proofpoint.

2020 Informe sobre amenazas en el sector de servicios financieros y de seguros

INTRODUCCIÓN

La pandemia mundial ha obligado a muchas empresas de servicios financieros y aseguradoras a acelerar su proceso de digitalización. Este proceso ha dado numerosos resultados positivos: una experiencia diaria más dinámica para los clientes remotos, una infraestructura reforzada para facilitar la ampliación del perímetro y medidas para adaptarse a los rápidos cambios en las necesidades de comunicación y cumplimiento de normativas. Aunque estos avances han ayudado a directivos bancarios, asesores patrimoniales, operadores y agentes a gestionar los flujos financieros y del mercado, también han abierto más oportunidades para los ciberdelincuentes.

Los ciberdelincuentes se aprovechan rápidamente de cualquier crisis social, y la COVID-19 no es ninguna excepción. A medida que el sector de servicios financieros y de seguros se desplaza fuera del perímetro de la red, también lo hacen los agresores. Pero las amenazas no solo se desplazan, también adoptan nuevas formas y objetivos. Todas las personas de su empresa representan un riesgo de incumplimiento o de seguridad diferente según los datos a los que tienen acceso y la forma de utilizar la tecnología para hacer su trabajo.

Para ayudar a los directivos de este sector a entender la evolución del panorama de amenazas, hemos analizado un año de datos, centrándonos en la primera mitad de 2020. El equipo de investigación sobre amenazas de Proofpoint ha estudiado miles de amenazas en millones de mensajes. Este informe describe nuestras conclusiones, y proporciona datos, ejemplos del mundo real y opiniones que arrojan luz sobre las amenazas que tienen como objetivo el sector de servicios financieros y de seguros.

Destinatarios y objetivo

Este informe va destinado a los directivos y ejecutivos de seguridad del sector de los servicios financieros y los seguros. Su propósito es ayudar a reducir el riesgo al que se enfrentan las empresas de este sector en relación con los datos de identificación personal, los datos financieros, la propiedad intelectual, la información no pública, los ecosistemas externos y el fraude. Además, está diseñado para ayudar con la formación de los empleados del sector con el fin de mejorar su nivel de concienciación en seguridad y protección.

Metodología de investigación

Esta investigación analiza una combinación de datos de Proofpoint sobre distintos ciberdelincuentes, campañas, ataques BEC y personas muy atacadas (VAP, Very attacked People™) en el cuarto trimestre de 2019 y la primera mitad de 2020. En algunos casos, utilizamos información obtenida de forma colaborativa para temas de seguridad incluidos en la investigación, pero no directamente observados en datos obtenidos de Proofpoint.

Índice

Resumen ejecutivo

El sector de servicios financieros y de seguros es un objetivo sistemático para los ciberdelincuentes, tanto si su motivación es el lucro, el hacktivismo o el terrorismo. Las reflexiones principales de este informe son:

El vector de ataque más frecuente son las personas, no las tecnologías.

Según la inteligencia de amenazas de Proofpoint, más del 96 % de todos los ataques se inician con técnicas de ingeniería social, pretexting, phishing y amenazas internas, aunque muchas organizaciones invierten gran parte de sus presupuestos en soluciones tecnológicas.

Basándonos en el análisis de Proofpoint de los indicadores de compromiso (IoC) y las tácticas, técnicas y procedimientos (TTP), es posible elaborar una lista de las personas más atacadas entre el total de población afectada, lo que permite adaptar la seguridad a esas amenazas específicas.

Los ciberdelincuentes responden rápidamente a los cambios del entorno.

El informe de Verizon sobre las investigaciones de fugas de datos de 2020 subraya que durante el último año se han duplicado los ataques basados en la nube, en consonancia con el aumento de teletrabajadores.

En el sector de los servicios financieros, los ciberdelincuentes diseñan estrategias muy precisas, emplean tácticas extremadamente metódicas y se informan a fondo sobre sus objetivos.

Los riesgos asociados a la cadena de suministro se controlan con dificultad pasado el segundo nivel.

La cadena de suministro de los servicios financieros es económicamente volátil en todo el mundo —más que en ningún otro sector—, ya que incluye bolsas de valores, cámaras de compensación/liquidación y bancos centrales con alcance internacional.

Es preciso actuar con diligencia, pero también ser consciente de los matices que presentan las necesidades de seguridad de una cadena de suministro. Si fuerza el cumplimiento de las medidas de seguridad de los proveedores de primer y segundo nivel a costa de rebajar imprudentemente los requisitos internos de su organización, puede crear brechas de seguridad con ese proveedor o impedir que este le atienda correctamente.

Cada subsector tiene matices exclusivos de su panorama de amenazas.

Los datos de inteligencia sobre amenazas de Proofpoint y de los informes independientes indican variaciones en los IoC y los TTP de cada subsector, por lo que la defensa debería personalizarse por subsectores.

Las criptomonedas están a la vuelta de la esquina.

La Oficina del Contralor de la Moneda (OCC, por sus siglas en inglés) de EE. UU. acaba de publicar un comunicado por el que autoriza a las entidades bancarias a custodiar claves digitales de criptomonederos.

Si a los bancos se les permite custodiar legalmente activos digitales de sus clientes, las responsabilidades legales y los riesgos de ciberseguridad de esas criptomonedas se trasladan a los bancos custodios.

Métricas de amenazas y seguridad en los servicios financieros y los seguros

El sector de servicios financieros tiene varias características que prácticamente no se dan en ningún otro y que atraen a los ciberdelincuentes como abejas a la miel:

ALTA RECOMPENSA

La rentabilidad de abrir una brecha en una empresa de servicios financieros es más elevada que en otros sectores, sencillamente porque es el sector que maneja el dinero.

GRAN IMPACTO

Sea cual sea su tamaño, una brecha de seguridad puede saltar a los titulares, provocar una reacción en el mercado y desencadenar un efecto multiplicador que podría extrapolarse de una empresa aislada a toda la economía mundial.

REGULACIÓN

Cuando hay que cumplir con procesos y procedimientos normativos bien definidos, el adversario necesita menos esfuerzos de reconocimiento específicos.

TECNOLOGÍA TRADICIONAL

Al utilizar en gran medida tecnología informática anticuada, el riesgo de seguridad se genera cuando el fabricante interrumpe el soporte técnico, se acumulan sistemas patentados por las distintas fusiones y adquisiciones, hay sistemas que se consideran "demasiado importantes para actualizarlos" y se pierde la experiencia en el uso de los sistemas antiguos.

AMALGAMA DE INFRAESTRUCTURAS

Se trata de un sector históricamente activo en fusiones y adquisiciones, lo que genera complejidad y opacidad. Las integraciones mal ensambladas entre sistemas diferentes crean una infraestructura dividida que ofrece superficies de ataque más grandes e incrementa la presión sobre los recursos de supervisión y defensa de la seguridad.

TECNOLOGÍA EN CLOUD/CONTENEDORES

Cuando se suben las aplicaciones existentes a la nube (o a contenedores), pueden ponerse de manifiesto vulnerabilidades antes desconocidas o aparecer vulnerabilidades nuevas debidas al paradigma de despliegue. La contratación de nuevos proveedores de SaaS para el traspaso de los sistemas no críticos puede crear una nueva superficie de ataque donde la capacidad para gestionar incidentes está gravemente limitada.

AUTOMATIZACIÓN GENERALIZADA

Las organizaciones de este sector cada vez recurren más a la automatización para reducir costes y modernizar los sistemas antiguos. Sin embargo, la expansión de la automatización provoca fragilidad si la empresa depende de esos sistemas tradicionales, la transición introduce más complejidad en la lógica empresarial o no se documenta el proceso.

Hay datos estadísticos significativos propios de este sector en relación con la prevención contra la seguridad, las amenazas emergentes y los ataques persistentes:

Formación para concienciar en materia de seguridad

Las empresas del sector de servicios financieros y de seguros son ligeramente más conscientes de las amenazas internas y de autenticación de cuentas que en otros sectores.

- Los servicios financieros registran una tasa de fallos del 20 % en comparación con la media de la población, que alcanza el 22 %.
- Los servicios financieros obtuvieron una buena puntuación en "Identificar y prevenir amenazas internas" y en "Autenticación de cuentas".
- Los servicios financieros obtuvieron una mala puntuación únicamente en "Protección frente a riesgos físicos" y en "Evitar ataques de ransomware".

Amenazas del correo electrónico

Las amenazas a través de URL alcanzaron sistemáticamente cifras más elevadas que las procedentes de adjuntos del correo electrónico.

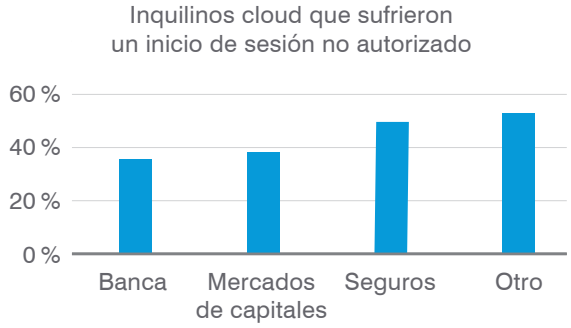
- El 82 % de los mensajes maliciosos de todo el sector de servicios financieros contenían URL.
- El 72 % de los ataques estaban basados en malware.

Acceso a cloud

Las tácticas de ingeniería social dirigidas contra el acceso a cloud registran una impresionante *tasa de éxito del 75 %*, mientras que la fuerza bruta solo funciona aproximadamente el 9,7 % de las veces. Está claro que los ataques centrados en las personas son los que presentan una rentabilidad más prometedora para los ciberdelincuentes.

El sector de seguros experimentó más inicios de sesión no autorizados que la banca y los mercados de capitales.

- En el 72 % de los casos, se trató de ataques con métodos de fuerza bruta, pero estos ataques solo tuvieron éxito el 7 % de las veces.
- En el 28 % de los casos, se trató de ataques con métodos de ingeniería social. En el 21 % de los casos, el ataque logró comprometer con éxito a las víctimas con métodos de phishing.



Prevención de pérdida de datos (DLP) y amenazas internas

Cada subsector del sector de servicios financieros y de seguros tiene sus propios índices de amenazas internas. En un estudio de incidentes internos en el periodo comprendido entre 1996 y 2018, la banca fue con diferencia el sector más afectado[1].

Segmento	Grupos	Riesgos de amenazas internas	N.º de incidentes internos[2]
Banca	Ahorro, crédito, financiación	Información de identificación personal, usurpación de cuentas	190
Mercados de capitales	Banca de inversiones, gestión de activos	Propiedad intelectual, fusiones y adquisiciones, tráfico de influencias	no hay datos disponibles
Seguros	Tarificación de riesgos, inmobiliarios y accidentes	Información de identificación personal, fraude en seguros	14
Ecosistema	Bolsas de valores, servicios de liquidación, datos de mercado, nube/SaaS, cadena de suministro	Prevención de blanqueo de capitales, contraparte, SWIFT, ACH, manipulación del mercado	33

TTP utilizados en incidentes internos en los servicios financieros

El CERT, en colaboración con el DHS y el USSS, investigó los incidentes internos ocurridos entre 2005 y 2012 para responder a la pregunta: "¿Cuáles son los precursores técnicos y conductuales observables del fraude interno en el sector financiero y, como resultado, qué estrategias de mitigación deben contemplarse?"[3]. Entre sus principales conclusiones figuran las siguientes:

La estrategia "low and slow" (lentos y de baja intensidad) hizo más daño y eludió la detección durante más tiempo.

Las soluciones tecnológicas orientadas a las anomalías no solo fueron ineficaces, sino también contraproducentes, porque estas actividades maliciosas a largo plazo se convirtieron en parte de las actividades básicas de los usuarios.

Los medios de los usuarios internos no eran sofisticados técnicamente.

La falta de sofisticación significa que los datos de sensores existentes pueden utilizarse en el programa de detección de amenazas internas. Por supuesto, el truco está en el análisis del comportamiento.

El fraude llevado a cabo por directivos difiere considerablemente en daño y duración del fraude que cometen empleados de menor grado.

Los directivos están facultados para modificar procesos empresariales, a veces manipulando a subordinados, para beneficiarse económicamente. Cuando se trata de personas de menor grado en el escalafón, a menudo son representantes del servicio al cliente que modifican cuentas o roban información de identificación personal en su propio beneficio.

La mayoría de los incidentes se detectaron a raíz de una auditoría, la queja de un cliente o la sospecha de un trabajador.

Esta es una observación importante: así como las intrusiones externas dejan un rastro de anomalías, las amenazas internas se alimentan de sentimientos, motivaciones y formas de pensar, elementos que la tecnología no detecta fácilmente.

El zorro, guardián del gallinero

En ocasiones, la amenaza interna procede de la agencia designada para disuadir e investigar amenazas internas. En 2019, un antiguo examinador de cumplimiento de valores de la SEC fue acusado de acceder a la información de una investigación pendiente sobre una firma de capital riesgo y de utilizar esa información para obtener el puesto de director de cumplimiento de esa misma firma[4]. El hecho de que esta persona procediera de un puesto relacionado con el cumplimiento normativo —y ascendiera a otro— no solamente es irónico, sino que demuestra que la ética no es ningún impedimento para las amenazas internas.

[1] Miller y Trotman (2018), "*Insider Threats in Finance and Insurance (Part 4 of 9: Insider Threats Across Industry Sectors)" (Las amenazas internas en finanzas y seguros [Parte 4 de 9: Las amenazas internas en los sectores industriales]),* CMU SEI

[2] Ibid.

[3] Cummings, Lewellen, McIntire, Moore y Trzeciak (2012), "*Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector*" (Estudio sobre las amenazas internas: ciberactividad ilícita con fraude en el sector de servicios financieros estadounidense), CMU SEI, DHS S&T, USSS y Centro de Amenazas Internas del CERT

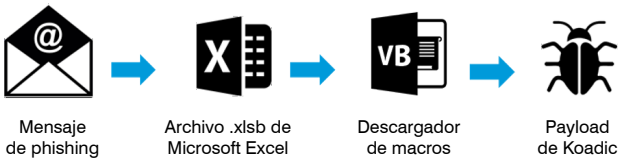
[4] Godoy y Lorenzo (2019), "Ex-SEC Compliance Expert Denies Pilfering Info For PE Firm" (Antiguo experto en cumplimiento de la SEC niega haber robado información para una firma de capital riesgo), Law360

Tácticas frecuentes en los ataques al sector

La inteligencia de amenazas de Proofpoint ha observado que los ciberdelincuentes utilizan cada vez con más frecuencia varias tácticas concretas:

"VBA stomping"

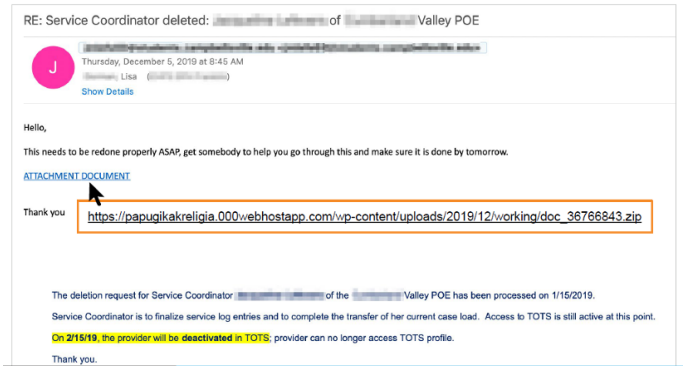
Esta técnica basada en adjuntos maliciosos presenta a los motores de análisis de seguridad un código VBA (ejecutable) diferente del que se ejecuta en realidad, con lo que elude muchas herramientas de detección heurística y firmas de código.



Secuestro de hilos de discusión

Esta técnica BEC (business email compromise) capta muchas víctimas inyectando contenido falso (por ejemplo, URL maliciosas) en un hilo existente de correo electrónico. Las conversaciones de correo electrónico existentes despiertan cierto grado de confianza y por eso numerosas víctimas están más dispuestas a abrirlas y a hacer clic en los enlaces que contienen.

Otra táctica utilizada por esta técnica es incrustar URL maliciosas en la sección "mensaje original" del mensaje de correo electrónico, a partir de la cual muchas herramientas de seguridad del correo electrónico dejan de analizar; de este modo, una vez más, el malware elude muchas herramientas de detección heurística.


RE: Service Coordinator deleted: [redacted] of [redacted] Valley POE

[redacted]

Thursday, December 5, 2019 at 8:45 AM

[redacted] Lisa [redacted]

Show Details

Hello,

This needs to be redone properly ASAP, get somebody to help you go through this and make sure it is done by tomorrow.

ATTACHMENT DOCUMENT

Thank you https://papugikakreligia.000webhostapp.com/wp-content/uploads/2019/12/working/doc_36766843.zip

The deletion request for Service Coordinator [redacted] of the [redacted] Valley POE has been processed on 1/15/2019.

Service Coordinator is to finalize service log entries and to complete the transfer of her current case load. Access to TOTS is still active at this point.

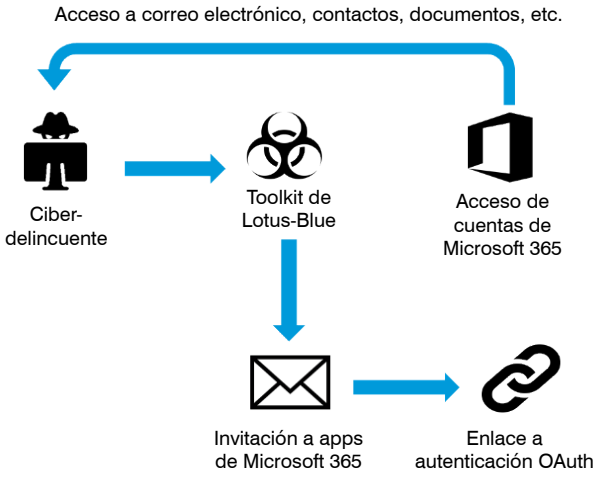
On 2/15/19, the provider will be deactivated in TOTS; provider can no longer access TOTS profile.

Thank you.

En el caso de Emotet, el malware más prolífico de los dos últimos años, en realidad los ciberdelincuentes automatizaron el proceso de creación de plantillas para utilizar esta técnica a una escala increíble y eliminar el análisis directo y personalizado que normalmente exigiría.

Autenticación de terceros maliciosos (3PA)

Esta técnica de usurpación de cuentas utiliza la clásica distorsión de DNS para convencer a los usuarios de que otorguen permisos basados en un token SAML para acceder a las aplicaciones de un usuario en la nube (como Microsoft 365, Google Workspace y otras). Normalmente, empieza como un BEC y rápidamente se transforma en un EAC (compromiso de cuentas de correo electrónico). Al disponer de acceso a la cuenta de correo electrónico del usuario, es posible cambiar las contraseñas de otras aplicaciones y usurpar la cuenta por completo.



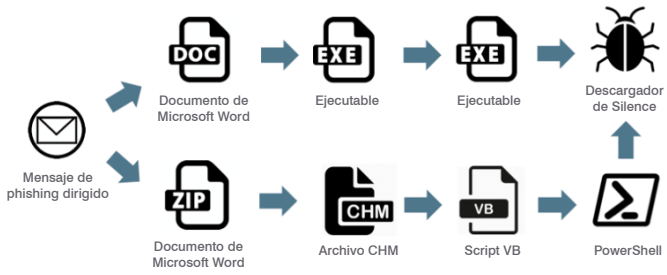
El motivo por el que este tipo de usurpación es más nefasta que otras es que, una vez que la cuenta está comprometida, no sirve de nada modificar la contraseña ni utilizar la autenticación multifactor. La única manera de impedir el acceso del ciberdelincuente es eliminar expresamente los permisos de token, un proceso que desconoce la mayoría de los usuarios finales.

Ataque multicapa a recursos compartidos de archivos

Esta técnica presenta un documento alojado que a su vez señala a varias capas de URL, ubicadas en diferentes recursos compartidos de archivos, que al final terminan en una carga maliciosa distribuida con malware.

La frecuencia con que los servicios financieros utilizan los recursos compartidos de archivos en la nube (y la autenticación de terceros) ha incrementado el uso de esta técnica.

Por ejemplo, una carga maliciosa (un script VB que distribuye Ursnif, un troyano bancario incrustado) se protege (cifra) con la contraseña que se indica en el cuerpo del mensaje del correo electrónico.



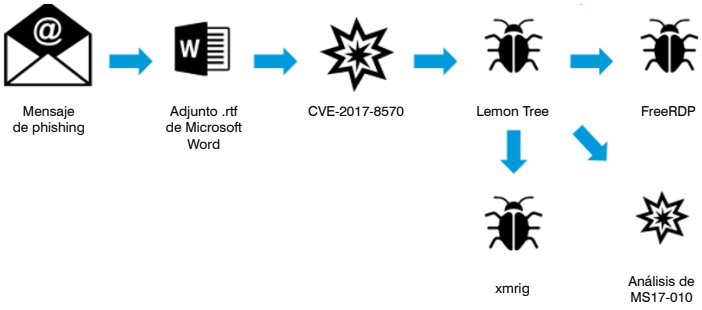
Por un lado, parece contraproducente añadir pasos, como obligar a la víctima elegida a introducir una contraseña, ya que, cuantos más pasos sean necesarios, mayor será la probabilidad de que el usuario cometa algún error o abandone antes de llegar al final.

Por el otro, así se evita el análisis directo del archivo adjunto. Las soluciones han tenido que implementar técnicas que consisten en incluir un diccionario creciente de contraseñas utilizadas habitualmente (los ciberdelincuentes quieren que sean sencillas por el motivo ya mencionado y no las cambian para cada campaña) o en analizar los cuerpos de los mensajes (algo difícil de hacer a gran escala).

Hemos visto casos donde la contraseña era en realidad una imagen en lugar de texto, por lo que aquí no funcionaría este último método de analizar en busca de contraseñas de texto.

Ataques "Living-Off-the-Land" (sin archivos/sin servidor)

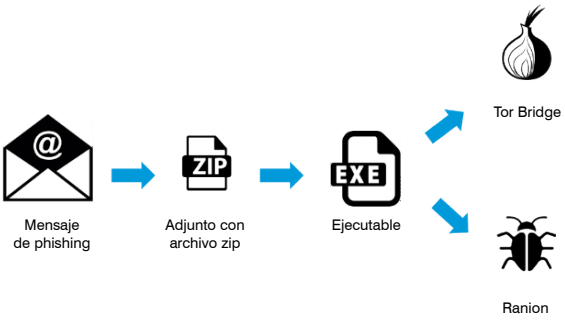
Esta técnica de ataque utiliza funciones existentes del sistema operativo de la víctima, como PowerShell, para ejecutar su carga maliciosa. La carga en sí no es binaria, así que puede sortear los métodos de firmas y de detección heurística.



Ransomware como servicio (RaaS)

Las plataformas de ransomware se han generalizado en la misma medida que otras muchas plataformas de ataque.

Los proveedores de plataformas de ransomware han migrado a un servicio de suscripción y ya no se llevan un porcentaje del pago; esto no solo hace el RaaS más atractivo que otras plataformas, sino que además logra que los proveedores dejen de ser considerados indebidamente responsables directos de un hecho delictivo. (Imaginemos la cantidad de demandas de culpabilidad directa que se interpondrían contra los fabricantes de armas si cobraran una cuota por cada bala disparada).



Las nuevas iteraciones de este servicio incluyen la instalación automática de clientes TOR en el ordenador de las víctimas, lo que facilita que estas paguen el rescate.

Perspectivas sobre el sector de servicios financieros

Banca

El sector bancario es el que ha experimentado más innovación y progreso en los últimos años, desde la llegada de las transacciones móviles y los servicios habilitados por API hasta el uso del procesamiento basado en inteligencia artificial. Con las nuevas tecnologías llegan nuevos métodos de ataque, pero las motivaciones y los objetivos de los ciberdelincuentes en el sector bancario son los mismos. De hecho, Accenture calcula que el riesgo para el sector bancario asciende a 347 000 millones de dólares[5].

VISTA RÁPIDA: ESPECIFICIDADES DEL SECTOR BANCARIO	
VAP:	**Phishing general**: • Equipo de tecnología • Ejecutivo **Ataques BEC (business email compromise) dirigidos:** • Director de relaciones • Relaciones con los inversores/asesores financieros • Desarrollo comercial
Objetivos:	• Clientes (directo) • Empleados (directo) • Clientes (indirecto): personal con acceso a datos/sistemas del cliente • Empleados (indirecto): personal con acceso a datos/sistemas de Recursos Humanos (RR. HH.)
Finalidades:	• Pérdida económica del cliente

Banca: ataques dirigidos

La inteligencia de amenazas de Proofpoint ha identificado ataques dirigidos a un solo cargo o banco, lo que implica la elección de objetivos muy precisos y el uso de técnicas de reconocimiento específicas para cada empresa.

Grandes entidades bancarias

Comentarios de los analistas: una entidad bancaria del Fortune 100 recibió 12 mensajes (100 %) que utilizaban una técnica nueva denominada WhiteShadow[6] para desplegar un conjunto de malware desconocido. Esto es interesante por dos razones.

El hecho de que el malware no esté identificado podría indicar que esta firma es simplemente una víctima de prueba para un ataque sistémico mayor.

WhiteShadow suele utilizarse para desplegar Crimson, un troyano de acceso remoto (RAT, Remote Access Trojan) identificado por primera vez en 2016 como la payload que utiliza un autor de amenazas persistentes avanzadas (APT) con conexiones pakistaníes denominado "Transparent Tribe"[7]. Desde entonces, el RAT Crimson se ha generalizado entre varios ciberdelincuentes, pero la inteligencia de amenazas de Proofpoint ha recibido múltiples consultas de entidades bancarias sobre si la cadena de ataque de WhiteShadow a Crimson podría seguir siendo una actividad patrocinada por algún Estado.

Las instancias de la técnica WhiteShadow que, aparte de Crimson, distribuyen malware adicional desde una infraestructura que no tiene vínculos explícitos con la red pakistaní refuerzan la idea de que está aumentando la adopción de esta técnica y las cargas maliciosas asociadas.

Cooperativas de ahorro: ataque de la cadena de suministro

Comentarios de los analistas: una cooperativa de ahorro y crédito recibió 67 mensajes (87 %) y varias empresas de contabilidad de la región recibieron los mismos mensajes. Cualquier relación entre la cooperativa de ahorro y estas empresas podría indicar un ataque de canal lateral o de cadena de suministro.

La cadena de payload de GuLoader QuasarRAT es bastante corriente, pero constituye un ejemplo del cambio en las TTP experimentado a gran escala en todo el panorama de amenazas en los dos últimos años. Ahora el objetivo es únicamente conseguir introducirse para desplegar cargas maliciosas adicionales. Además, al ser código abierto, QuasarRAT ofrece a los ciberdelincuentes sofisticados un medio para complicar la atribución; por ejemplo, si un autor puede introducirse en un sistema con un software genérico o de uso frecuente, es más difícil averiguar quién ha iniciado el ataque en realidad. Si la intrusión tiene éxito, con esta técnica el autor puede desplegar una segunda carga maliciosa después de reconocer el terreno.

[5] Accenture (2020), "The State of Cybercrime in Banking and Capital Markets" (El estado de la ciberdelincuencia en la banca y los mercados de capitales)
[6] https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware
[7] https://www.proofpoint.com/us/threat-insight/post/Operation-Transparent-Tribe

Banca: análisis y tendencias de amenazas

Durante un periodo de seis meses, desde el cuarto trimestre de 2019 hasta el segundo trimestre de 2020, la inteligencia de amenazas de Proofpoint ha llevado el seguimiento de las amenazas que atacan constantemente al subsector bancario, mostradas en la Figura 1.

Transferencias bancarias

Comentarios de los analistas: este es un caso en el que la banca comercial recibe casi el doble de mensajes que el siguiente sector de la línea, aunque reciben mensajes todos los clientes de inversión financiera, servicios de transacción financiera y el ecosistema de las finanzas. Los mensajes se distribuyen bastante uniformemente entre muchas instituciones y regiones, en lugar de concentrarse en su mayoría en un solo cliente y enviar el resto a unos cuantos clientes similares. El engaño en sí consiste en suplantar la identidad de Western Union en una transferencia de dinero, indicar el cumplimiento de normativas como asunto y distribuir un RAT.

Otras campañas notables

Bot de TeamViewer (MINEBRIDGE) | Documentos de Word | "Indeed Application: Full Time Teller" (Solicitud de empleo en Indeed: cajero a tiempo completo)
Mensajes generalizados a servicios financieros que simulan ser una solicitud de empleo de cajero a tiempo completo procedente de una compañía de contratación falsa.

GuLoader / "warii" Parallax | Archivos adjuntos | "MAJ Code Banques" (Actualización de códigos de entidad)
Los mensajes llevan archivos adjuntos de Microsoft Office con macros que, cuando se activan, descargan y ejecutan GuLoader; este a su vez descarga e instala Parallax. Las principales víctimas fueron las empresas de banca y de servicios.

jSocket "88.150.189[.]98" | URL | "Tax return" (Declaración fiscal)
Estos mensajes contienen URL que conducen a un archivo Java comprimido. Casi todos los mensajes se enviaron a una entidad bancaria.

Get2 / SDBbot | Documentos de Excel
Los mensajes de correo electrónico llevan archivos adjuntos de Microsoft Excel con macros que, si se activan, ejecutan una DLL incrustada (malware cargador "Get2"). Get2 descarga SDBbot y malware desconocido. El objetivo principal fue la banca. El 76 % de los mensajes de esta campaña se dirigió al sector de servicios financieros. En diciembre de 2018 y enero de 2019 se detectaron ataques de esta campaña dirigidos contra entidades bancarias. Las entidades bancarias continuaron siendo blanco frecuente.

URL | Documentos de Word | PDF
Los Estados Unidos son objetivo de ataques con mensajes de correo electrónico que contienen URL, documentos de Word o archivos PDF. Los PDF hacen un uso ilícito del nombre de muchos bancos del Fortune 100. Varios servicios financieros reciben mensajes cuyo remitente suplanta a un minorista y cuyo asunto alude a un supuesto pago.

CobInt | Grupo Cobalt | URL
Los mensajes contienen enlaces a un archivo PDF alojado en Microsoft OneDrive. El PDF incluye enlaces que conducen a la descarga de "Documents.rtf". El documento contiene exploits que, si tienen éxito, descargan CobInt. En Estados Unidos, varios empleados recibieron el malware CobInt, que forma parte de las familias de ataques de puerta trasera y descargadores. Este ataque procedía de un ciberdelincuente conocido que suele atacar a entidades bancarias y crediticias, así como a empresas del sector de medios de comunicación y entretenimiento. En este caso, más del 50 % de los mensajes se enviaron a empleados del sector de servicios financieros, lo que convierte a este grupo en el mayor objetivo.

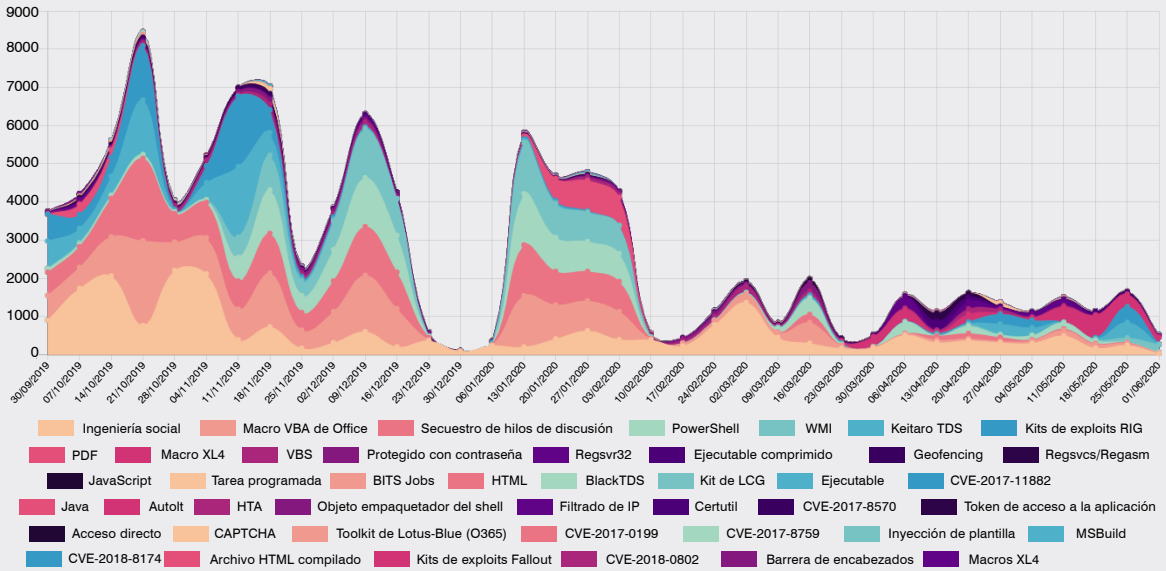


Figura 1: Instituciones de ahorro: exploits dirigidos (fuente: Proofpoint).

Mercados de capitales

Accenture calcula que, en los mercados de capitales, el riesgo derivado de ciberataques asciende a 47 000 millones de dólares[8].

VISTA RÁPIDA: ESPECIFICIDADES DEL SECTOR DE MERCADOS DE CAPITALES	
VAP:	**Phishing general**: • Equipo de tecnología • Partner ejecutivo/directivo **Ataques BEC dirigidos:** • Asesores financieros/analistas • Gestor de fondos/cartera • Director de investigación
Objetivos:	• Dinero/activos (directo): personal con acceso a activos • Clientes (indirecto): personal con acceso a datos/sistemas del cliente
Finalidades:	• Alteración del sector • Alteración del merado/economía

Mercados de capitales: ataques dirigidos

La inteligencia de amenazas de Proofpoint ha identificado ataques dirigidos a un solo cargo o empresa del mercado de capitales, lo que implica la elección de objetivos muy precisos y el uso de técnicas de reconocimiento específicas para cada empresa.

Posiblemente, las cargas maliciosas ocultas son en realidad la vanguardia

Aunque en estos ataques en particular se utilizaron señuelos sencillos, como facturas de envío, seguimiento de paquetes y cuestiones fiscales, la novedad aquí es la carga maliciosa que depende de NodeJS para ejecutarse. NodeJS es un popular entorno de ejecución para servidores y hosts web, por lo que sería lógico concluir que la carga maliciosa no se ejecutaría si se descargara en un endpoint local.

Y aquí es donde la cosa se pone interesante: hay varios marcos de desarrollo de aplicaciones que utilizan un despliegue local de NodeJS[9]. Aunque la mayoría de las aplicaciones financieras compiladas en estas plataformas están orientadas a las criptomonedas, hay varias aplicaciones de código abierto y freeware para notificación de seguimiento de acciones de bolsa, análisis de datos financieros y plataformas de operaciones bursátiles abiertas (que con gran probabilidad utilizan las firmas de corretaje atacadas)[10].

Mercados de capitales: análisis y tendencias de amenazas

El sector de inversiones financieras es el más atacado, con un 31 % de mensajes y un 23 % de clientes. Cabe notar que muestra cierta similitud con la banca comercial.

Durante un periodo de seis meses, desde el cuarto trimestre de 2019 hasta el segundo trimestre de 2020, la inteligencia de amenazas de Proofpoint ha llevado el seguimiento de las siguientes amenazas que atacan constantemente al subsector de los mercados de capitales (véase la Figura 2).

[8] Accenture (2020), "The State of Cybercrime in Banking and Capital Markets" (El estado de la ciberdelincuencia en la banca y los mercados de capitales)

[9] https://brainhub.eu/blog/javascript-frameworks-for-desktop-apps/

[10] https://www.electronjs.org/apps?category=finance

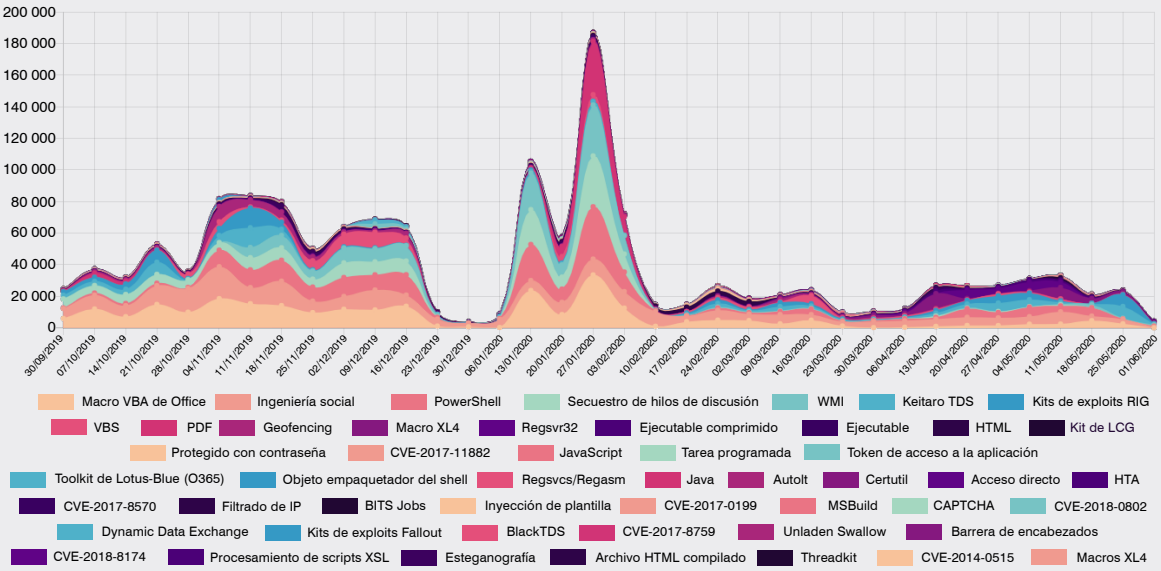


Figura 2: Sociedades de valores: exploits dirigidos (fuente: Proofpoint).

Tendencia de los ataques por regiones

Comentarios de los analistas: al inspeccionar los 20 bancos de inversiones más importantes del mundo —que tienen su sede en Estados Unidos y cuya plantilla sería de esperar que trabajara en su mayoría en Londres y Nueva York—, las 50 VAP de casi todas las empresas se encontraban en Singapur, China o Japón.

Quizá esto se deba al repunte de nuevas contrataciones en APAC, en concreto para responder al renovado interés por invertir en los países de esta región. "Los bancos han constatado que las empresas estatales chinas desempeñaron un papel fundamental para hacer negocios en 2020 y prevén grandes salidas al mercado primario [...] para estimular la actividad de los mercados de capitales"[11].

Otras campañas notables

QuasarRAT | HTML | "IRS correspondence Notices"

Los mensajes de correo electrónico con el asunto "IRS correspondence Notices" (Notificación fiscal) contienen un adjunto HTML comprimido. Si se abre, el adjunto descarga un documento de Word incrustado. El documento utiliza macros para descargar un VBscript que, a su vez, descarga QuasarRAT. El único blanco de esta campaña fueron los mercados de capitales (inversiones y valores).

Seguros

El sector de seguros está clasificado como subsector del sector de servicios financieros, ya que se basa en la gestión fiduciaria de fondos que deben estar disponibles en caso de desastre. Sin embargo, el sector de las aseguradoras es muy diferente de otros subsectores porque sus principales riesgos proceden de acontecimientos externos.

Dada esta abundancia de objetivos maliciosos posibles, es importante prestar atención no solo a qué personas de la empresa son objeto de ataque, sino a por qué las eligen como blanco.

VISTA RÁPIDA: ESPECIFICIDADES DEL SECTOR DE SEGUROS

VAP:	**Phishing general**: • Equipo de tecnología • Ejecutivo • Recursos Humanos/Reclutador **Ataques BEC dirigidos:** • Agente de seguros/Responsable de cuenta • Director de programa/plan (planes de jubilación, prestaciones colectivas, etc.)

Además, el informe de la inteligencia de amenazas de Proofpoint indica que en el subsector de seguros se produjeron con éxito más inicios de sesión de inquilinos cloud no autorizados que en la banca y los mercados de capitales.

Esto puede deberse a que las compañías de seguros utilizan más tecnologías de big data e inteligencia artificial[12], algo que solo puede ser rentable mediante despliegues cloud[13]. O quizá se deba a la continua optimización del coste de las operaciones con el uso de la automatización robótica de procesos (RPA), la externalización de operaciones básicas o la migración de datos y operaciones a la nube[14].

[11] Chatterjee, Murdoch (2020), "Exclusive: Bank of America to hire 50 bankers for Asia dealmaking team in 2020—sources" (Exclusiva: el Bank of America contratará a 50 banqueros en 2020 para su equipo de intermediarios en Asia), Reuters

[12] Oliver (2019), "Insurance sector prepares for disruption" (El sector de seguros se prepara para el trastorno), Financial Times

[13] Thomson (2020), "Are Insurers' Confidence in their Cyber Defense Exposing Them to Revenue Losses?" (¿Provoca pérdidas de ingresos la confianza de las aseguradoras en sus ciberdefensas?) Accenture

[14] Deloitte (2020), "Deloitte Insights—2020 Insurance Outlook" (Perspectivas sobre el sector de seguros)

Seguros: ataques dirigidos

La inteligencia de amenazas de Proofpoint ha identificado ataques dirigidos a un solo cargo o aseguradora, lo que implica la elección de objetivos muy precisos y el uso de técnicas de reconocimiento específicas para cada empresa.

La franquicia de TrickBot

Comentarios de los analistas: en términos generales, cuanto mayor es una campaña en volumen general de mensajes y número de clientes destinatarios (difusión), menos probable es que se trate de una campaña dirigida. En el sector de seguros, estamos apreciando una concentración muy alta de grupos de clientes en una sola campaña.

En este caso, 21 de 26 organizaciones destinatarias (81 %) pertenecían al sector de seguros y el 96 % de todos los mensajes se dirigieron al cliente de una aseguradora. La mayoría de los mensajes se dirigieron específicamente a una compañía de seguros concreta, pero no es casualidad que los otros 25 clientes que recibieron menos mensajes perteneciesen al mismo sector. Normalmente, la distribución de sectores afectados está más diversificada, pero el de seguros se incluye de forma habitual entre un 10 y un 13 % de los casos, cuando el sector más atacado quizá recibe solo entre el 16 y el 18 % de los mensajes.

La carga del malware propiamente dicha se basa en uno de los troyanos de banca más destacados: los operadores ejecutan su red de bots con un modelo de afiliación. Para entender lo generalizados que están los TTP, veamos cómo funciona esta amenaza. Un ciberdelincuente se hace cliente de los operadores de TrickBot y recibe una "etiqueta de grupo" diferenciadora, en este caso "yas24", donde el código de tres letras denota la campaña/subgrupo/afiliado responsable de la infección. El número tiende a ser iterativo, ya que el grupo continúa distribuyendo el malware.

Seguros: análisis y tendencias de amenazas

Durante un periodo de seis meses, desde el cuarto trimestre de 2019 hasta el segundo trimestre de 2020, la inteligencia de amenazas de Proofpoint ha llevado el seguimiento de las amenazas que atacan constantemente al subsector de seguros (véase la Figura 3).

AZORult | "daffy"

Los mensajes de correo electrónico con el asunto "Mail Report From support@WellsFargo.com" (Informe de correo de support@WellsFargo.com) llevan un archivo adjunto de Microsoft Word denominado "purchase order nl5753637.doc" (pedido de compra nl5753637.doc) que aprovecha la vulnerabilidad CVE-2017-8570. Si se abre, el adjunto descarga y ejecuta AZORult (también conocido como "daffy.exe"). Aunque solo comprende al 18 % de los clientes controlados por nuestro equipo, el sector de seguros recibe el 85 % de los mensajes.

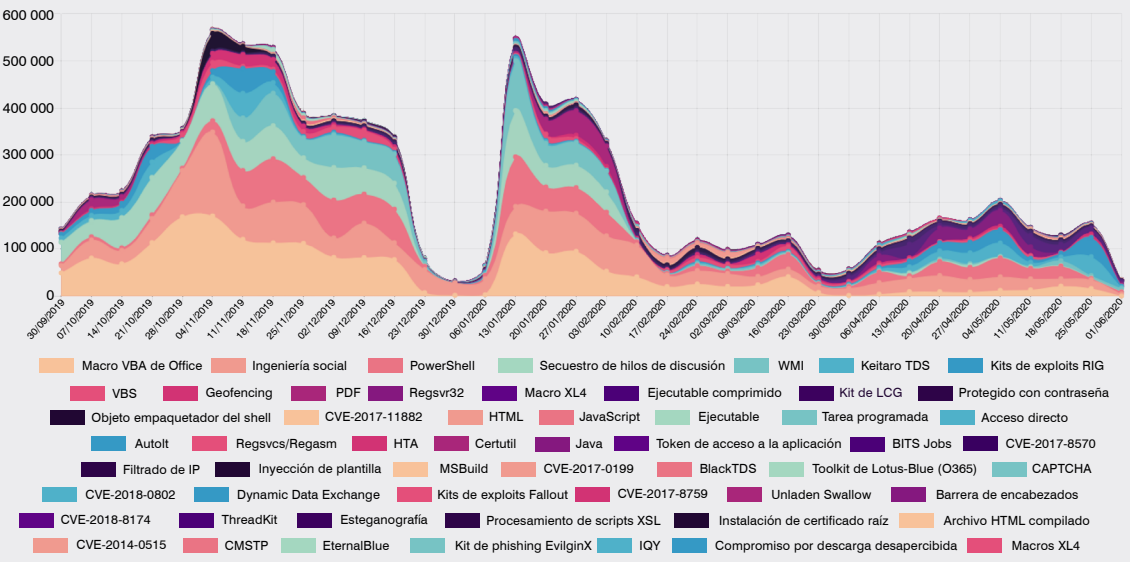


Figura 3: Seguros: exploits dirigidos (fuente: Proofpoint).

Conclusiones y recomendaciones

La ciberseguridad en el sector de servicios financieros y de seguros no solo debe tener en cuenta las superficies de ataque externas, sino también las brechas de seguridad que se crean al intentar optimizar procesos y tecnologías internamente. El objetivo de los ciberataques actuales no es la tecnología; son las personas. Explotan el "factor humano" de las empresas modernas de servicios financieros y de seguros: el deseo de ayudar a los clientes a conseguir sus objetivos y de ser un motor de oportunidades. La pandemia mundial ha obligado a muchas empresas de servicios financieros y aseguradoras a acelerar la digitalización para mejorar la gestión omnicanal de la relación con el cliente, la asistencia y la venta de soluciones. Aunque simultáneamente intentan afianzar y mejorar la eficacia del personal que trabaja de forma remota, nunca ha sido tan complejo ni tan esencial garantizar la seguridad y la conformidad de la información. En la actualidad las amenazas para el sector de servicios financieros y de seguros y los riesgos de incumplimiento normativo requieren un enfoque nuevo centrado en las personas.

Estas son nuestras recomendaciones para las empresas del sector:

- **Adopte una estrategia de seguridad centrada en las personas.** Los atacantes no ven el mundo como un diagrama de red. Su objetivo son las personas. Despliegue una solución que le permita ver a quién se dirige el ataque, cómo actúa y si la víctima ha hecho clic en un enlace malicioso. Considere el riesgo concreto que presenta cada usuario. Una solución centrada en las personas le mostrará cómo se ataca a sus empleados, los datos a los que tienen acceso y si son propensos a caer en las trampas de los atacantes.
- **Use los datos de su programa centrado en las personas para planificar y recibir financiación para sus programas de seguridad.** Estos datos le servirán para explicar a los directivos y ejecutivos sus prioridades y sus programas destinados a reducir el perfil de riesgo de la empresa. Utilice también los datos para explicar a sus compañeros los motivos de su programa y para que puedan defenderse ellos y a la empresa.
- **Forme a los usuarios para que detecten y denuncien si hay correo electrónico malicioso.** La formación periódica y los ataques simulados pueden reducir el riesgo de dos formas fundamentales. En primer lugar, dotan a los usuarios de lo que necesitan para detener muchos ataques. En segundo lugar, ayudan a descubrir qué usuarios pueden ser particularmente vulnerables. Las mejores simulaciones imitan las técnicas de ataque del mundo real. Considere soluciones que aborden las tendencias de ataque actuales al sector de servicios financieros y de seguros y que incorporen lo último en inteligencia sobre amenazas. Cuando los usuarios denuncian mensajes sospechosos, la automatización puede ayudar a verificar y resolver las amenazas verdaderas.
- **Al mismo tiempo, dé por hecho que en algún momento los usuarios harán clic en un enlace.** Los atacantes siempre encontrarán nuevas formas de aprovecharse de la naturaleza humana. Busque una solución que detecte y bloquee las amenazas que llegan por correo electrónico, dirigidas contra los usuarios, antes de lleguen a la bandeja de entrada. Frene las amenazas externas que utilizan su dominio para atacar a los clientes. Una herramienta de prevención de pérdida de datos del correo electrónico (DLP) ayuda a proteger los datos y garantizar su acceso. Busque una solución que clasifique con precisión la información confidencial y esencial, y que garantice que solo las personas adecuadas acceden a esos datos.
- **Construya una defensa sólida contra estafas por correo electrónico.** Detectar los mensajes de correo electrónico de impostores con herramientas de seguridad convencionales puede resultar difícil. Invierta en una solución que le permita administrar el correo electrónico con políticas de cuarentena y bloqueo personalizadas. Los atacantes pueden utilizar cuentas para engañar a los usuarios de la misma organización, por lo que su solución debe analizar tanto el correo interno como externo. Utilice autenticación del correo electrónico DMARC (Domain-based Message Authentication, Reporting and Conformance) para detener los mensajes falsificados, antes de que los empleados o los socios externos sufran una estafa.
- **Adopte un enfoque seguridad “zero-trust” (de confianza cero) para el acceso remoto.** Hoy día las empresas de servicios financieros y las aseguradoras almacenan y procesan más datos que nunca, gestionan una huella digital mayor y trabajan con plantillas más dispersas. Todo esto unido abre a los ciberdelincuentes nuevas oportunidades. Además, la tecnología VPN tradicional no ha evolucionado al mismo ritmo. Invierta en una solución seguridad “zero-trust” (de confianza cero) que pueda conectar con rapidez y seguridad a los empleados y a los socios y clientes externos a su centro de datos y a la nube
- **Aísle las URL y los sitios web peligrosos.** Mantenga el contenido de los sitios web peligrosos fuera del entorno. La tecnología de aislamiento web puede evaluar las páginas web sospechosas y las URL no verificadas en un contenedor protegido dentro del navegador web habitual de los usuarios. Este método puede ser una protección esencial para las cuentas de correo electrónico compartidas, que son difíciles de proteger con autenticación multifactor. La misma tecnología puede aislar los servicios personales de navegación web y correo electrónico web. Con el aislamiento, puede dar a los usuarios más libertad y privacidad sin exponer a su organización a más riesgos.

- **Proteja Microsoft 365 y otras plataformas cloud.** En el sector de los servicios financieros y los seguros, cada vez se trasladan más datos y aplicaciones a la nube, por lo que necesita ver la actividad de la nube a medida que se produce. Un agente de seguridad de acceso a cloud (CASB) puede ayudarle a realizar análisis y actuar con rapidez si se detectan infracciones de directivas del correo electrónico, para garantizar la continuidad del servicio.
- **Identifique y detenga las amenazas internas.** Protéjase frente a pérdidas de datos, sabotajes y daños a la imagen de marca provocados por personal interno malicioso, negligente o comprometido. Adopte una solución de gestión de amenazas internas que correlacione la actividad y los movimientos de datos para ayudarle a encontrar la correspondencia entre el comportamiento y la intención de los usuarios. Ayude a los equipos de seguridad a identificar el riesgo para los usuarios, detectar y responder a las fugas de datos internas y agilizar la respuesta a incidentes.
- **Reduzca el riesgo de incumplimiento de normativas.** Las normativas del sector de servicios financieros y de seguros evolucionan continuamente. Las organizaciones se enfrentan a más auditorías, multas más cuantiosas y las molestias normativas de los socios externos. Busque una solución de archivado y cumplimiento que pueda detectar y mitigar rápidamente las fugas de datos internas, ya sean maliciosas o accidentales. E identifique y detenga las prácticas empresariales fraudulentas, como las de facturación y sobornos.
- **Asóciese con un proveedor de inteligencia sobre amenazas.** Los ataques focalizados y dirigidos exigen disponer de inteligencia sobre amenazas avanzada. Utilice una solución que combine técnicas estáticas y dinámicas para detectar nuevas herramientas de ataque, tácticas y objetivos, y luego aprenda de ellas.

MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.

---

proofpoint.

0400-003-01-01 1/21