



Correo electrónico: haga clic con precaución

Cómo protegerse contra la suplantación de
identidad, el fraude y otras estafas

Contenido

Introducción	3
Remitente vs. destinatario	3
Lo que esto significa para los negocios	3
Respuesta requerida	4
El panorama actual del correo electrónico y la suplantación de identidad	6
Tipos de ataque de correo electrónico comunes	7
Suplantación de identidad de Office 365	7
Riesgo de correo electrónico comercial	8
Extorsión digital	9
Paquete y correo electrónico no deseado de facturación	10
Fraude de tarifa por adelantado	11
Malware en el correo electrónico	12
Infraestructura de entrega por correo electrónico	13
Botnets	13
Kits de herramientas de correo electrónico masivo	14
El fraude como método	15
Cómo protegerse contra ataques de correo electrónico	17
Señales indicativas de un correo electrónico de suplantación de identidad	17
Estrategias de prevención de ataques	19
Prepárese	20
Cómo proteger su correo electrónico	21
Serie de ciberseguridad de Cisco	22

Introducción

El año pasado, el correo electrónico no deseado cumplió 40 años. Sí, en 1978, se hizo evidente que Gary Thuerk, gerente de marketing de Digital Equipment Corporation, [envió el primer correo electrónico no deseado](#) a 393 personas en la ARPANET original para comercializar un nuevo producto. No sorprende que este mensaje se haya recibido con el mismo fastidio que gran parte del correo electrónico no deseado de la actualidad. Thuerk recibió una dura reprimenda y se le pidió que no volviera a hacerlo.

Si tan solo fuera así de simple hoy en día. Cuarenta años después, el correo electrónico no deseado ha crecido exponencialmente en su prevalencia, inundando nuestras bandejas de entrada con ofertas no deseadas de productos farmacéuticos, productos dietéticos y oportunidades de trabajo. No solo eso, sino que ahora se han sumado sus primos mucho más peligrosos, la suplantación de identidad y el malware. La suplantación de identidad se concibió por primera vez hace más de 30 años, y el malware también tiene una historia de varias décadas de distribución de correo electrónico.

Hoy en día, la triste realidad es que muchos correos electrónicos son no deseados y peor. El volumen es asombroso: [el 85 por ciento de todo el correo electrónico en abril de 2019 fue no deseado](#), según Talos Intelligence. El volumen de correo electrónico no deseado también está aumentando y ha alcanzado su punto máximo en 15 meses en abril.

Remitente vs. destinatario

Se podría argumentar que el correo electrónico está estructurado en un formato casi ideal para los estafadores. El correo electrónico obliga al usuario a leer y hacer evaluaciones sobre lo que recibe, y, luego, como resultado, a tomar decisiones sobre lo que abre o en lo que hace clic. La cantidad adecuada de ingeniería social, que aprovecha la buena disposición del individuo, puede empujar al usuario a la acción.

Es esta ingeniería social la que no solo lo convierte en un vector de entrega tentador, sino que también hace muy difícil de defender sistemáticamente. Un ataque por correo electrónico no suele omitir al usuario. Si bien son comunes las URL que conducen a sitios web riesgosos o maliciosos y utilizan kits de explotación, aún dependen de

convencer al usuario de que primero haga clic en un enlace de correo electrónico.

Lo que esto significa para los negocios

No es de extrañar que el correo electrónico sea uno de los desafíos principales que mantienen despiertos a los CISO. En nuestro estudio más reciente [de referencia de CISO](#), descubrimos que el 56 % de los encuestados de los CISO consideró que defenderse de los comportamientos de los usuarios, como hacer clic en un enlace malicioso de un correo electrónico, es muy o extremadamente difícil. Esto es más importante que cualquier otra preocupación de seguridad evaluada en la encuesta: más importante que los datos de la nube pública y más importante que el uso de un dispositivo móvil.

También es la frecuencia de tales intentos de ataque lo que llama la atención de los CISO. Por ejemplo, el 42 % de los CISO encuestados tuvo que enfrentar un incidente de seguridad que se produjo como resultado de un correo electrónico malicioso abierto dentro de su organización. El 36 % sufrió un incidente similar como resultado de la información robada en un ataque de suplantación de identidad. De acuerdo con nuestros datos de referencia de CISO, los CISO consideran que las amenazas de correo electrónico son el riesgo de seguridad número uno para sus organizaciones.

En un estudio diferente, [encargado por Cisco y llevado a cabo por ESG](#) en 2018, el 70 % de los encuestados informó que la protección contra amenazas de correo electrónico es cada vez más difícil. En cuanto a las consecuencias de los ataques por correo electrónico, el 75 % de los encuestados afirmó haber experimentado importantes impactos operativos y el 47 % informó importantes impactos financieros.



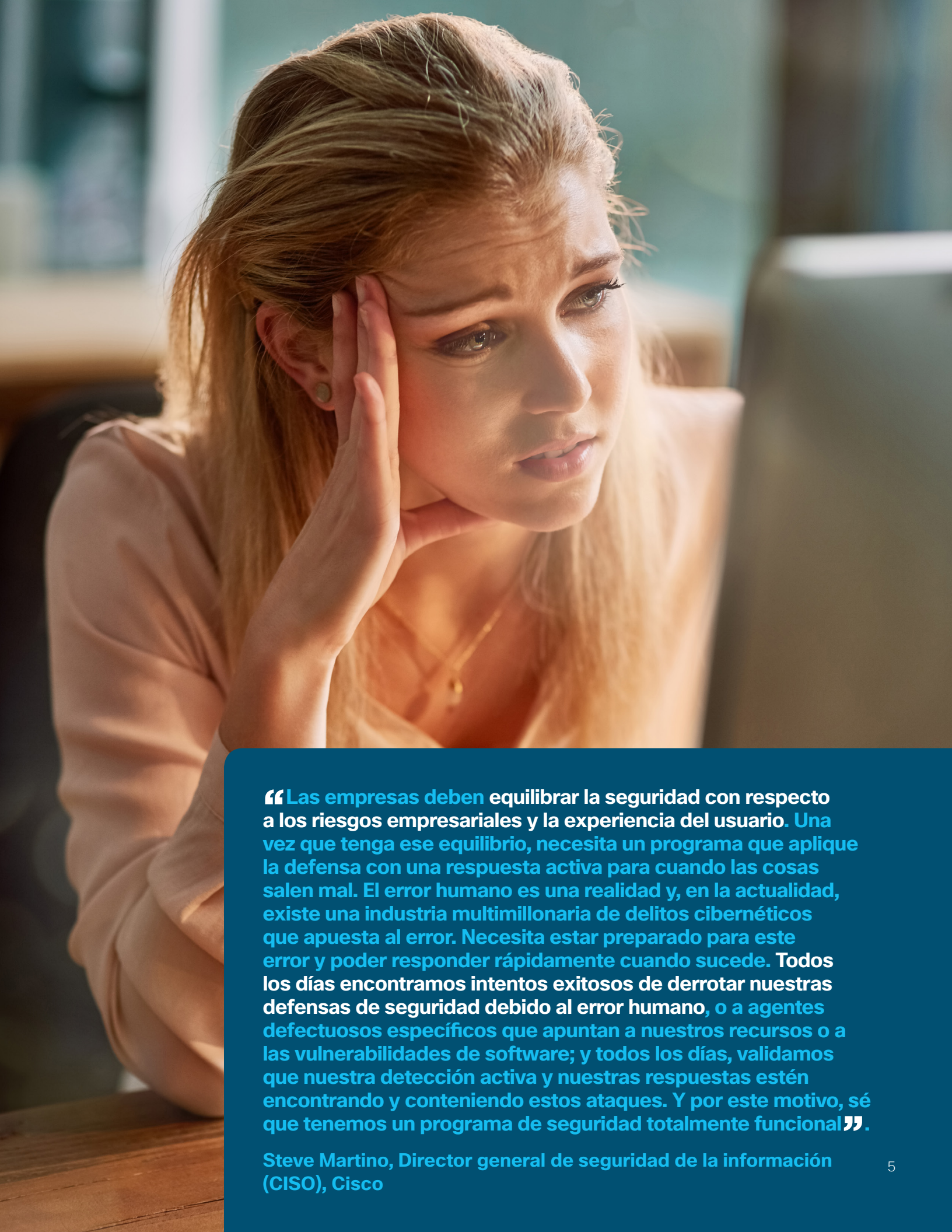
Respuesta requerida

¿Cómo puede proteger algo que es una necesidad y un riesgo al mismo tiempo? Para muchas organizaciones, la transición a la nube se ha visto como una solución. Sin embargo, la nube no es un arma infalible contra los peligros del correo electrónico. En la mayoría de los casos, es simplemente posponer el riesgo. Los problemas de seguridad no desaparecen, sino que persisten.

Hay varias maneras de minimizar el impacto que las amenazas de correo electrónico representan en general. En este informe, abordaremos el panorama de amenazas actual, lo cual ofrece una descripción general de los tipos de ataque de correo electrónico más comunes en la actualidad. Desglosaremos la forma en que se despliegan, sus objetivos y la infraestructura detrás de ellos. Analizaremos lo que puede hacer para proteger su empresa, como también cómo identificar amenazas por correo electrónico cuando los usuarios las encuentren.

“En un día promedio, recibimos alrededor de 412 000 mensajes de correo electrónico, de los cuales 266 000 ni siquiera llegan a nuestros motores SMTP porque Talos los bloquea en función de su inteligencia de amenazas globales”.

Milind Samant, Gerente de seguridad, SUNY Old Westbury



“Las empresas deben equilibrar la seguridad con respecto a los riesgos empresariales y la experiencia del usuario. Una vez que tenga ese equilibrio, necesita un programa que aplique la defensa con una respuesta activa para cuando las cosas salen mal. El error humano es una realidad y, en la actualidad, existe una industria multimillonaria de delitos cibernéticos que apuesta al error. Necesita estar preparado para este error y poder responder rápidamente cuando sucede. Todos los días encontramos intentos exitosos de derrotar nuestras defensas de seguridad debido al error humano, o a agentes defectuosos específicos que apuntan a nuestros recursos o a las vulnerabilidades de software; y todos los días, validamos que nuestra detección activa y nuestras respuestas estén encontrando y conteniendo estos ataques. Y por este motivo, sé que tenemos un programa de seguridad totalmente funcional”.

Steve Martino, Director general de seguridad de la información (CISO), Cisco

El panorama actual del correo electrónico y la suplantación de identidad

Los riesgos presentados por el correo electrónico son numerosos. Según el [Informe de investigaciones sobre la infiltración de datos de 2018 de Verizon](#), del que Cisco es un colaborador, el correo electrónico es el principal vector para la distribución de malware (92,4 %) y la suplantación de identidad (96 %). Abra el correo electrónico incorrecto y podría verse víctima de criptominería, podrían robar sus credenciales o, si es víctima de una estafa de ingeniería social, podrían robarle grandes sumas de dinero. Escale esto a nivel de la empresa y el correo electrónico equivocado puede causar estragos.

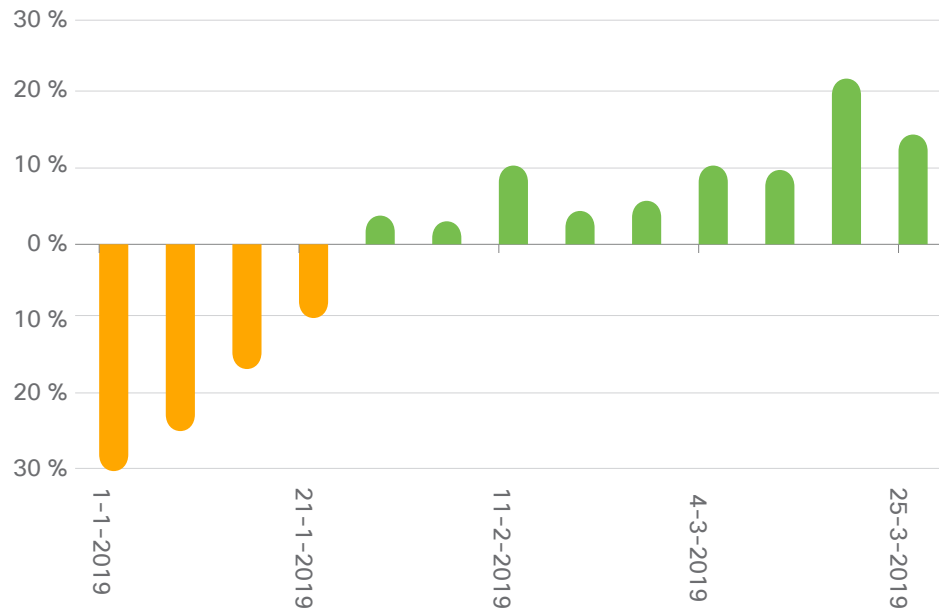
Desafortunadamente, muchas personas caen en la trampa. Según el [Informe de acceso confiable de Duo 2018](#), el 62 % de las campañas de simulación de suplantación de identidad que se ejecutaron, capturaron al menos un conjunto de credenciales de usuario. De todos los destinatarios, casi un cuarto de ellos hizo clic en el enlace de suplantación de identidad en el correo electrónico. Y la mitad de ellos ingresó las 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 suplantación de identidad. De hecho, parece que la actividad de suplantación de identidad podría ir en aumento, si la cantidad de nuevos dominios de suplantación de identidad identificados por Cisco Umbrella es una indicación válida. 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 lentamente, se aceleró la producción de nuevos dominios, lo que vio un aumento del 64 % de la primera semana del trimestre a la última.



¿Con qué frecuencia los usuarios son víctimas de estafas por correo electrónico? Pregúnteles a las personas de Duo Security. El equipo creó la [herramienta Duo Insight](#) gratuita hace unos años, lo que permite a los usuarios crear sus propias campañas falsas de suplantación de identidad y probarlas dentro de sus propias organizaciones para ver quiénes caen y quiénes no.

Figura 1 Nuevos dominios semanales de suplantación de identidad en comparación con el promedio semanal del primer trimestre.



Fuente: Cisco Umbrella

Tipos de ataque de correo electrónico comunes

Los siguientes son ejemplos de las estafas basadas en correo electrónico más comunes de la actualidad. Tome su computadora portátil, abra su bandeja de entrada e imagine los siguientes mensajes no leídos.

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

Suplantación de identidad de Office 365

El correo electrónico parece provenir de Microsoft. Dice que su dirección de correo electrónico de Office 365 se desconectará debido a errores o violaciones de políticas. La única manera de evitar que esto suceda es verificando la dirección en el enlace proporcionado.

Este estilo de ataque va en aumento. Según los datos publicados por nuestros partners en Agari en el informe de [Tendencias de fraude y suplantación de identidad de correo electrónico del segundo trimestre de 2019](#), el 27 % de los ataques de correo electrónico avanzado se lanzan a partir de cuentas de correo electrónico en riesgo. Esto ha aumentado siete puntos porcentuales desde el último trimestre de 2018, cuando el 20 % de los ataques de suplantación de identidad procedían de correos electrónicos en riesgo.

Tampoco es solo Office 365 la que está siendo atacada. Se han observado ataques de suplantación de identidad similares contra otros servicios de correo electrónico basados en la nube, como Gmail y G Suite, la oferta de correo electrónico en la nube de Google. Dada la prevalencia de las cuentas de Google y la forma en que se aprovechan a través de Internet para iniciar sesión en diferentes sitios web, no es de extrañar que los atacantes hayan creado sitios de suplantación de identidad en esta área también.



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

Este es un intento de suplantar la identidad de sus credenciales de Office 365. Los correos electrónicos y las URL utilizados pueden incluso parecerse a lo que está acostumbrado a encontrar en Office 365, por ejemplo: micros0ftsupport@hotmail.com. Si hace clic en el enlace, lo llevará a una página de inicio de sesión de aspecto oficial y solicitará su dirección de correo electrónico y contraseña.

Sin embargo, el sitio es falso. Una vez que los estafadores tienen sus credenciales, pueden intentar iniciar sesión en otros servicios relacionados con Microsoft, así como también

Figura 2 Sitio de suplantación de identidad diseñado deliberadamente para que se parezca a la página de inicio de sesión de Microsoft.

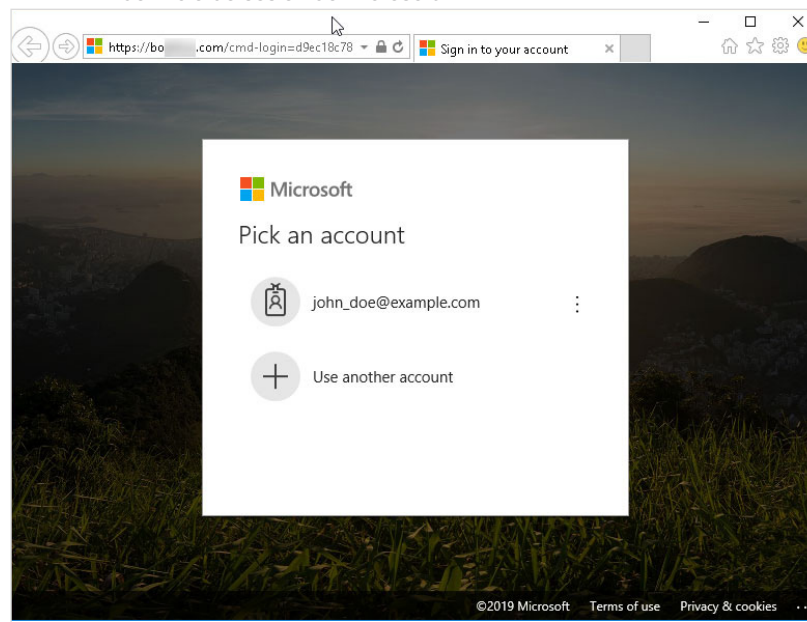
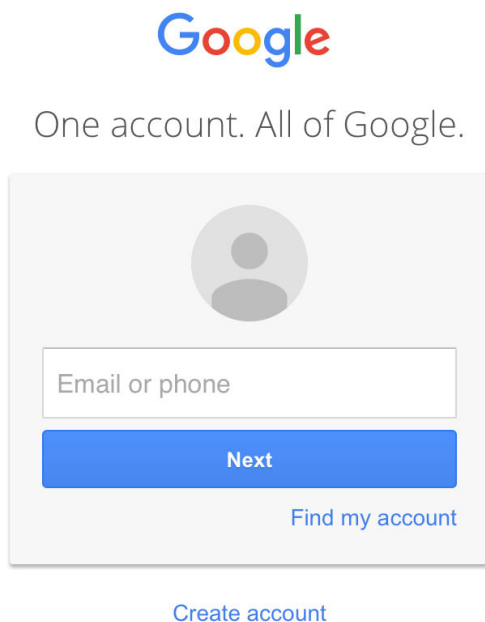


Figura 3 Ejemplo de inicio de sesión de cuenta de Google. ¿Puede distinguir lo real de lo falso?



Riesgo de correo electrónico comercial

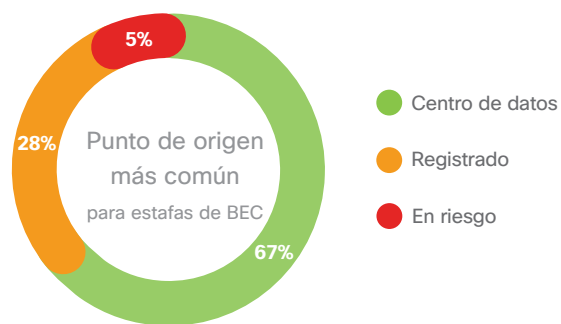
Es la semana de la gran cumbre de la empresa y todo el mundo está fuera de la oficina, excepto por un puñado de personas que mantienen funciones críticas. Usted es miembro del equipo de finanzas y parte del personal mínimo que aún está en el sitio. De repente, llega un correo electrónico a su bandeja de entrada que parece provenir del CFO con el asunto " Pago omitido". El correo electrónico explica que se perdió un pago que se suponía debía emitirse la semana pasada y que podría provocar una interrupción en la cadena de abastecimiento de la empresa. Se adjuntan las instrucciones de transferencia bancaria. El remitente termina diciendo que lo llamará en una hora con respecto a esto.

Este es esencialmente el riesgo de correo electrónico comercial (BEC). Las estafas de BEC son una forma de fraude por correo

electrónico en la que el atacante se hace pasar por un ejecutivo de nivel C o superior e intenta engañar al destinatario para que desempeñe su función comercial, para un propósito ilegítimo, como la transferencia de dinero al atacante. De hecho, a veces llegan a llamar a la persona y se hacen pasar por el ejecutivo. Y parece funcionar. Según el Centro de quejas de delitos de Internet (IC3), había [1300 millones de dólares en pérdidas](#) en 2018 debido a estafas de BEC.

Uno podría pensar que los atacantes aprovechan cuentas comprometidas en estafas de BEC, como lo hacen con las estafas de suplantación de identidad de Office 365. Sorprendentemente, según el [informe de Tendencias de fraude y suplantación de identidad por correo electrónico de Agari del segundo trimestre de 2019](#), solo el cinco por ciento de estas estafas lo hace. Dos tercios de estos ataques aún utilizan cuentas de correo electrónico gratuitas para lanzar los ataques, mientras que el 28 % restante lleva a cabo ataques a medida mediante dominios registrados. El último nivel de personalización se extiende al cuerpo del correo electrónico, donde, según Agari, uno de cada cinco correos electrónicos de BEC incluye el nombre del destinatario seleccionado.

Figura 4 Punto de origen de correo electrónico BEC.



Fuente: Agari Data, Inc.

Figura 5 Un ejemplo reciente de extorsión digital.**DEBE TOMARLO MUY EN SERIO.**

MR

Lunes 04/08/2019 08:30 h
Usted

Supongo que se está preguntando por qué está recibiendo este correo electrónico, ¿no?

He colocado un malware en un sitio web para adultos (sitio... P... O... r... n...o) y, cuando usted visitó el sitio y reprodujo el video, su dispositivo se vio afectado e ingresó un spyware en su máquina. Este lo grabó a usted con la cámara web y una captura de pantalla mientras usted "se divertía", permitiéndome ver exactamente lo que usted ve.

Esto también afectó su smartphone a través de un ataque. Por lo tanto, no piense ni por un minuto que puede eludir esto reinstalando el SO. Usted ya quedó grabado.

Después de esto, mi malware recopiló todos sus contactos de servicios de mensajería, correos electrónicos y redes sociales.

Esta no es una buena noticia, ¿no cree?

Pero no se preocupe demasiado, hay una manera en que podemos solucionar este problema de privacidad. Todo lo que necesito es un pago en Bitcoin de £850, que creo que es un precio justo, teniendo en cuenta las circunstancias.

Debe realizar el pago en bitcoins

Mi dirección de billetera de Bitcoin: 36QEsmKieqmfCBuAdcWg9beAj3ANAp6cAN (es sensible a mAYúscUlAs y miNúscUlAs, por lo que debe copiarla y pegarla).

Solo tiene 48 horas después de leer este correo electrónico para enviar el pago (se lo advierto, sé cuándo ha abierto y leído este correo electrónico, he colocado una imagen de píxeles dentro de este. Esto me permite saber el momento exacto en que ha abierto el mensaje, el día y la hora.

Si decide ignorar este correo electrónico, no me quedará más remedio que reenviarlo a todos los contactos recopilados que tiene en su cuenta de correo electrónico, así como publicarlo en sus cuentas de medios sociales y enviarlo como mensaje personal a todos sus contactos de Facebook, y, por supuesto, hacer que el video esté disponible públicamente en Internet, a través de YouTube y sitios web para adultos. Teniendo en cuenta su reputación, realmente dudo que desee quedar expuesto ante su familia/amigos/compañeros de trabajo en este momento.

Si recibo el pago, se destruirá todo el material y no volverá a saber de mí. Si no obtengo mi dinero por algún motivo, como la incapacidad de enviar dinero en efectivo a una billetera en la lista negra, su reputación se verá destruida. Por eso, hágalo rápido.

No intente ponerse en contacto conmigo porque estoy usando el correo electrónico de una víctima que fue hackeado y expuesto.

Si no me cree y quiere comprobarlo, responda este correo electrónico con "PROOF" (prueba) y enviaré su video a 5 de sus contactos por correo electrónico y lo publicaré en su muro de Facebook. Y aquí, podrá eliminarlo una única vez, no para siempre.

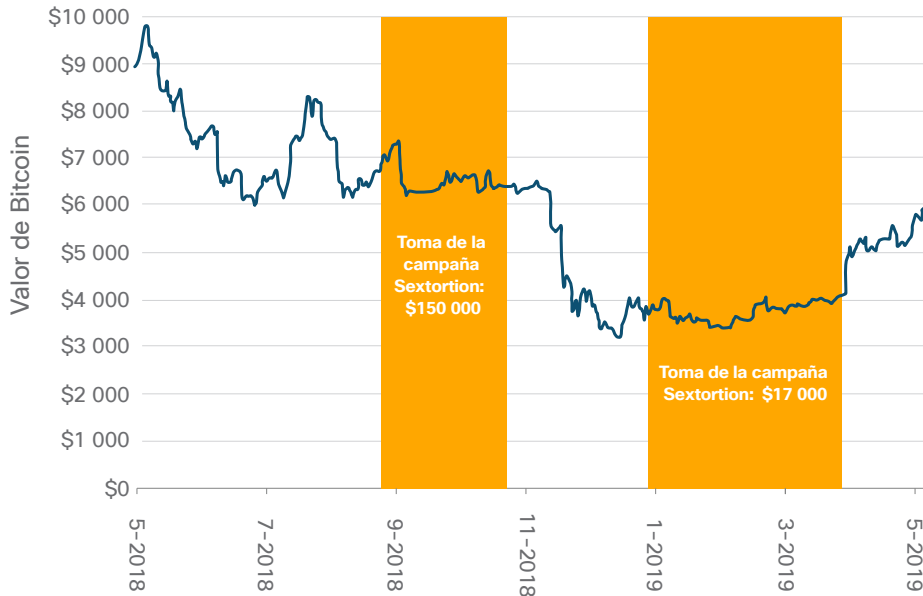
Extorsión digital

Llega un correo electrónico a su bandeja de entrada con el asunto **"DEBE TOMAR ESTO MUY SERIAMENTE"**. El o la remitente del correo electrónico afirma haber puesto en riesgo un sitio web de videos para adultos y que usted visitó el sitio. También afirma haberlo grabado a través de su cámara web, viendo los videos que afirma que usted reprodujo. Asimismo, el remitente afirma haber obtenido acceso a sus contactos y les enviará a todos la grabación, a menos que les pague cientos, si no miles, de dólares en bitcoins.

Esto es extorsión digital. Lo único que distingue esta situación de las extorsiones más tradicionales es que las afirmaciones son completamente inventadas. Los estafadores no han puesto en riesgo ningún sitio web, no lo han grabado y no tienen su lista de contactos. Simplemente esperan engañarlo para que crea que es así.

Abarcamos las diferentes formas de este tipo de estafa por correo electrónico en nuestra publicación de blog [Amenaza del mes, titulada Su dinero o su vida: estafas de extorsión digital.](#)

Figura 6 Comparación del valor de Bitcoin (USD) con la toma de campañas de extorsión sexual.



Fuente: Cisco Talos

Es un truco interesante y lucrativo para los atacantes, y las ganancias obtenidas de una campaña de extorsión digital alcanzaron las seis cifras a fines de 2018. Sin embargo, según [el análisis más reciente realizado por Cisco Talos](#), que abarca de enero a marzo de 2019, las ganancias han disminuido. Aun así, el aumento y la disminución de estas ganancias está vinculado con el valor de Bitcoin, aunque las disminuciones son mayores. Como el valor de Bitcoin parece ir en aumento en la actualidad, será interesante ver si sucede lo mismo con los pagos por extorsión digital.

Paquete y correo electrónico no deseado de facturación

"No recuerdo haber adquirido una suscripción a esta aplicación móvil", usted se dice a sí mismo. Al menos, esto es lo que implica el correo electrónico: una suscripción de por vida a, por ejemplo, un club de películas. Espere, la ubicación que aparece en la factura indica que se adquirió en Sri Lanka. Y usted ni siquiera vive en Sri Lanka. "Debe haber algún error", se dice a usted mismo, a medida que abre rápidamente el PDF adjunto para investigar.

Desafortunadamente, ese PDF contenía un ataque que acabó por [descargar Emotet en su dispositivo](#). La estafa varía, pero, generalmente, se centra en un paquete que usted no ordenó, una factura por algo que no adquirió o un pago mensual por una suscripción o un servicio en el que no se inscribió. Esto puede generar resultados maliciosos, desde credenciales bancarias robadas hasta criptominería.

Figura 7 Correo electrónico de estafa de Emotet, que finge provenir de UPS.

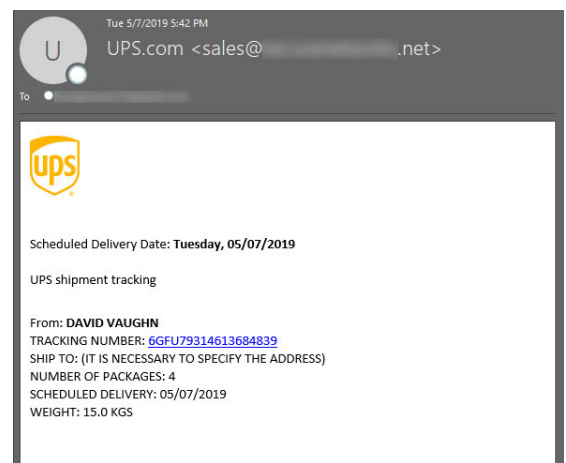


Figura 8 Ejemplo de fraude de tarifa por adelantado reciente.

Sr. Christopher A. Wray



Director de la Oficina Federal de Investigaciones (FBI)

A: [Redacted]

Responder a: [Redacted]

ATENCIÓN: destinatario.

De acuerdo con la ética de una oficina, la presentación siempre es muy importante en un primer contacto como este. Soy el Sr. Christopher A. Wray, Director de la Oficina Federal de Investigaciones (FBI). Esta comunicación oficial es para informarle que descubrimos que algunos funcionarios que trabajan para el gobierno de los Estados Unidos han intentado desviar sus fondos a través de un canal oculto. En realidad, descubrimos esto hoy, a través de nuestros agentes secretos en la unidad disciplinaria de la Oficina Federal de Investigaciones (FBI) después de arrestar a un sospechoso.

El sospechoso mencionado fue detenido en el Aeropuerto Internacional de Dulles esta mañana, mientras intentaba transportar la enorme cantidad de dinero en efectivo fuera de las costas de los Estados Unidos. Con respecto al decreto contra el lavado de dinero de los Estados Unidos, dicha cantidad de dinero en efectivo no se puede transportar fuera de los Estados Unidos porque tal intento es un delito penal punible en virtud de la ley contra el lavado de dinero de 1982 de los Estados Unidos de América. Este decreto es una ley globalizada aplicable en la mayoría de los países desarrollados para controlar el terrorismo y el lavado de dinero.

De nuestra información recopilada en esta unidad, descubrimos que los fondos en cuestión de hecho le pertenecen, pero se habían retrasado intencionalmente porque los funcionarios a cargo de su pago se encuentran en algún tipo de irregularidades, lo cual va en contra de la ética de cualquier institución de pagos. En la actualidad, estos fondos están bajo la custodia del banco pagador y puedo asegurarle que sus fondos se le liberarán sin problemas, siempre que usted sea sincero con nosotros en este asunto. Además, requerimos su cooperación positiva en todos los niveles porque estamos monitoreando de cerca esta misma transacción para evitar los aspectos negativos de la sociedad actual.

El día de hoy, 9 de mayo de 2019, hemos ordenado a la gestión ejecutiva del banco pagador que libere dichos fondos a usted, como el beneficiario certificado en cuestión, porque contamos con información valiosa y registros de autenticidad que confirman que dichos fondos realmente le pertenecen. De cualquier manera, solicitamos que nos proporcione la información que figura a continuación (para la verificación oficial).

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

Esperamos su cumplimiento inmediato de esta obligación oficial, para que el banco pagador autorizado le pueda abonar.

Con sello oficial.

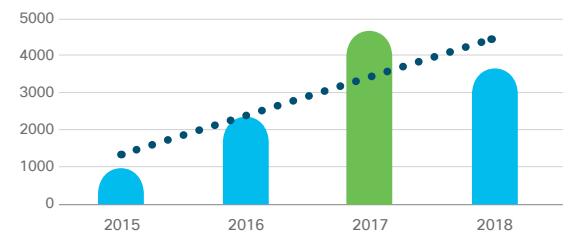
Sr. Christopher A. Wray
Director de la Oficina Federal de Investigaciones (FBI)

Fraude de tarifa por adelantado

No todos los días recibe un correo electrónico del FBI. ¡Es aún menos común recibir uno que le informa acerca de una transferencia pendiente de 10,5 millones de dólares! Solo debe responder al correo electrónico y le indicarán lo que debe hacer para recibir el pago.

Esta es una estafa clásica de fraude de tarifa por adelantado. Como su nombre lo indica, los estafadores pedirán una suma antes de enviarle el dinero prometido, el cual nunca aparece. Es también una de las estafas de correo electrónico más antiguas y ha adoptado diferentes formas a lo largo de los años, desde un príncipe extranjero que desea compartir su riqueza hasta aprobaciones de préstamos para personas con malos antecedentes de crédito. Aun así, las estafas continúan, y cada año, miles de estas estafas por correo electrónico [se informan a la Better Business Bureau \(BBB\) de los EE. UU.](#)

Figura 9 Estafas de fraude de tarifa por adelantado según lo informado al BBB por año. (Categorías de tipo de estafa por préstamo total de tarifa por adelantado, intercambio de dinero nigeriano/extranjero, romance, reparación de crédito/reducción de la deuda, inversión y viajes/vacaciones).



Fuente: Better Business Bureau

Malware en el correo electrónico

Una buena parte del malware aún se envía a través del correo electrónico. Solía ser más notorio y se adjuntaban archivos .exe directamente a correos electrónicos. Pero, a medida que los usuarios se fueron dando cuenta de que abrir un ejecutable no era una decisión segura, los actores maliciosos cambiaron sus tácticas.

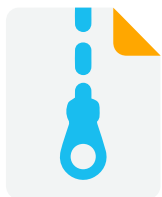
Hoy en día, es mucho más probable que el malware se envíe en forma indirecta, ya sea a través de adjuntos menos sospechosos, como documentos comerciales comúnmente usados o por URL contenidas en el cuerpo del mensaje, todos los cuales son elementos que se suelen enviar a través de un correo electrónico regular y válido. La idea aquí es ir más allá de los análisis de correo electrónico tradicionales que capturan y colocan en cuarentena un archivo binario u otros adjuntos distribuidos con poca frecuencia.

Esto se hace evidente cuando se observan los adjuntos de correo electrónico marcados en el presente año (enero-abril de 2019). Los archivos binarios representan menos del 2 % de todos los adjuntos maliciosos, que no son solo archivos .exe, sino todos los binarios. Este es un gran cambio en relación a años pasados, cuando se encontraron periódicamente archivos ejecutables, Java y Flash. De hecho, Java y Flash se han dejado de usar tanto que, si los agrega a los binarios, solo estará observando el 1,99 % de los archivos adjuntos.

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

Entonces, ¿qué tipos de adjuntos han pasado a usar los atacantes? Archivos como los .zip conforman casi un tercio de los archivos adjuntos y cuatro de los diez principales tipos de archivos. Scripts como los archivos .js representan el 14,1 %. Estos scripts han mostrado un drástico aumento desde la última vez que analizamos los tipos de adjuntos en el [Informe de ciberseguridad anual \(ACR\)](#) de 2018, cuando los archivos .js, combinados con XML y HTML, solo representaron el uno por ciento de extensiones de archivos maliciosos.

Su frecuencia como adjuntos maliciosos ha seguido creciendo, llegando a casi cinco puntos porcentuales desde el ACR 2018. Agregue documentos PDF a la mezcla y verá que más de la mitad de todos los adjuntos maliciosos son tipos de documentos que se utilizan regularmente y predominan en el lugar de trabajo moderno.



Archivos como los .zip conforman casi un tercio de los adjuntos maliciosos y cuatro de los diez principales tipos de archivos usados por atacantes.

Tabla 1 Tipos de adjuntos maliciosos.

Tipo	Porcentaje
Office	42,8 %
Archivo	31,2 %
Script	14,1 %
PDF	9,9 %
Binario	1,77 %
Java	0,22 %
Flash	0,0003 %

Fuente: Talos Intelligence

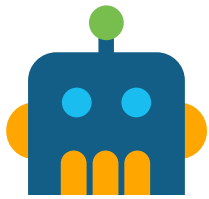
Tabla 2 Las 10 principales extensiones maliciosas en el correo electrónico.

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 entrega por correo electrónico

Observemos lo que ocurre detrás de la cortina, en lugar de los tipos de correos electrónicos o las cargas útiles, y echemos un vistazo a la forma en que se distribuyen los correos electrónicos maliciosos. Existen dos métodos principales que los estafadores utilizan para lanzar campañas de spam: botnets y kits de herramientas de correo electrónico masivo.



Botnets

Los botnets de correo electrónico no deseado son por lejos los principales culpables de la mayoría de dichos correos que se envía hoy. Los siguientes son algunos de los actores clave en el panorama de botnets de correo no deseado.

Necurs

El botnet Necurs surgió por primera vez en 2012 y ha diseminado una variedad de amenazas, que van desde Zeus hasta ransomware. Si bien su actividad ha recibido mucha más atención en el pasado, Necurs parece haber quedado en segundo plano, al menos en términos de cobertura de prensa. Sin embargo, este botnet sigue estando muy activo. De hecho, el botnet Necurs es el principal vehículo de distribución para una variedad de estafas, incluida la extorsión digital.

Para obtener más información sobre Necurs, consulte el análisis [Los muchos tentáculos del botnet Necurs](#), desarrollado por Cisco Talos.

Emotet

Muchos de los correos no deseados enviados por Emotet se ubican en la categoría de paquetes y facturación. Emotet es un malware modular e incluye un complemento de spambot. Teniendo en cuenta cómo los agentes detrás de Emotet ganan dinero usándolo como canal de distribución para otras amenazas, el objetivo de la mayoría del correo electrónico no deseado enviado por el módulo spambot es infectar más sistemas con Emotet, lo que amplía aún más el alcance de los canales de distribución maliciosos.

Debido a que Emotet roba contenido de los buzones de entrada de las víctimas, a menudo es capaz de crear mensajes de subprocesos maliciosos, pero de aspecto realista, que a los destinatarios les parecen ser parte de conversaciones establecidas. Emotet también es conocido por robar credenciales SMTP, requisando los propios servidores de correo electrónico salientes de las víctimas como vehículo para el correo malicioso saliente.

Para obtener más información sobre Emotet, lea nuestro informe anterior de amenazas en [Defensa contra las amenazas críticas de la actualidad, la serie de informes sobre ciberseguridad](#).

“Cisco Email Security disminuyó el tiempo dedicado a la detección y disminuyó el correo electrónico no deseado en un 80 % aproximadamente”.

Jacquelyn Hemmerich, Funcionario de seguridad, Ciudad de Sarasota, FL

Gamut

El botnet Gamut ha estado ocupado enviando correo no deseado de citas y relaciones íntimas, principalmente en torno a la premisa de conocer personas en su área. En otras campañas, los agentes detrás del botnet envían mensajes que pregonan la venta de productos farmacéuticos u oportunidades de trabajo (consulte la Figura 10).

Han registrado una variedad de dominios, aunque la infraestructura en sí parece bastante simple, con varios subdominios en un dominio y, a menudo, señalando una dirección IP. Si bien Cisco no ha confirmado si los servicios ofrecidos son legítimos, el proceso de registro parece intentar suplantar la información personal.

Figura 10 Correo electrónico no deseado enviado por el botnet Gamut.

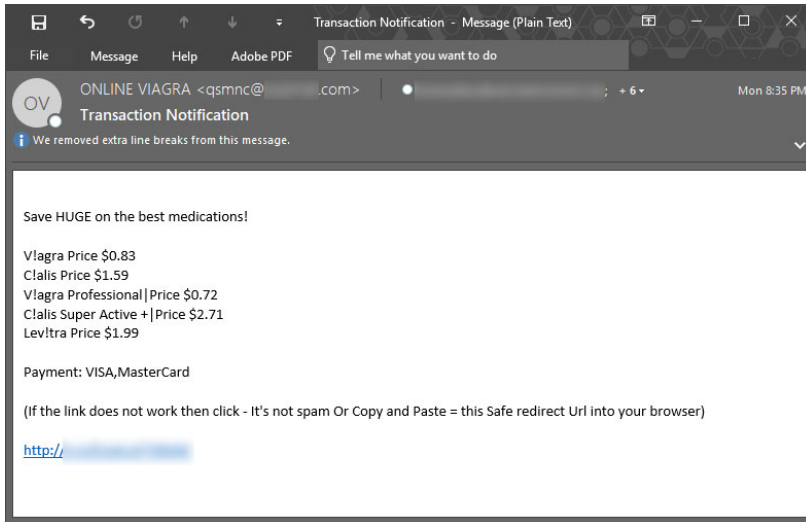
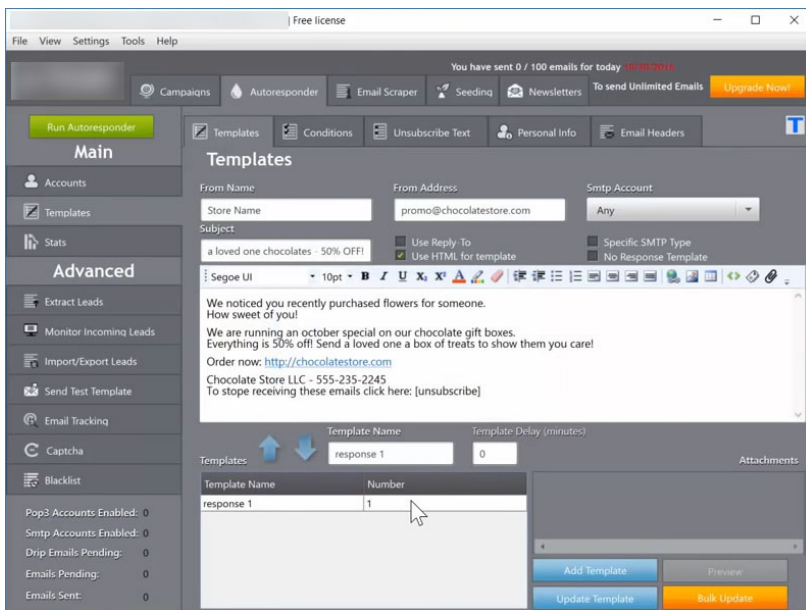


Figura 11 Ejemplo de kit de herramientas de correo electrónico no deseado.



Kits de herramientas de correo electrónico masivo

Un enfoque alternativo que muchos remitentes de correo no deseado adoptan es la compra de kits de herramientas para enviar una gran cantidad de correos electrónicos. Muchas de estas herramientas son semilegítimas, lo que significa que, si estuviera vendiendo sus propias cortinas de ducha hechas a mano y personalizadas, podría usar uno de estos kits de herramientas para crear conciencia de marca a través del correo electrónico masivo a su propia lista de correo de suscripción. Sin embargo, algunas de las características incluidas en estos kits de herramientas, como las que permiten la rotación del envío de direcciones IP y la reconstrucción personalizada de adjuntos para generar valores de hash exclusivos, son mucho menos propensas a ser utilizadas en tales situaciones.

Recientemente, los ingenieros de Cisco Talos descubrieron grupos de Facebook en los que los agentes maliciosos vendían herramientas de correo electrónico masivo junto con extensas listas de direcciones de correo electrónico, probablemente tomadas de violaciones de datos. En estos casos, los compradores de dichas herramientas las usaban claramente para fines nefastos.

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. Los agentes maliciosos detrás de las estafas de BEC intentan realizar estafas a las empresas por miles de dólares. Los extorsionistas digitales están engañando en forma fraudulenta a los usuarios para que les paguen en Bitcoins. Y cuando se trata de fraude de tarifa por anticipado, bien, el propio nombre lo dice.



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

Nada de esto es nuevo. El correo electrónico es solo una de las últimas herramientas que los delincuentes han utilizado para cometer fraude. Históricamente hablando, los delincuentes siempre se han esforzado por aprovechar al máximo las oportunidades ilícitas que presenta cada generación de tecnología.

En vista de las pérdidas registradas por la Policía Federal de Alemania (Bundeskriminalamt BKA) y el FBI, más del 80 % de todas las pérdidas registradas por delitos cibernéticos puede atribuirse a la intención de fraude. Se debe poner énfasis en "registradas", ya que puede haber pérdidas intangibles que son difíciles de cuantificar y registrar con precisión. Esto significa que las estadísticas registradas son bastante confiables.

Por lo tanto, es correcto afirmar que el fraude es la fuerza motriz detrás de las pérdidas por delitos cibernéticos. De hecho, al examinar dos métodos de fraude que indican las estadísticas del FBI, a saber, el riesgo de correo electrónico comercial (BEC) y el riesgo de cuentas de correo electrónico (EAC), vemos que las pérdidas en 2018 fueron de 1300 millones de dólares. Como comparación, las pérdidas equivalentes registradas debido a ransomware, una forma a menudo mencionada y analizada de delitos cibernéticos, fueron por 3,6 millones de dólares. Y el hecho sigue siendo el mismo: todo indica que las pérdidas asociadas con el fraude no detectado seguirán aumentando, ya que las pérdidas asociadas solo con BEC/EAC aumentaron un 78 % entre 2016 y 2017.

“Cisco Email Security literalmente ha retirado la seguridad de correo electrónico de nuestras tareas de administración y nos ha permitido centrarnos en otras áreas. ¡Atrapa todo! ¡Es una tranquilidad saber que hemos tomado la decisión perfecta para la seguridad de correo electrónico!”

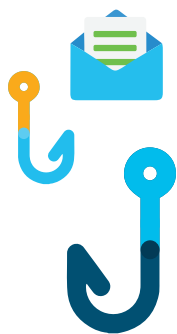
Steven Wujek, Arquitecto senior de TI, Technology Concepts & Design, Inc.

Para más información sobre el fraude y las pérdidas por delitos cibernéticos, consulte nuestra serie de blogs sobre [delitos cibernéticos y fraude](#).



“Adoptar un enfoque integral de seguridad no es simplemente un problema de productos de seguridad o un imperativo comercial. Se trata de observar a las personas, los procesos y la tecnología en todo el negocio. En Cisco, comenzamos con un enfoque centrado en las personas, el cual se enfoca en los individuos y el trabajo que realizan, y en ayudarlos a hacer su trabajo de manera segura. Una de las maneras en que lo logramos es ofreciendo a los trabajadores consejos prácticos para reconocer e informar el correo electrónico sospechoso antes de que hagan clic en este”.

Steve Martino, Director general de seguridad de la información (CISO), Cisco



Cómo protegerse contra ataques de correo electrónico


Señales indicativas de un correo electrónico de suplantación de identidad

El lado positivo cuando se trata de amenazas enviadas por correo electrónico es que generalmente hay discrepancias que las identifican como tales, si solo se sabe a qué prestar atención. Los siguientes son algunos ejemplos. Consulte la siguiente página para obtener detalles sobre cada uno.

Para: you@youremail.com

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

Asunto: Su pedido reciente



2 Estimado/a:

Gracias por su pedido. Los detalles son los siguientes:


Compra: suscripción de entrega mensual a Puppy Food™
 comida de marca para cachorros
 Costo mensual: 121 USD
 Fecha y hora: 03 de mayo de 2019 a las 10:21 h
 Dirección IP: 254.189.234.159.01
 País de compra: Guatemala

3 Si ya no desea suscribirse, cancele inmediatamente siguiendo las instrucciones del adjunto o ingresando los datos de su tarjeta de crédito aquí:

4

5 <http://badphishingsite.com/dontgothere.html>

Cordialmente.
 Envío de Amazon



6 **dontopenthis.bad**

Figura 12 Advertencia de Microsoft Office sobre macros en el documento abierto.



BLOCKED CONTENT Macros in this document have been

- 1 **La dirección De:** ¿El nombre en la dirección De: no se alinea con la dirección de correo electrónico?
- 2 **Muchos errores ortográficos y gramaticales o logotipos borrosos.** Si el correo electrónico parece haber sido diseñado de manera descuidada, puede que no sea legítimo.
- 3 **Sentido de urgencia.** Si, en un correo electrónico, se le pide que tome medidas inmediatas, si tiene un sentido de urgencia o si despierta su curiosidad, actúe con sospecha.
- 4 **Solicitud de información personal o confidencial.** Nunca responda a un correo electrónico no deseado que le solicite información personal, financiera o confidencial.
- 5 **URL de aspecto ilegítimo.** Muchas URL de correo electrónico de suplantación de identidad parecen inusuales, si se analizan, y no se deben hacer clic. Si la URL está oculta dentro de un enlace de texto, sitúese sobre esta y observe la parte inferior de su navegador para examinarla. En caso de duda, no haga clic.
- 6 **Tipo de archivo no reconocido.** En la mayoría de los asuntos profesionales, solo debería recibir por correo electrónico unos pocos tipos de archivos. Si el tipo de archivo parece extraño, no lo abra.

Además de:

- **Actúe con tranquilidad.** Una persona promedio pasa de 8 a 10 segundos escaneando un correo electrónico antes de realizar una acción. Tranquilícese y busque las pistas que podrían indicar un intento de suplantación de identidad.
- **Si parece demasiado bueno para ser verdad, probablemente no es verdadero.** ¿El correo electrónico le ofrece millones de dólares? ¿Amenaza con avergonzarlo o lastimarlo? Es probable que sea completamente inventado.
- **Preste mucha atención a las advertencias.** Si reconoce al remitente y abre un adjunto, preste mucha atención a las advertencias del banner sobre extensiones o macros que deben habilitarse (Figura 12). No suelen ser necesarios.



Estrategias de prevención de ataques

Se pueden adoptar varios enfoques para reducir el riesgo que representan las amenazas de correo electrónico.

Ejecute ejercicios regulares de suplantación de identidad. Sus empleados son su mayor defensa contra la suplantación de identidad, especialmente los intentos de suplantación de identidad más personalizados. Los empleados que pueden aprender a reconocer un intento de suplantación de identidad directamente pueden detener la principal causa de riesgo de los terminales.

Para crear conciencia, ejecute ejercicios de suplantación de identidad corporativa regulares para probar y educar a los usuarios. Emule las últimas técnicas reales para que las personas estén al tanto de lo que pueden encontrar. Cisco sugiere ejecutar estos ejercicios mensualmente, comenzando con campañas de prueba de suplantación de identidad fáciles de detectar y aumentando gradualmente la complejidad. Ofrezca educación inmediata a los usuarios que caen víctimas de ataques de suplantación de identidad emulados, (por ej., envíe una URL "maliciosa" de prueba que conduzca a más información sobre la suplantación de identidad). En el caso de usuarios de alto riesgo en su organización, donde podrían producirse daños significativos si caen en una trampa, lleve a cabo ejercicios de campaña de suplantación de identidad personalizados.

Use autenticación de varios factores. En caso de que logren robar credenciales de una cuenta de correo electrónico corporativo, la autenticación de varios factores puede impedir que un atacante obtenga acceso a la cuenta y cause estragos.

La belleza de la autenticación de varios factores radica en su simplicidad. Supongamos que alguien logra obtener sus credenciales de inicio de sesión o las de alguien en su red, e intenta iniciar sesión. Con la autenticación de varios factores, se envía automáticamente un mensaje al individuo que

posee la credencial para verificar si acaba de intentar iniciar sesión. En esta situación, al darse cuenta de que no intentó iniciar sesión, el usuario niega la solicitud de inmediato. Esto frustra el ataque con éxito.

Mantenga el software actualizado. En algunos casos, los correos electrónicos que incluyen URL maliciosas pueden enviar a los usuarios a páginas con ataques. Mantener los navegadores y el software actualizados, así como cualquier complemento, ayuda a reducir los riesgos que representan dichos ataques.

Nunca transfiera dinero a un extraño. Esto se aplica al fraude de tarifa por anticipado y a las estafas de BEC. Si tiene alguna sospecha sobre una solicitud, no responda. Para BEC en particular, establezca políticas estrictas que requieran la autorización de transferencia bancaria de un individuo de alto rango dentro de la empresa y tengan un signatario secundario específico.

Tenga cuidado con las solicitudes para iniciar sesión. Los agentes maliciosos decididos a robar las credenciales de inicio de sesión, se esfuerzan mucho para que sus páginas se vean como las páginas de inicio de sesión con las que está familiarizado. Si encuentra dicho aviso de inicio de sesión, asegúrese de revisar la URL para asegurarse de que provenga del sitio del propietario legítimo. Si encuentra una ventana de estilo emergente, expanda la ventana para asegurarse de que la URL completa, o al menos el dominio completo, sea visible.

Asegúrese de que el correo electrónico parezca convincente. En el caso de estafas como extorsión digital y fraude de tarifa por anticipado, los remitentes suelen inventar historias elaboradas para intentar convencerlo de que el correo electrónico es legítimo. ¿Tiene sentido el escenario establecido? ¿Hay errores en sus historias, desde un punto de vista técnico, una perspectiva del proceso financiero u otro aspecto? Si es así, abórdela con escepticismo.



Prepárese

Hay muchas maneras diferentes en las que las amenazas de correo electrónico intentan engañarlo o inducirlo a responder, hacer clic en varias URL o abrir archivos adjuntos. Esto justifica el uso del software de seguridad de correo electrónico que puede capturar y poner en cuarentena correos electrónicos maliciosos y filtrar correos no deseados.

Desafortunadamente, hemos descubierto una tendencia preocupante: el porcentaje de organizaciones que utilizan la seguridad de correo electrónico está disminuyendo. De acuerdo con nuestro último [Estudio de referencia de CISQ](#), solo el 41 % de los encuestados actualmente utiliza la seguridad de correo electrónico como parte de sus defensas contra amenazas, incluso al reportarlo como el principal vector de amenazas que pone en riesgo a sus organizaciones. Esta cifra ha disminuido desde 2014, cuando el 56 % de las organizaciones utilizó la seguridad de correo electrónico.

Hay varias razones posibles para esta disminución. Una causa podría ser la transición a la nube. En un estudio reciente [realizado por ESG en nombre de Cisco](#), más del 80 % de los encuestados informó que su organización está utilizando servicios de correo electrónico basados en la nube. A medida que más y más organizaciones optan por que sus servicios de correo electrónico estén alojados en la nube, los dispositivos de correo electrónico específicos en el sitio parecen menos necesarios, y algunos equipos de TI asumen que pueden prescindir de ellos.

Sin embargo, si bien muchos servicios de correo electrónico en la nube proporcionan funciones de seguridad básicas, es fundamental contar con una protección en capas. De hecho, en la misma encuesta realizada por ESG, el 43 % de los encuestados descubrió que necesitaba seguridad adicional para defender su correo electrónico después de la transición. Al fin y al cabo, aún hay necesidades válidas para que los equipos de TI establezcan políticas, obtengan visibilidad y control, utilicen entornos de prueba y aprovechen las funcionalidades de bloqueo externo.

Otro problema que enfrentan los equipos de seguridad en la actualidad es una mayor superficie de ataque, lo que naturalmente da lugar a más áreas en las que se necesita protección. Si los presupuestos de seguridad no se han actualizado con respecto a este aumento, es posible que los equipos deban volver a escalar algunos recursos para cubrir la superficie de ataque más grande.

Dado que el correo electrónico es el vector de amenazas más común, se debe destacar la importancia de protegerlo. Al realizar cualquier evaluación de riesgo cibernético, es importante priorizar los puntos de entrada más críticos con sistemas de administración de riesgos y defensa completos, e ir bajando en orden de probabilidad de ataque y riesgo para la organización si se produce una violación. Luego, asigne recursos que se correspondan con la criticidad de las posibles pérdidas.

Asimismo, Gartner sugiere que la seguridad y los administradores de riesgos (SRMS) adopten un triple enfoque para mejorar sus defensas contra ataques de suplantación de identidad:

1. Actualice el gateway de correo electrónico seguro y otros controles para mejorar la protección de la suplantación de identidad.
2. Integre a los empleados en la solución y desarrolle funcionalidades para detectar y responder a los ataques sospechosos.
3. Trabaje con los gerentes de negocios para desarrollar procedimientos operativos estándares para el manejo de datos confidenciales y transacciones financieras.

Cómo proteger su correo electrónico

Hemos observado los indicios de un correo electrónico de suplantación de identidad y las estrategias de prevención de ataques. Ahora, analizaremos las expectativas de tecnología de seguridad de correo electrónico en 2019.

Al igual que en el pasado, un enfoque en capas a la seguridad es fundamental para defender su organización de ataques basados en correo electrónico. Existen varias capacidades de seguridad de correo electrónico comprobadas que, en la actualidad, continúan siendo importantes.



Por ejemplo:

- Aún debe mantenerse implementada una defensa contra el correo electrónico no deseado para evitar que estos correos maliciosos ingresen en las bandejas de entrada.
- La defensa contra amenazas de correo electrónico, como las funcionalidades de bloqueo de malware y URL, son vitales para bloquear malware, spear phishing, ransomware y criptominería en los adjuntos, junto con inteligencia de URL, para combatir enlaces maliciosos en correos electrónicos.
- El entorno de pruebas integrado debe ocurrir automáticamente en segundo plano para los nuevos archivos que llegan por correo electrónico para comprender rápidamente si son maliciosos.

Sin embargo, es muy importante destacar que el panorama de amenazas está en constante evolución y los agentes maliciosos están siempre buscando nuevas vías para lanzar ataques.

Además de las pruebas realizadas, las siguientes tecnologías de seguridad pueden ayudar a combatir este panorama en constante cambio:

- Han surgido más protecciones contra la suplantación de identidad avanzada mediante el aprendizaje automático para comprender y autenticar las identidades de correo electrónico y las relaciones de comportamiento para bloquear ataques de suplantación de identidad avanzada.

- Las protecciones de dominio de DMARC ahora se pueden activar para proteger la marca de una empresa evitando que los atacantes utilicen un dominio corporativo legítimo en campañas de suplantación de identidad.
- La funcionalidad de cuarentena de mensajes es útil para conservar un mensaje mientras se analiza un archivo adjunto antes de enviar un mensaje al destinatario, eliminar el adjunto malicioso o eliminar el mensaje por completo.
- La corrección de correo electrónico ayuda si se identifica un archivo como malicioso después de la entrega al destinatario, lo que le permite volver y colocar el mensaje en cuarentena con un adjunto malicioso desde un buzón de entrada.
- Las fuentes de amenazas por correo electrónico externas en STIX ahora son comúnmente utilizadas por productos de seguridad de correo electrónico, lo cual es útil si una organización desea utilizar una fuente de amenazas vertical más allá de la inteligencia de amenazas nativa en el producto.
- La integración de la seguridad de correo electrónico con portafolios de seguridad más amplios también se está volviendo común para comprender si el malware avanzado o los mensajes en un entorno pueden haberse entregado a usuarios o buzones de entrada en particular.

“Cisco es líder en el informe de Seguridad de correo electrónico empresarial de 2019 de Forrester Wave, y recibe las calificaciones más altas en opciones de implementación, protección contra ataques y autenticación de correo electrónico, rendimiento y operaciones (incluida la escalabilidad y la confiabilidad), y liderazgo en tecnología”.

The Forrester Wave™: Seguridad de correo electrónico empresarial, segundo trimestre de 2019

Acerca de la Serie de Ciberseguridad de Cisco

A lo largo de la última década, Cisco ha publicado una gran cantidad de información crucial de seguridad e inteligencia de amenazas para profesionales de seguridad interesados en el estado de la ciberseguridad global. Estos informes exhaustivos proporcionaron explicaciones detalladas de los panoramas de amenazas y las consecuencias para las organizaciones, así como mejores prácticas para defenderse frente a efectos adversos de violaciones de datos.

En nuestro nuevo enfoque de liderazgo intelectual, el departamento de seguridad de Cisco está realizando una serie de publicaciones basadas en investigaciones e impulsadas por datos bajo el banner: Serie de ciberseguridad de Cisco. Hemos ampliado el número de títulos para incluir diversos informes para profesionales de seguridad con intereses diferentes. Invocando la amplitud y profundidad de conocimientos de los investigadores de amenazas innovadores en el sector de seguridad, la recopilación previa de informes de la serie 2019 incluye el Reporte de referencia de privacidad de datos, el Reporte de amenazas, y el Reporte de referencia de CISO, pero vendrán otros más a lo largo del año.

Para más información y para acceder a todos los informes y las copias archivadas, visite www.cisco.com/mx/securityreports.



Sede central en América
Cisco Systems, Inc.
San Jose, CA

Sede central en Asia Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

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

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones y los números de teléfono y fax están disponibles en el sitio web de Cisco en www.cisco.com/go/offices.

Publicado en junio de 2019

THRT_02_0519_r1

© 2019 Cisco y/o sus filiales. Todos los derechos reservados.

Cisco y el logotipo de Cisco son marcas registradas o marcas comerciales de Cisco y/o de sus filiales en los Estados Unidos y otros países. Para ver una lista de las marcas comerciales de Cisco, visite: www.cisco.com/go/trademarks. Todas las marcas comerciales de terceros mencionadas en este documento pertenecen a sus respectivos propietarios. El uso de la palabra partner no implica la existencia de una asociación entre Cisco y cualquier otra compañía. (1110R)