

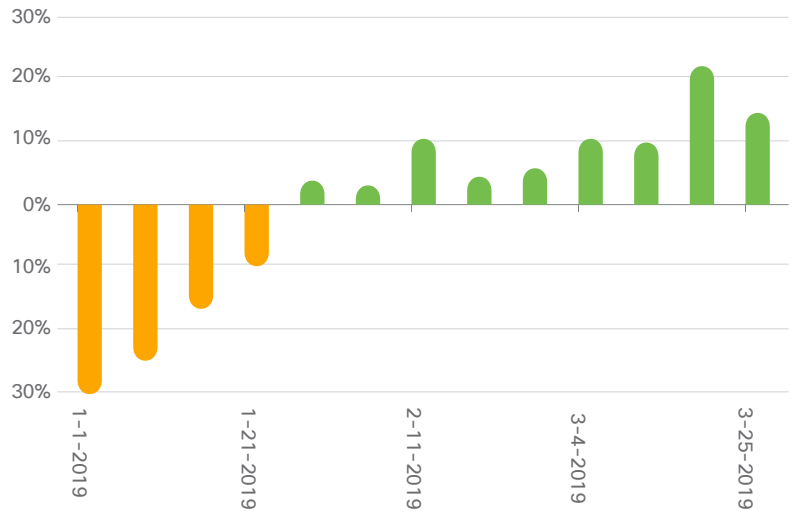
Duo Insight

¿Con qué frecuencia caen los usuarios en las estafas de correo electrónico? Pregúntele a la gente de Duo Security. Hace unos años, el equipo creó la herramienta gratuita Duo Insight, que permite a los usuarios crear sus propias campañas falsas de suplantación de identidad y ponerlas a prueba en el seno de sus propias empresas para ver quién «pica» y quién no.

Desafortunadamente, muchas personas lo hacen. Según The 2017 Duo Trusted Access Report, el 62% de las campañas de simulación de phishing que se ejecutaron consiguieron sustraer al menos un juego de credenciales de usuario. De todos los destinatarios, casi una cuarta parte de ellos pulsó en el enlace de suplantación de identidad del mensaje de correo electrónico. Y la mitad de ellos introdujo sus credenciales en el sitio web falso.

Con este nivel de éxito, no es de extrañar que el correo electrónico sea una opción tan popular para lanzar campañas de phishing. De hecho, parece que la actividad de suplantación de identidad podría estar aumentando, si es que el número de nuevos dominios de phishing identificados por Cisco Umbrella sirve de indicio. Tomamos un promedio semanal para el primer trimestre de 2019 y luego comparamos cada semana con este promedio. Los resultados de la Figura 1 muestran que, si bien el año comenzó con calma, el número de nuevos dominios producidos se fue acelerando, registrando un aumento del 64% desde la primera semana del trimestre hasta la última. Lo siguiente es un resumen de las estafas por correo electrónico más comunes hoy en día. Tome su portátil, abra su bandeja de entrada e imagine que le esperan los siguientes mensajes no leídos.

Figura 1 Dominios de phishing nuevos cada semana comparado con la media semanal del primer trimestre.



Fuente: Cisco Umbrella

Ataques de correo electrónico más comunes

Se han observado ataques similares de suplantación de identidad contra otros servicios de correo electrónico basados en la nube, como Gmail y G Suite.

Suplantación de identidad en Office 365

El mensaje de correo electrónico parece provenir de Microsoft. Dice que se suspenderá su dirección de correo electrónico de Office 365 por errores o infracciones de la política. La única manera de evitar que esto suceda es verificando la dirección pulsando en el enlace proporcionado.

Se trata de un intento de usurpar sus credenciales de Office 365. Los mensajes de correo electrónico y las URL utilizadas pueden incluso tener un aspecto similar al de Office 365, por ejemplo: micros0ftsupport@hotmail.com. Si pulsa sobre el enlace, le llevará a una página de inicio de sesión de aspecto oficial en la que se le solicitará su dirección de correo electrónico y su contraseña.

Sin embargo, el sitio es falso. Una vez que los estafadores tengan sus credenciales, podrán intentar iniciar sesión en otros servicios relacionados con Microsoft, así como hacerse con sus contactos.

Una técnica común es iniciar sesión en su cuenta de correoelectrónico y enviar a sus contactos un mensaje de correo electrónico informal (por ejemplo, Asunto: FYI) que incluya otra URL de suplantación de identidad.

Este tipo de ataque va en aumento. De acuerdo con los datos publicados por nuestros socios de Agari en sus Tendencias de uso de identidades ficticias y fraude por correo electrónico en el 2T de 2019, el 27% de los ataques avanzados de correo electrónico se lanzan desde cuentas de correo electrónico saboteadas. Esto supone un aumento de siete puntos porcentuales con respecto al último trimestre de 2018, cuando el 20% de los ataques de suplantación de identidad procedían de direcciones de correo electrónico saboteadas.

Pero Office 365 no es el único en el punto de mira. Se han observado ataques similares de suplantación de identidad contra otros servicios de correo electrónico basados en la nube, como Gmail y G Suite, el servicio de correo electrónico en la nube de Google. Dada la prevalencia de las cuentas de Google y la forma en que se usan en Internet para acceder a distintos sitios web, no es de extrañar que los atacantes también hayan creado sitios de phishing en este entorno.

Figure 2 Sitio de phishing deliberadamente diseñado para que se parezca a la página de inicio de sesión de Microsoft.

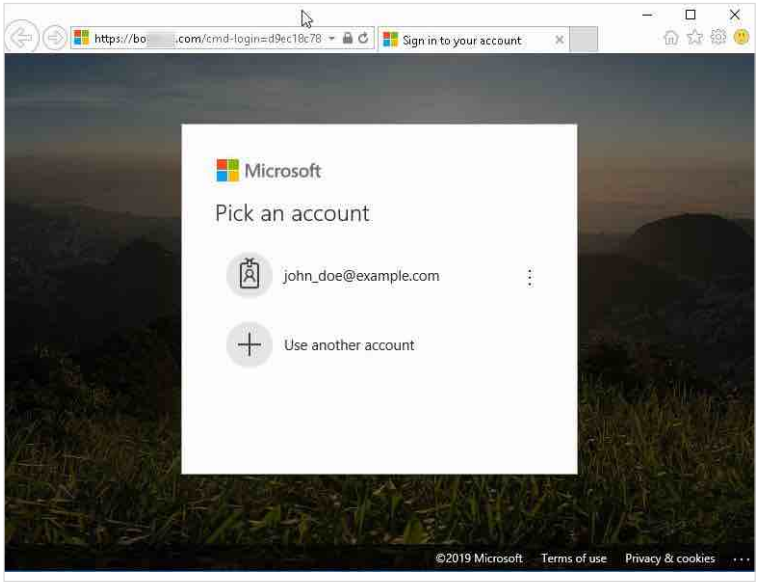
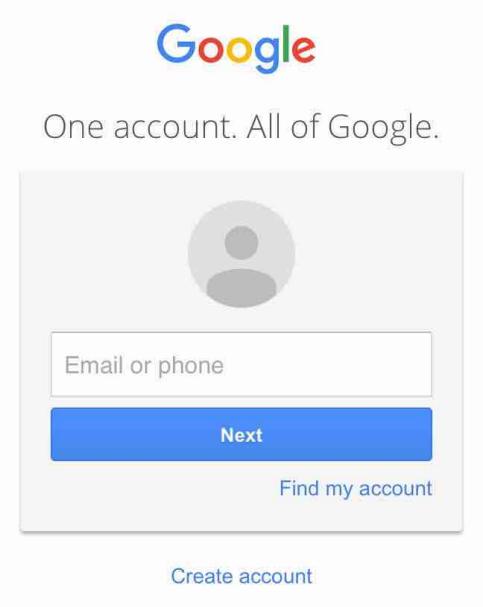


Figura 3 Ejemplo de inicio de sesión a una cuenta de Google. ¿Puede diferenciar la verdadera de la falsa?



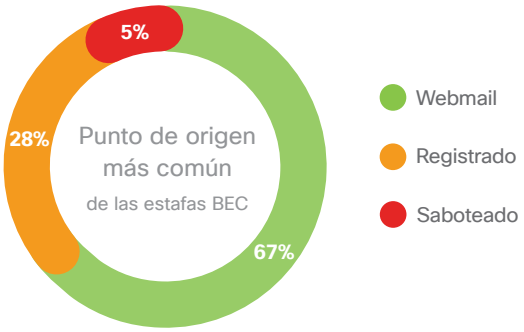
Sabotaje del correo electrónico profesional

Es la semana de la cumbre de las grandes empresas y todo el mundo está fuera de la oficina, excepto un pequeño número de personas encargadas de atender funciones críticas. Usted forma parte del equipo financiero y de la plantilla mínima que sigue en la oficina. De pronto, llega un mensaje de correo electrónico a su bandeja de entrada que parece provenir del Director Financiero, con el asunto «Falta de pago». En el mensaje se explica que no se ha atendido un pago que debía haber salido la semana pasada, lo que podría provocar una interrupción en la cadena de suministro de la empresa. Se adjuntan instrucciones para el pago por transferencia bancaria. El remitente termina diciendo que le llamará en el plazo de una hora para hablar del tema.

Se trata de un caso típico de ataque BEC (business email compromise, o sabotaje del correo electrónico profesional). Las estafas BEC son una forma de fraude por correo electrónico en la que el timador se hace pasar por un ejecutivo de nivel C o superior e intenta engañar al destinatario para que realice su función profesional, con un propósito ilegítimo, como enviarle dinero. En ocasiones, en efecto, llegan a llamar al destinatario y a hacerse pasar por el ejecutivo en cuestión. Y parece que funciona. Según el Internet Crime Complaint Center (IC3), en 2018 se produjeron pérdidas por valor de 1.300 millones de dólares como consecuencia de las estafas BEC.

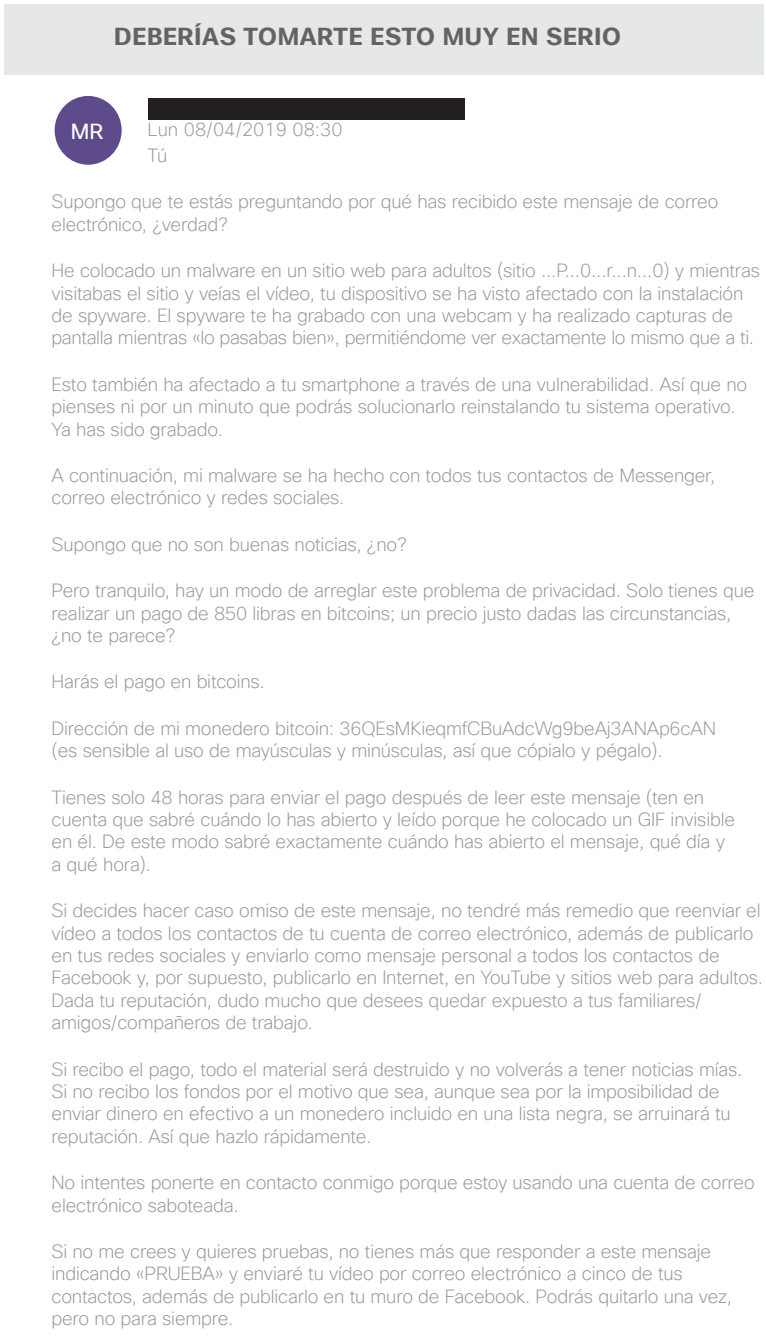
Se podría pensar que los timadores aprovecharían las cuentas saboteadas en las estafas BEC, como lo hacen con las estafas de suplantación de identidad de Office 365. Sorprendentemente, de acuerdo con el informe de Tendencias de uso de identidades ficticias y fraude por correo electrónico en el T2 de 2019, solo el 5% de estas estafas lo hacen. Dos terceras partes de estos ataques siguen utilizando cuentas de correo webmail gratuitas para lanzarlos, mientras que el 28% restante realiza ataques a medida utilizando dominios registrados. Este último nivel de personalización se extiende al cuerpo del mensaje de correo electrónico, donde, según Agari, uno de cada cinco mensajes BEC incluye el nombre del destinatario.

Figura 4 Punto de origen del correo BEC.



Fuente: Agari Data, Inc.

Figure 5 Ejemplo reciente de extorsión digital.



DEBERÍAS TOMARTE ESTO MUY EN SERIO

MR [redacted]
Lun 08/04/2019 08:30
Tú

Supongo que te estás preguntando por qué has recibido este mensaje de correo electrónico, ¿verdad?

He colocado un malware en un sitio web para adultos (sitio ...P...0...r...n...0) y mientras visitabas el sitio y veías el vídeo, tu dispositivo se ha visto afectado con la instalación de spyware. El spyware te ha grabado con una webcam y ha realizado capturas de pantalla mientras «lo pasabas bien», permitiéndome ver exactamente lo mismo que a ti.

Esto también ha afectado a tu smartphone a través de una vulnerabilidad. Así que no pienses ni por un minuto que podrás solucionarlo reinstalando tu sistema operativo. Ya has sido grabado.

A continuación, mi malware se ha hecho con todos tus contactos de Messenger, correo electrónico y redes sociales.

Supongo que no son buenas noticias, ¿no?

Pero tranquilo, hay un modo de arreglar este problema de privacidad. Solo tienes que realizar un pago de 850 libras en bitcoins; un precio justo dadas las circunstancias, ¿no te parece?

Harás el pago en bitcoins.

Dirección de mi monedero bitcoin: 36QEsMKieqmfCBuAdcWg9beAj3ANAp6cAN (es sensible al uso de mayúsculas y minúsculas, así que cópialo y pégalo).

Tienes solo 48 horas para enviar el pago después de leer este mensaje (ten en cuenta que sabré cuándo lo has abierto y leído porque he colocado un GIF invisible en él. De este modo sabré exactamente cuándo has abierto el mensaje, qué día y a qué hora).

Si decides hacer caso omiso de este mensaje, no tendré más remedio que reenviar el vídeo a todos los contactos de tu cuenta de correo electrónico, además de publicarlo en tus redes sociales y enviarlo como mensaje personal a todos los contactos de Facebook y, por supuesto, publicarlo en Internet, en YouTube y sitios web para adultos. Dada tu reputación, dudo mucho que desees quedar expuesto a tus familiares/amigos/compañeros de trabajo.

Si recibo el pago, todo el material será destruido y no volverás a tener noticias mías. Si no recibo los fondos por el motivo que sea, aunque sea por la imposibilidad de enviar dinero en efectivo a un monedero incluido en una lista negra, se arruinará tu reputación. Así que hazlo rápidamente.

No intentes ponerte en contacto conmigo porque estoy usando una cuenta de correo electrónico saboteada.

Si no me crees y quieres pruebas, no tienes más que responder a este mensaje indicando «PRUEBA» y enviaré tu vídeo por correo electrónico a cinco de tus contactos, además de publicarlo en tu muro de Facebook. Podrás quitarlo una vez, pero no para siempre.

Extorsión digital

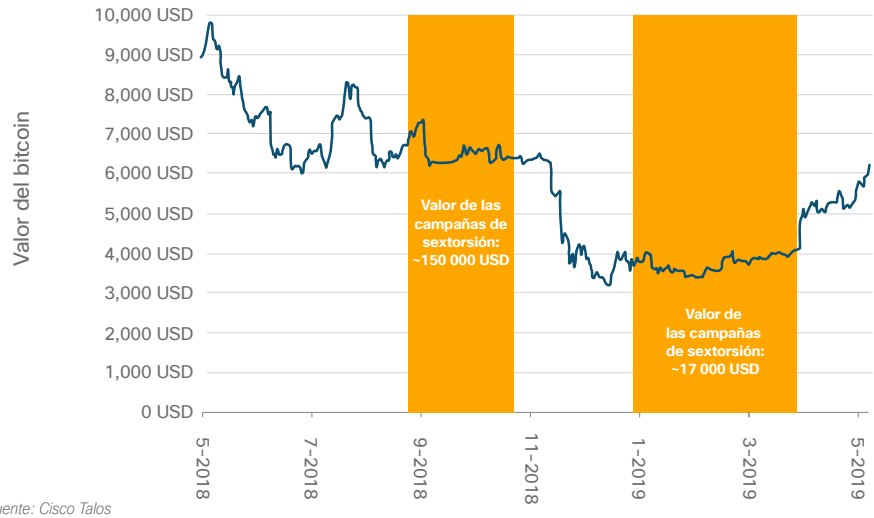
Llega un mensaje de correo electrónico a su bandeja de entrada con el asunto **«DEBERÍAS TOMARTE ESTO MUY EN SERIO»**.

El remitente del mensaje afirma haber saboteado un sitio web de vídeos para adultos y saber que usted ha visitado el sitio. También afirma haberle grabado con su webcam, junto con los vídeos que afirma que usted ha visto. Además, afirma haber accedido a sus contactos, a los que les enviará todo el material, a menos que le pague cientos, si no miles, de dólares en bitcoins.

Se trata de un caso de extorsión digital. Lo único que lo diferencia de los casos de extorsión más tradicionales es que las afirmaciones son totalmente inventadas. Los estafadores no han saboteado un sitio web, no le han grabado y no tienen su lista de contactos. Simplemente esperan engañarle para que crea que lo han hecho.

Tratamos muchas formas de este tipo de estafa en el artículo de nuestro blog, «Amenaza del Mes», La bolsa o la vida: extorsión digital.

Figure 6 Comparación del valor del bitcoin (USD) con los sobornos obtenidos de las campañas de sextorsión.



Fuente: Cisco Talos

Es un truco interesante y muy lucrativo para los timadores: los beneficios de una campaña de extorsión digital alcanzaron las seis cifras a finales de 2018. Sin embargo, de acuerdo con el último análisis realizado por Cisco Talos, que abarca el periodo comprendido entre enero y marzo de 2019, las ganancias han disminuido. Aun así, el aumento y la disminución de estos beneficios siguen de forma imprecisa el valor del bitcoin, aunque con mayores descensos. Como el valor del bitcoin está actualmente en alza, será interesante ver si ocurre lo mismo con los pagos de extorsión digital.

Spam de paquetes y facturas

«No recuerdo haber comprado una suscripción a esta aplicación móvil», se dice a sí mismo. Eso es al menos lo que dice el mensaje de correo electrónico: una suscripción de por vida a, digamos, un club de cine. Un momento, la ubicación que aparece en la factura dice que se contrató en Sri Lanka. Y ni siquiera vive en Sri Lanka. «Debe de haber algún error», se dice a sí mismo al abrir rápidamente el PDF adjunto para investigar el tema.

Desgraciadamente, ese PDF contenía un exploit que ha descargado Emotet a su dispositivo. La estafa varía, pero normalmente gira en torno a un paquete que no encargó, una factura por algo que no compró o un pago mensual por una suscripción o un servicio al que no se inscribió. Esto puede producir cualquier número de resultados maliciosos, desde el robo de credenciales bancarias hasta criptominería.

Figure 7 Correo electrónico con troyano bancario (Emotet), supuestamente procedente de UPS.

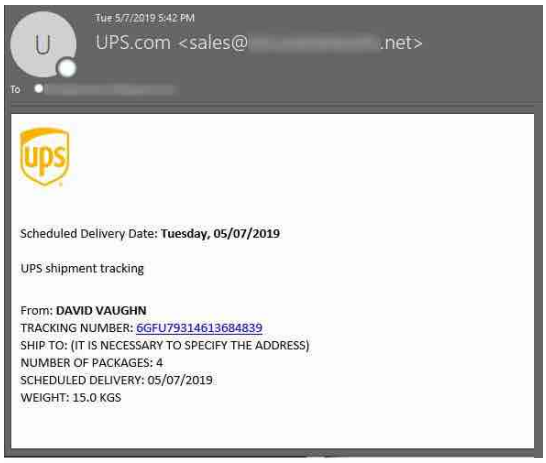


Figura 8 Ejemplo reciente de estafa de pago por adelantado.

D. Christoper A. Wray

CW

Director del FBI
Para: [redacted]
Responder a: [redacted]

Atn.: Beneficiario.

La ética profesional dicta que es muy importante presentarse en un primer contacto como este. Soy Christopher A. Wray, Director del FBI. Por medio de esta comunicación oficial, le informamos de que hemos descubierto que algunos funcionarios que trabajan para el gobierno de los Estados Unidos han intentado desviar sus fondos por canales ilícitos. De hecho, lo hemos descubierto hoy mismo a través de nuestros agentes secretos de la Unidad Disciplinaria del FBI, después de que detuviéramos a un sospechoso.

Este sospechoso fue detenido en el Aeropuerto Internacional de Dulles esta misma mañana temprano, cuando intentaba sacar de Estados Unidos la cuantiosa cantidad de dinero. De acuerdo con la ley estadounidense contra el blanqueo de capitales, no es posible sacar esa cantidad de efectivo de Estados Unidos porque sería un acto constitutivo de delito, punible con arreglo a dicha ley de 1982. Dicha ley es una ley globalizada aplicable en la mayoría de los países desarrollados con el fin de poner en jaque al terrorismo y al blanqueo de capitales.

Según la información recopilada en esta Unidad, hemos descubierto que los fondos en cuestión son realmente suyos, pero se han aplazado deliberadamente porque los funcionarios a cargo de su pago están envueltos en algún tipo de irregularidades que van totalmente en contra de la ética de cualquier entidad de pago. Actualmente, dichos fondos están bajo la custodia del Banco Pagador y puedo asegurarle que sus le serán liberados sin problemas, siempre y cuando sea sincero con nosotros en este asunto. Además, necesitamos su colaboración positiva a todos los niveles porque estamos siguiendo muy de cerca esta misma transacción para detectar las ovejas negras de nuestra sociedad actual.

Hoy, 9 de mayo de 2019, hemos dado instrucciones a la Dirección Ejecutiva del Banco Pagador para que le libere los fondos como su beneficiario acreditado, ya que disponemos de información/registros valiosos para acreditar que los fondos son efectivamente suyos. Sea como fuere, deberá proporcionarnos la siguiente información (a efectos de verificación oficial):

1. Nombre, segundo nombre y apellido.
2. Edad.
3. Ocupación.
4. Estado civil.
5. Número de teléfono directo/fax.
6. Domicilio particular.

Quedamos a la espera de que dé cumplimiento inmediato a esta obligación oficial, para que pueda ser pagado por un Banco Pagador autorizado.

Sello oficial.

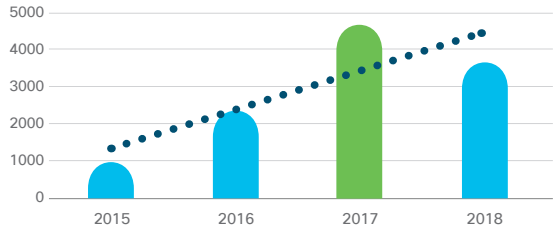
D. Christopher A. Wray
Director del FBI

Estafa de pago por adelantado

No todos los días recibe uno un mensaje de correo electrónico del FBI. ¡Y mucho menos uno en el que se le informe de una transferencia pendiente por valor de 10,5 millones de dólares! Lo único que tiene que hacer es responder al mensaje de correo electrónico y ellos le indicarán lo que tiene que hacer para recibir el pago.

Se trata de la clásica estafa de pago por adelantado. Como su nombre indica, los estafadores le pedirán un pago antes de enviarle la suma prometida, dinero que nunca aparecerá. También es una de las estafas por correo electrónico más antiguas, que ha adquirido diferentes formas a lo largo de los años, desde un príncipe extranjero que desea compartir su riqueza hasta la aprobación de préstamos a personas con malos antecedentes crediticios. Aun así, las estafas persisten y son miles las estafas de este tipo denunciadas cada año a la Better Business Bureau (BBB) estadounidense.

Figure 9 Estafas de pago por adelantado denunciadas a la BBB por año.
(Total de las categorías de Préstamo anticipado, Cambio de divisas/estafa nigeriana, Falso romance, Reparación de crédito/Alivio de la deuda, Inversión y Viajes/Vacaciones.)



Fuente: Better Business Bureau

Malware en el correo electrónico

Una buena parte del malware se sigue enviando por correo electrónico. Solía ser más prominente, cuando se adjuntaban archivos. exe directamente a los mensajes de correo electrónico. Pero cuando los usuarios se dieron cuenta de que abrir un ejecutable no era seguro, los malhechores cambiaron de táctica.

Hoy es mucho más probable que el malware se envíe indirectamente, en archivos adjuntos menos sospechosos, como documentos comerciales de uso común, o por URL incluidas en el cuerpo del mensaje, elementos todos ellos que suelen enviarse normalmente en comunicaciones electrónicas legítimas. La idea es burlar los análisis tradicionales del correo electrónico que identifican y ponen en cuarentena un archivo binario u otros adjuntos poco frecuentes.

Esto es más evidente si observamos los archivos adjuntos maliciosos detectados en lo que va de año (enero a abril de 2019). Los archivos binarios suponen menos del dos por ciento de todos los archivos adjuntos maliciosos: no son solo los archivos .exe, sino todos los binarios. Supone un gran cambio con respecto a años anteriores, cuando era habitual encontrar archivos ejecutables, Java y Flash. De hecho, el uso de Java y Flash ha disminuido tanto que si los sumamos a los binarios, seguirían representando el 1,99% de los archivos adjuntos.

Los archivos como los .zip constituyen casi una tercera parte de los archivos adjuntos maliciosos, y cuatro de los diez tipos principales de archivos utilizados por los atacantes.

Tabla 1 Tipos de archivos adjuntos maliciosos.

Tipo	Porcentaje
Oficina	42.8%
Archivo	31.2%
Script	14.1%
PDF	9.9%
Binario	1.77%
Java	0.22%
Flash	0.0003%

Fuente: Talos Intelligence

Los tipos de archivos adjuntos más comunes son simplemente los que se envían a la oficina en un día normal: dos de cada cinco archivos maliciosos son documentos de Microsoft Office.

Entonces, ¿por qué tipo de archivos adjuntos optan ahora los atacantes? Los archivos como los .zip constituyen casi una tercera parte de los archivos adjuntos, y cuatro de los diez tipos principales de archivos. Los scripts como los archivos .js constituyen el 14,1%. Estos scripts han registrado un aumento espectacular desde la última vez que analizamos los tipos de archivos adjuntos en el Informe anual de ciberseguridad (ACR) de 2018, cuando los archivos .js, junto con los XML y HTML, constituían solamente el 1% de las extensiones de archivo maliciosas. Su frecuencia como archivos adjuntos maliciosos ha seguido creciendo, aumentando casi cinco puntos porcentuales desde el ACR de 2018. Arrojemos los PDF a la ecuación, y más de la mitad de todos los archivos adjuntos maliciosos son tipos de documentos que se utilizan con regularidad y que son omnipresentes en el lugar de trabajo moderno.

Tabla 2 10 extensiones maliciosas electrónico más habituales en el correo electrónico.

Extensión	Porcentaje
.doc	41.8%
.zip	26.3%
.js	14.0%
.pdf	9.9%
.rar	3.9%
.exe	1.7%
.docx	0.8%
.ace	0.5%
.gz	0.5%
.xlsx	0.2%

Fuente: Talos Intelligence

Infraestructura de envío de emails

Adentrémonos ahora entre bambalinas, lejos de los tipos de correo electrónico y las cargas explosivas, y echemos un vistazo a cómo se distribuyen los mensajes maliciosos. Los estafadores utilizan principalmente dos métodos para lanzar campañas de spam: botnets y toolkits para el envío masivo de mensajes de correo electrónico.

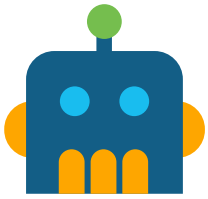
Botnets

Los botnets de spam son de lejos los principales responsables de la mayoría del spam que se envía hoy en día. Los siguientes son algunos de los actores clave del panorama de las botnets de spam.

Necurs

La botnet Necurs surgió por primera vez en 2012 y ha propagado una gran variedad de amenazas, desde Zeus hasta ransomware. Si bien su actividad recibió mucha más atención en el pasado, Necurs parece haber pasado a un segundo plano, al menos en términos de cobertura de prensa. Sin embargo, esta botnet sigue estando muy activa. De hecho, la botnet Necurs es el principal vehículo de distribución de una variedad de estafas, incluida la extorsión digital.

Para obtener más información acerca de Necurs, consulte el análisis Los muchos tentáculos de la botnet Necurs, realizado por Cisco Talos.



Emotet

Gran parte del spam enviado por Emotet se engloba en la categoría de paquetes y facturas. Emotet es un malware modular e incluye un plugin spambot.

Dado que aquellos tras Emotet ganan dinero usándolo como canal de distribución para otras amenazas, el objetivo de la mayoría del spam enviado por el módulo spambot es infectar más sistemas con Emotet, extendiendo aún más el alcance del canal de distribución maliciosa. Como Emotet roba contenido de los buzones de las víctimas, suele ser capaz de crear cadenas de mensajes maliciosos, pero de aspecto realista, que parecen formar parte de conversaciones reales. Emotet también es conocido por robar credenciales SMTP, apropiándose de los propios servidores de correo electrónico saliente de las víctimas como vehículo para el spam saliente.

Para obtener más información sobre Emotet, lea nuestro informe previo sobre amenazas de la Cybersecurity Report Series, Defiéndase contra actuales amenazas críticas.

> **"Cisco Email Security bloquea entre el 90 y el 95% de nuestros mensajes de correo electrónico por sus propiedades sospechosas o maliciosas."**
>
> **Diogo Rodrigues de Sousa, Especialista de redes, Caixa Seguradora**

Gamut

La botnet Gamut ha estado muy ocupada enviando spam de citas y relaciones íntimas, principalmente en torno a la premisa de conocer gente en su zona. En otras campañas, los responsables de la botnet envían mensajes pregonando productos farmacéuticos u oportunidades de empleo (véase la Figura 10). Han registrado una variedad de dominios, aunque la infraestructura en sí misma parece bastante sencilla, con múltiples subdominios bajo un dominio, que a menudo apuntan a una dirección IP. Si bien Cisco no ha confirmado si los servicios ofrecidos son legítimos, el proceso de registro parece intentar ocultar información personal.

Figura 10 Mensaje de spam enviado por la botnet Gamut.

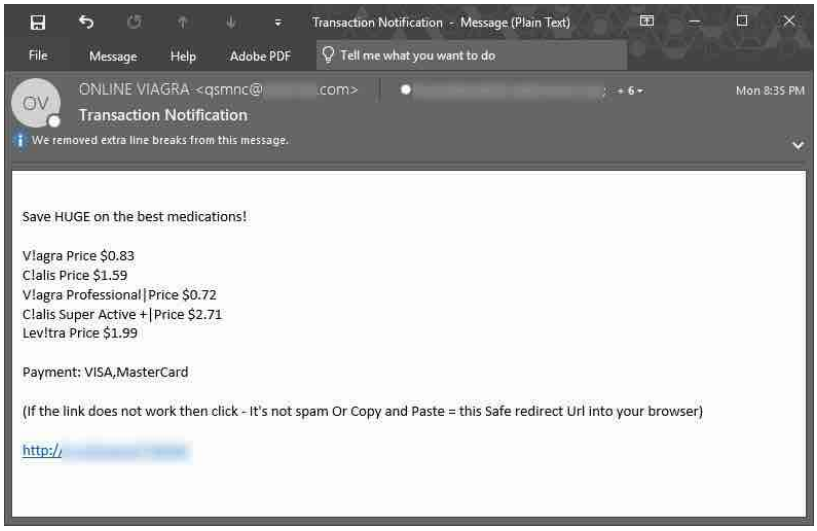
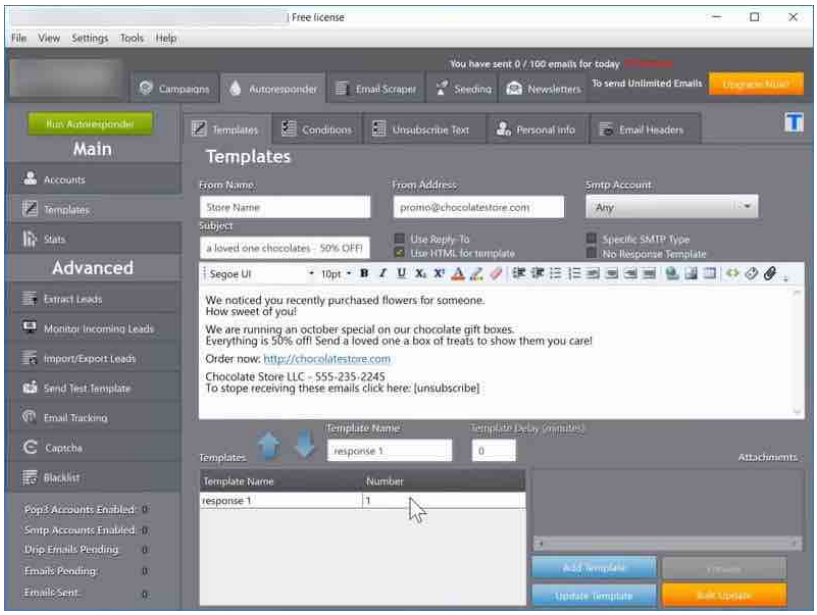


Figura 11 Ejemplo de un toolkit de spam.



Toolkits para el envío masivo de mensajes de correo electrónico

Un enfoque alternativo que muchos estafadores adoptan es la compra de toolkits para enviar un gran número de mensajes de correo electrónico. Muchas de estas herramientas son semilegítimas, lo que significa que si usted estuviera vendiendo sus propias cortinas de ducha hechas a mano y a medida, técnicamente podría utilizar uno de estos toolkits para aumentar la conciencia de marca a través del envío masivo de correo electrónico a su propia lista de mailing. Sin embargo, algunas de las funcionalidades de estos toolkits, como las que permiten la rotación de las direcciones IP de envío y la reconstrucción personalizada de archivos adjuntos con el fin de generar valores hash únicos, son mucho menos probables de ser utilizadas en tales escenarios.

Hace poco, ingenieros de Cisco Talos descubrieron grupos de Facebook en los que actores maliciosos vendían herramientas para el envío masivo de mensajes de correo electrónico junto con extensas listas de direcciones de correo electrónico, probablemente extraídas de filtraciones de datos. En este caso, los compradores de estas herramientas las estaban utilizando claramente con fines maliciosos.

El fraude como método

Si el correo electrónico es el vector más común, el fraude es el método más común, especialmente para el crimen organizado.

Si el correo electrónico es el vector más común, el fraude es el método más común, especialmente para el crimen organizado. Los malhechores ocultos tras las estafas BEC están tratando de estafar miles de dólares a las empresas. Los extorsionistas digitales están engañando fraudulentamente a los usuarios para que les paguen con bitcoins. Y en cuanto a la estafa de pago por adelantado, bueno, su propio nombre lo indica.

Nada de esto es nuevo. El correo electrónico es solo una de las últimas herramientas que los delincuentes han utilizado para cometer fraude. Históricamente, los delincuentes han aspirado siempre a aprovechar las oportunidades de maximizar los ingresos ilícitos que presenta cada generación tecnológica.

Si nos fijamos en las pérdidas registradas por la policía federal alemana (Bundeskriminalamt BKA) y el FBI, más del 80% de todas las pérdidas registradas por ciberdelincuencia pueden atribuirse a la persecución del fraude. Hay que hacer hincapié en el término «registradas», ya que puede haber pérdidas intangibles que son difíciles de cuantificar y registrar con precisión. Esto significa que las estadísticas registradas son bastante fiables.

Por lo tanto, afirmar que el fraude es la fuerza impulsora de las pérdidas por ciberdelincuencia es correcto. De hecho, al examinar dos métodos de fraude incluidos en las estadísticas del FBI, a saber, Business Email Compromise (BEC) y Email Account Compromise (EAC), vemos que las pérdidas en 2018 ascendieron a 1300 millones de dólares. A modo de comparación, las pérdidas equivalentes registradas por ransomware, una forma de ciberdelincuencia a menudo mencionada y analizada, fueron de 3,6 millones de dólares. Y el hecho es que todo indica que las pérdidas asociadas con el fraude no detectado seguirán creciendo, ya que las pérdidas asociadas con estafas BEC/EAC se incrementaron en un 78% solo entre 2016 y 2017.

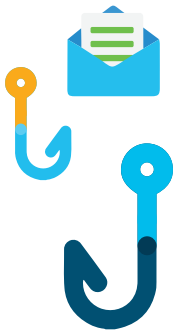
"Cisco Email Security ha sacado literalmente la seguridad del correo electrónico de la agenda de la dirección y nos ha permitido centrarnos en otras áreas. ¡Lo atrapa todo! ¡Es tranquilizador saber que hemos adoptado la decisión perfecta para la seguridad del correo electrónico!"

Steven Wujek, Arquitecto informático sénior de Technology Concepts & Design, Inc.

Para obtener más información sobre las pérdidas por fraude y ciberdelincuencia, consulte nuestra serie de blogs de Ciberdelincuencia y fraude.

“Adoptar un enfoque de seguridad holístico no es simplemente una cuestión de usar productos de seguridad o un imperativo empresarial. **Se trata de estudiar a las personas, los procesos y la tecnología en todo el negocio.** En Cisco, comenzamos con un enfoque centrado en las personas que pone el foco en el trabajador y el trabajo que realiza, que les ayuda a hacer su trabajo de forma segura. Una de las maneras en que lo hacemos es proporcionando a los trabajadores consejos prácticos para reconocer y denunciar mensajes de correo electrónico antes de pulsar en ellos.”

Steve Martino, SVP y CISO, Cisco



Cómo protegerse de los ataques de correo electrónico

Signos que indican la presencia de un correo electrónico fraudulento

El lado positivo cuando se trata de amenazas enviadas por correo electrónico es que por lo general hay anomalías que los identifican como tales, siempre que uno sepa en qué fijarse. Los siguientes

Para: usted@sudirección.com

1 De: Amazon Shipping <amz@123fnord.com>

Asunto: El suyo pedido

2 Hola:

Gracias por su pedido. Los detalles son los siguientes:

Compra: Suscripción de entrega mensual de comida para perro de la marca Puppy Food™

Coste mensual: 121 USD

Fecha y hora: Mei 03, 2019 10:21

Dirección IP: 254.189.234.159.01

País de compra: Guatemala

3 Si ya no desea estar suscrito, cancélelo inmediatamente siguiendo las instrucciones que aparecen en el anexo o introduciendo los datos de su tarjeta de crédito aquí:

4 5 http://badphishingsite.com/dontgothere.html

Atentamente,

Amazon Shipping

FILE

6 **dontopenthisis.bad**

Figura 12 Advertencia de Microsoft Office en relación con las macros en el documento abierto.

1. on algunos ejemplos. En la página siguiente se incluyen más detalles sobre cada uno de ellos.

2. **La dirección De:** ¿El nombre que aparece en la dirección De: no coincide con la dirección de correo electrónico?

3. **Numerosos errores ortográficos y gramaticales o logotipos borrosos.** Si el correo electrónico parece haber sido redactado de forma descuidada, puede que no sea legítimo.

4. **Carácter apremiante.** Si en un mensaje de correo electrónico se le pide que tome medidas inmediatas, si tiene un carácter apremiante o despierta su curiosidad: sospeche de él.

5. **Solicitud de información personal o sensible.** Nunca responda a un mensaje de correo electrónico no solicitado en el que se le pida información personal, financiera o confidencial.

6. **URL de apariencia ilegítima.** Muchas URL de correo electrónico fraudulento tienen un aspecto inusual, si se analizan, y no se debe pulsar sobre ellas. Si la URL está oculta en un enlace de texto, pase el puntero del ratón por encima y fíjese en la parte inferior de su navegador para examinarla. En caso de duda, no pulse.

7. **Tipo de archivo no reconocido.** Como parte de la mayoría de las competencias profesionales, solo deben enviarse unos pocos tipos de archivos por correo electrónico. Si el tipo de archivo parece extraño, no lo abra.

Además:

- **Más despacio.** De media, una persona pasa de 8 a 10 segundos examinando un mensaje de correo electrónico antes de adoptar medidas. Cálmese y busque las pistas que podrían indicarle la presencia de un intento de suplantación de identidad.
- **Si suena demasiado bueno para ser verdad, probablemente no lo sea.** ¿El mensaje de correo electrónico le ofrece millones de dólares? ¿Le amenaza con avergonzarle o lastimarle? Es probable que sea completamente falso.
- **Preste mucha atención a las señales de advertencia.** Si reconoce al remitente y abre un archivo adjunto, preste mucha atención a las advertencias sobre extensiones o macros que deban activarse (Figura 12). Rara vez son necesarias, si es que alguna vez lo son.

Estrategias de prevención de ataques

Existen varios enfoques que se pueden adoptar para reducir el riesgo que suponen las amenazas al correo electrónico.

Realice ejercicios regulares de suplantación de identidad. Sus empleados son su mayor medio de defensa contra la suplantación de identidad, especialmente contra los intentos más personalizados. Aquellos empleados que puedan aprender a reconocer un intento de suplantación de identidad pueden detener la fuente más importante de amenaza en los puntos finales.

Con el fin de aumentar la sensibilización, realice periódicamente ejercicios de phishing corporativo para probar y educar a sus usuarios. Emule las últimas técnicas del mundo real para mantener a las personas al tanto de lo que se pueden encontrar. Cisco sugiere realizar estos ejercicios con carácter mensual, comenzando por campañas de phishing fáciles de detectar y aumentando gradualmente la complejidad. Proporcione formación inmediata a aquellos usuarios que caigan en los ataques de phishing simulados (por ejemplo, envíeles una URL de prueba «maliciosa» que les dirija a más información sobre el phishing). Por lo que respecta a los usuarios de alto riesgo de su empresa, que podrían provocar daños significativos en caso de caer en la trampa, practique ejercicios personalizados de suplantación de identidad.

Utilice la autenticación multifactorial. En caso de que las credenciales de una cuenta de correo electrónico corporativa sean robadas con éxito, la autenticación multifactorial puede impedir que un atacante obtenga acceso a la cuenta y cause estragos.

La belleza de la autenticación multifactorial reside en su simplicidad. Supongamos que alguien se las arregla para obtener sus credenciales de inicio de sesión o las de alguien de su red e intenta iniciar sesión. Con la autenticación multifactorial, se envía automáticamente un mensaje a la persona propietaria de las credenciales para comprobar si acaba de intentar iniciar sesión. En esta situación, el usuario, al percatarse de que no lo ha hecho, rechaza la solicitud directamente. Esto frustrará el ataque con éxito.

Mantenga el software actualizado. En algunos casos, los mensajes de correo electrónico que incluyen URL maliciosas pueden dirigir a los usuarios a páginas con vulnerabilidades. Mantener actualizados los navegadores y el software, así como los plugins, ayuda a mitigar los riesgos que plantean estos ataques.

Nunca envíe dinero a un extraño. Esto se aplica a los fraudes de pago por adelantado y a los ataques BEC. Si tiene alguna sospecha acerca de una solicitud, no responda. En el caso concreto de las estafas BEC, establezca políticas estrictas que requieran la autorización de un alto cargo de la empresa para realizar transferencias y designe un firmante secundario.

Tenga cuidado con las solicitudes de inicio de sesión. Los malhechores, con la intención de robar las credenciales de inicio de sesión, hacen todo lo posible para que sus páginas se parezcan a las páginas de inicio de sesión con las que usted esté familiarizado. Si se encuentra con un aviso de inicio de sesión de este tipo, asegúrese de comprobar la URL para asegurarse de que proviene del sitio del propietario legítimo. Si se encuentra con una ventana de tipo emergente, expanda la ventana para asegurarse de que la URL completa, o al menos el dominio completo, sean visibles.

Asegúrese de que el mensaje de correo electrónico suene plausible. En el caso de las estafas como la extorsión digital y el fraude de pago anticipado, los remitentes suelen inventar historias muy complejas para tratar de convencerle de que el mensaje de correo electrónico es legítimo.

¿Tiene sentido la situación presentada? ¿Hay alguna laguna en la historia, desde un punto de vista técnico, perspectiva del proceso financiero u otros? En tal caso, aborde la cuestión con cierto escepticismo.

Esté preparado

Las amenazas de correo electrónico tienen muchas formas distintas de intentar engañarle o tentarle para que responda, pulse en una URL o abra archivos adjuntos. Esto justifica el uso del software de seguridad para correo electrónico que permite identificar y poner en cuarentena los mensajes maliciosos y filtrar el spam.

Afortunadamente, hemos descubierto que España no está siguiendo la tendencia global de disminución en el porcentaje de uso de seguridad para el correo electrónico. Según nuestro último Estudio comparativo sobre CISO, en España, el 47% de los encuestados utiliza actualmente seguridad para el correo electrónico como parte de sus mecanismos de defensa contra las amenazas. Se trata del mismo porcentaje que en 2014, mientras que a nivel mundial el porcentaje es del 41% y sigue bajando desde el 2014, cuando el 56% de las empresas la utilizaba.

Existen varias posibles razones para explicar este declive. Una causa podría ser el salto a la nube. En un estudio reciente realizado por ESG para Cisco, más del 80% de los encuestados refirió que sus empresas utilizaban servicios de correo electrónico en la nube. A medida que más empresas optan por tener sus servicios de correo electrónico alojados en la nube, los dispositivos in situ específicos de correo electrónico parecen menos necesarios, e incluso algunos equipos informáticos consideran que pueden prescindir de ellos.

Sin embargo, aunque muchos servicios de correo electrónico en la nube proporcionan funcionalidades de seguridad básicas, no podemos cansarnos de insistir en la necesidad de la protección multicapa. De hecho, en la misma encuesta realizada por ESG, el 43% de los encuestados descubrió que precisaban seguridad adicional para proteger su correo electrónico tras el cambio. En última instancia, los equipos de informática siguen teniendo necesidades válidas de establecer políticas, obtener visibilidad y control, utilizar entornos aislados (sandboxes) y aprovechar las capacidades externas de bloqueo. Otro problema al que se enfrentan actualmente los equipos de seguridad es el aumento de la superficie de ataque, lo que, naturalmente, da lugar a un mayor número de zonas en las que se necesita protección. Si los presupuestos de seguridad no se han mantenido a la par de este aumento, los equipos pueden verse obligados a reducir algunos recursos para cubrir esa mayor superficie de ataque.

Dado que el correo electrónico es el vector de amenaza más común, no se puede subestimar la importancia de protegerlo. Al realizar cualquier evaluación de riesgos cibernéticos, es importante priorizar los puntos de entrada más críticos con sistemas exhaustivos de defensa y gestión de riesgos e ir rebajando las exigencias en función de la probabilidad de ataque y el riesgo para la organización en caso de que se produzca una vulneración. A continuación, asignar recursos proporcionales a la importancia de las pérdidas potenciales.

Además, Gartner sugiere que los responsables de seguridad y riesgo (SRM por sus siglas en inglés) adopten un enfoque a tres vertientes para mejorar sus defensas contra los ataques de suplantación de identidad:

1. Actualizar la puerta de enlace segura del correo electrónico y otros controles para mejorar la protección contra la suplantación de identidad.
2. Integrar a los empleados en la solución y desarrollar capacidades para detectar ataques sospechosos y responder ante ellos.
3. Trabajar con los ejecutivos para desarrollar procedimientos operativos estándar para el manejo de datos sensibles y transacciones financieras.

Cómo proteger su correo electrónico

Hemos analizado los signos que indican la presencia de un correo electrónico fraudulento y las estrategias para la prevención de los ataques. A continuación, analizaremos las expectativas de la tecnología de seguridad del correo electrónico en 2019.

Igual que en el pasado, es vital tener un enfoque multicapa de la seguridad para proteger a su empresa de los ataques por correo electrónico. Hay varias funcionalidades de seguridad probadas y contrastadas que aún son importantes hoy en día.

Por ejemplo:

- Es preciso seguir protegiéndose contra el spam para mantener el correo electrónico no deseado y el spam malicioso lejos de las bandejas de entrada.
- La defensa contra las amenazas recibidas por correo electrónico como el malware y las capacidades de bloqueo de URL son vitales para bloquear el malware, la suplantación de identidad dirigida (spear phishing), el ransomware y la criptominería en los archivos adjuntos, junto con la inteligencia de URL para combatir los enlaces maliciosos en los mensajes de correo electrónico.
- El sandboxing integrado debería ejecutarse automáticamente en segundo plano para los nuevos archivos que lleguen al correo electrónico, para comprender rápidamente si son maliciosos.

Sin embargo, lo cierto es que el panorama de amenazas está en constante evolución, y los malhechores siempre andan buscando nuevas vías para atacar.

Estas son todas las funcionalidades presentes en la Solución de correo electrónico de Cisco.

Además de las probadas y comprobadas, las siguientes tecnologías de seguridad presentes en la AMP de Cisco para correo electrónico pueden ayudar a combatir este entorno en constante cambio:

- Han surgido protecciones más avanzadas contra la suplantación de identidad que utilizan el aprendizaje automático para comprender y autenticar las identidades de correo electrónico y las relaciones de comportamiento para bloquear los ataques avanzados de phishing.
- Las protecciones de dominio de DMARC ya pueden activarse para proteger la marca de una empresa impidiendo que los atacantes utilicen un dominio corporativo legítimo en sus campañas de suplantación de identidad.

- La función de cuarentena de mensajes es útil para retener un mensaje mientras se analiza un archivo adjunto antes de enviar el mensaje al destinatario, eliminar el archivo adjunto malicioso o eliminarlo por completo.
- La recuperación del correo electrónico ayuda si se identifica como malicioso un archivo tras su entrega al destinatario, lo que le permite dar marcha atrás y poner en cuarentena el mensaje que contiene el archivo adjunto malicioso desde un buzón de correo.
- Los feeds de amenazas externas al correo electrónico de STIX son muy usados actualmente por los productos de seguridad para correo electrónico, lo que resulta útil en caso de que una empresa desee consumir un feed de amenazas con enfoque vertical más allá de la inteligencia de amenazas nativa del propio producto.
- La integración de la seguridad del correo electrónico con carteras de seguridad más amplias también es cada vez más común para entender si el malware o los mensajes avanzados de un entorno pueden haber sido entregados a usuarios o bandejas de entrada concretos.

“Cisco es líder en seguridad del correo electrónico en el ámbito corporativo según el informe 2019 de The Forrester Wave, recibiendo las más altas calificaciones en cuanto a opciones de implantación, protección frente a ataques y autenticación, rendimiento y operaciones de correo electrónico (incluyendo escalabilidad y fiabilidad), y liderazgo en tecnología.”

The Forrester Wave™: Enterprise Email Security, T2 2019

Cómo puede ayudarle Cisco

¿Cómo proteger algo que es a la vez una necesidad y un riesgo?

Como se muestra en este informe, el correo electrónico es el vehículo de una amplia variedad de amenazas: el error humano más común de pulsar sobre un enlace inseguro, malware desconocido, ransomware o accesos no autorizados. Dada esta complejidad, lo que se necesita es un enfoque multicapa capaz de proteger a las empresas de los ataques por correo electrónico.

Por esta razón, Cisco creó una solución completa llamada Email sin preocupaciones para proporcionar una protección avanzada a su correo electrónico.

Email sin preocupaciones está compuesto por:

- La solución Cisco Email Security que actúa de forma integral para responder a las diferentes modalidades de amenazas que las empresas sufren a diario: defiende del phishing, protege de los programas malignos ocultos en los archivos adjuntos, hace inteligencia sobre URL amenazadores e identifica los ransomwares.
  Además, ofrece funciones avanzadas de prevención de la pérdida de datos y criptografía de los contenidos para proteger la información sensible, ayuda indispensable para garantizar la conformidad con las normativas estatales y del sector. malicioso o eliminarlo por completo.
- La solución AMP para el correo electrónico.

Advanced Malware Protection (AMP) desempeña diferentes funciones, entre las cuales:

1. Protege – De forma avanzada contra el phishing personalizado, los ransomwares y otros ataques sofisticados.

> **"La seguridad del correo electrónico es crucial para nuestra empresa. Es nuestro principal medio de comunicación, pero a menudo lo usan los atacantes para suplantar la identidad y robar información."**
>
> **Diogo Rodrigues de Sousa, Especialista en Redes, Caixa Seguradora**

2. Defiende – Nuestros expertos Cisco Talos analizan millones de muestras de programas malignos al día y se lo comunican a AMP, el cual relaciona archivos, datos de telemetría y comportamiento de los archivos para ayudar de manera proactiva a defenderse de las amenazas conocidas y emergentes.
3. Analiza – Cuando un archivo atraviesa la pasarela de correo electrónico, AMP continúa observando, analizando y registrando su actividad obteniendo análisis detallados sobre el comportamiento del archivo y sobre el nivel de amenaza para ayudar al equipo de seguridad a comprender, establecer las prioridades y bloquear los ataques.
4. Remedia – AMP monitoriza continuamente las amenazas. Si se detecta un comportamiento malévolo, la AMP envía un aviso retrospectivo para poder contener y corregir el programa maligno.
5. Unifica – AMP para Email Security puede integrarse con otros dispositivos AMP para interrumpir la amenaza en más vectores.

6. Controla – Cisco Threat Response (CTR) ofrece la integración automática entre diferentes productos de seguridad Cisco, entre ellos Email Security. El CTR sirve como base para investigaciones y respuestas veloces y eficientes a los incidentes. Añade las amenazas como Cisco Talos, en una única interfaz para optimizar la seguridad.

¿Cuál es el siguiente paso?

- Si desea saber cómo funciona Email sin preocupaciones y cómo puede ayudarlo a proteger su empresa, regístrese en el seminario web a pedido "Email sin preocupaciones".
- Si está listo para probar una demostración de correo electrónico sin preocupaciones, complete el formulario para solicitarlo.

"Aunque acabamos de empezar a utilizarlo, AMP parece una solución muy eficaz para detectar y bloquear los archivos dañinos en los mensajes de correo electrónico"

Diogo Rodrigues de Sousa, Especialista en Redes, Caixa Seguradora

Acerca de Cisco Cybersecurity Series

Durante la última década, Cisco ha publicado un rico acervo de información definitiva sobre seguridad e inteligencia de amenazas para profesionales de seguridad interesados en conocer el estado de la ciberseguridad global. Estos informes exhaustivos proporcionan informes detallados sobre el estado de las amenazas y sus consecuencias organizacionales, así como las mejores prácticas para protegerse de las consecuencias adversas de las filtraciones de datos.

En un esfuerzo por consolidar nuestro liderazgo de ideas, Cisco Security publica una serie de artículos basados en investigaciones y apoyados por datos, en la sección «Cisco Cybersecurity Series» (Serie de Ciberseguridad de Cisco). Hemos aumentado el número de títulos para incluir varios informes para profesionales de la seguridad con distintos intereses. Acudiendo a la experiencia de los innovadores e investigadores de las amenazas dentro de la industria de la seguridad, la recopilación de informes de la serie de 2019 incluye el Informe de referencia de Privacidad de Datos, el Informe de Amenazas y el Estudio comparativo sobre CISO, a los que se añadirán nuevos informes a lo largo del año.

Para obtener más información y acceder a todos los informes y copias archivadas, visite www.cisco.com/go/securityreports.

Oficinas centrales en América
Cisco Systems, Inc.
San José, CA

Sede central en Asia-Pacífico
Cisco Systems (USA), Pte. Ltd.
Singapur

Sede central en Europa
Cisco Systems International BV Amsterdam,
Países Bajos

Cisco cuenta con más de 200 oficinas en todo el mundo. Las direcciones y los números de teléfono y fax se encuentran en la web de Cisco en www.cisco.com/go/offices.

Publicado en junio de 2019 THRT_02_0519_r1