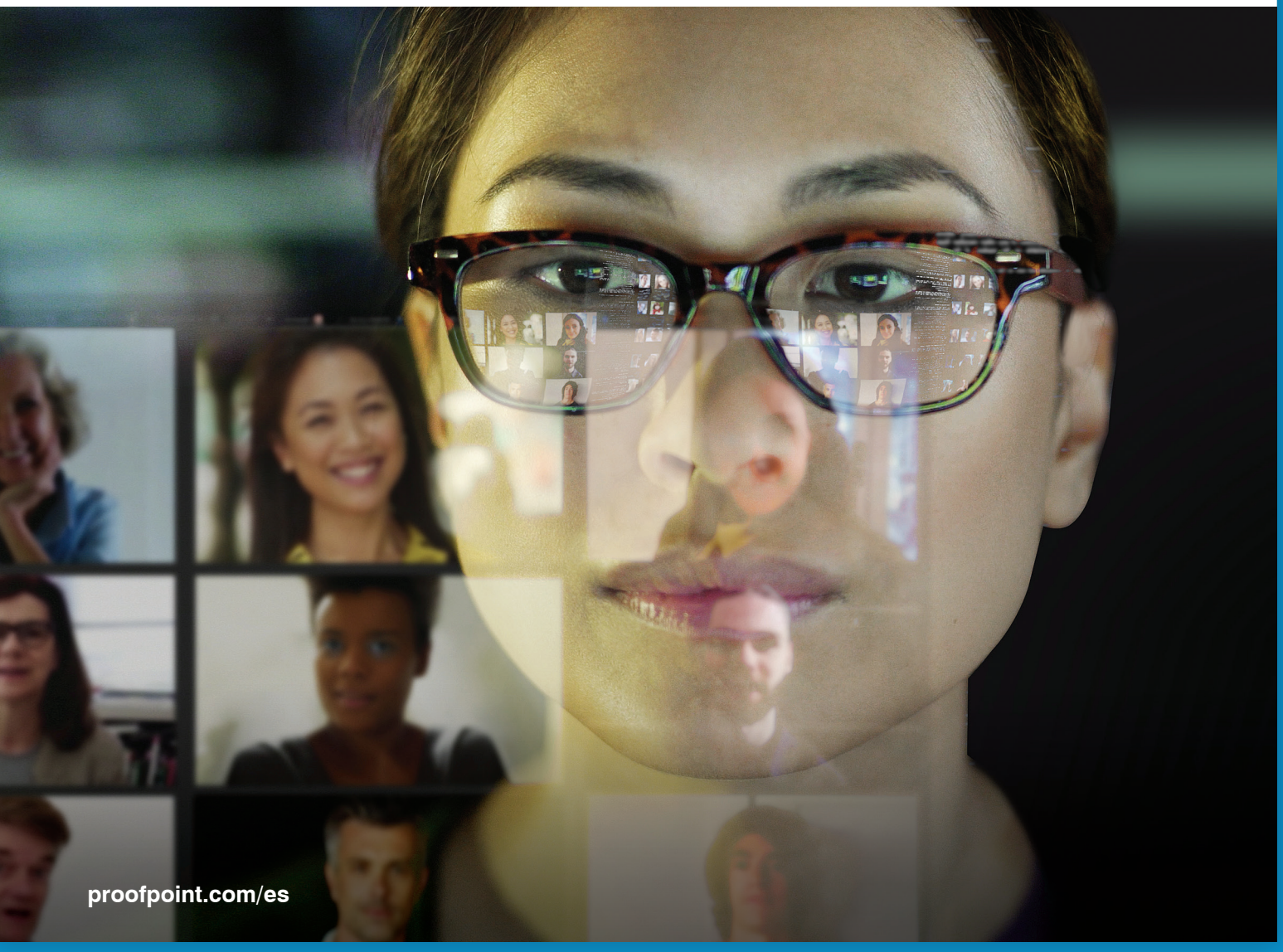
proofpoint.

INFORME

El factor humano 2021

Ciberseguridad, ransomware y estafas por correo electrónico en un año que cambió el mundo



proofpoint.com/es

Introducción

La tragedia, conmoción y cambios históricos que trajo 2020 han sido documentados en innumerables ocasiones. Pero en un momento en el que las organizaciones de todo el mundo se encaminan cautelosamente hacia la normalidad, "el año que no lo fue"[1] sigue ofreciendo valiosas lecciones que merece la pena explorar. Esto es especialmente cierto en el ámbito de la ciberseguridad.

Mientras la pandemia mundial puso patas arriba el trabajo y las rutinas domésticas, los ciberdelincuentes se abalanzaron para sacar provecho. Aprovecharon entornos laborales repentinamente poco familiares y el miedo, la incertidumbre y la duda de la gente para engañar a los usuarios y comprometer a las organizaciones. Y ahora en 2021 estamos viendo lo que ocurre cuando unos ciberdelincuentes envalentonados se aprovechan de su ventaja, mientras una ola de ataques de ransomware golpea importantes empresas e infraestructuras.

Ha comenzado el retorno a las oficinas, fábricas, tiendas y salas de exposiciones. Pero algunas tendencias de la era de la pandemia puede que hayan venido para quedarse. Muchos trabajadores pasarán a entornos híbridos, dividiendo su tiempo entre sus hogares y espacios de trabajo compartidos. Los equipos distribuidos colaborarán en distintas geografías y jurisdicciones legales. Cambios en el comercio electrónico, la nube y otras áreas, ya en marcha antes de la pandemia, no han hecho sino acelerarse.

No importa cómo será el mundo pos-COVID, la protección de las personas, dondequiera o comoquiera que trabajen, será un desafío permanente.

Acerca de este informe

Desde su creación en 2014, el informe El factor humano se ha basado en la sencilla premisa de que la gente, y no la tecnología, constituye la variable más crítica de las ciberamenazas actuales.

Desde entonces, esta noción un día contraria se ha convertido en una realidad ampliamente reconocida. El objetivo de los ciberdelincuentes son las personas. Se aprovechan de la gente. Después de todo, ellos mismos *son* personas.

Para prevenir, detectar y responder eficazmente a las amenazas y riesgos de incumplimiento actuales, los profesionales de la seguridad de la información deben comprender las dimensiones centradas en las personas del riesgo asociado a los usuarios: vulnerabilidad, ataque y privilegios. En términos prácticos, esto significa saber:

- Dónde son más vulnerables los usuarios
- Cómo les atacan los ciberdelincuentes
- El daño potencial cuando se compromete el acceso privilegiado a los datos, a los sistemas y a otros recursos

Abordar esos elementos (el *factor humano* de la ciberseguridad) constituye el pilar central de una defensa moderna.

Qué cubre el informe

Este informe profundiza en cada una de las tres facetas del riesgo asociado a los usuarios. Analiza cómo los extraordinarios eventos de 2020, y el cambio histórico que provocaron, han transformado el panorama de las amenazas. Examina el cambiante ecosistema de amenazas y sus repercusiones para el resto de nosotros, y explica cómo una defensa centrada en las personas puede hacer a los usuarios más resilientes, mitigar los ataques y gestionar los privilegios.

Este informe cubre las amenazas detectadas, mitigadas y resueltas durante 2020 en los despliegues de Proofpoint de todo el mundo, uno de los conjuntos de datos más amplios y diversos en el ámbito de la ciberseguridad.

Nos centramos en gran medida en las amenazas que forman parte de una campaña de ataques de mayor envergadura, o series de acciones llevadas a cabo por un ciberdelincuente para conseguir su objetivo. En ocasiones, podemos vincular estas campañas a un ciberdelincuente concreto, un proceso conocido como atribución. Pero por las razones que se explican en la sección **"El arte y la ciencia de la atribución" de la página 27**, esto no es siempre posible.

Alcance

Los datos de este informe se basan en el gráfico de amenazas Nexus de Proofpoint, utilizando datos recopilados de despliegues de Proofpoint en todo el mundo. Cada día analizamos más de 2200 millones de mensajes de correo electrónico, 35 000 millones de URL, 200 millones de adjuntos, 35 millones de cuentas cloud, etc., o lo que es lo mismo, billones de puntos de datos en todos los canales digitales relevantes.

Este informe cubre el período entre el 1 de enero y el 31 de diciembre de 2020. A menos que se indique, incluye amenazas observadas directamente por nuestra red mundial de investigadores de amenazas y vinculadas a una campaña de ataques, lo que definimos como una serie de acciones llevadas a cabo por un atacante para conseguir un objetivo.

Para la sección 3: Privilegios, 300 clientes compartieron sus alertas de Insider Threat Management, que indica qué tipos de abuso de privilegios eran los que más les preocupaban. Comparamos las alertas definidas desde febrero de 2020 hasta enero de 2021, el pico de la pandemia, con las definidas desde octubre de 2019 hasta enero de 2020.

[1] *The Economist*. "2020: The year that wasn't" (2020: El año que no fue), noviembre de 2020.

Índice

Hallazgos principales 4

1 **Vulnerabilidades** 6

Los usuarios a prueba: tasas de fallos en simulaciones de phishing . . . 9

Tasas de fallos del sector 10

2 **Ataques** 11

El ransomware va en aumento 11

Estados decisivos: ataques relacionados con las elecciones en EE. UU. 13

COVID-19: Cómo los ciberdelincuentes han aprovechado la pandemia 15

Tipo de ataques 21

Técnicas de ataque. 22

Herramientas de ataque 24

3 **Privilegios** 30

Conclusiones y recomendaciones 31

Hallazgos principales

A continuación repasamos las principales hallazgos del informe de este año.

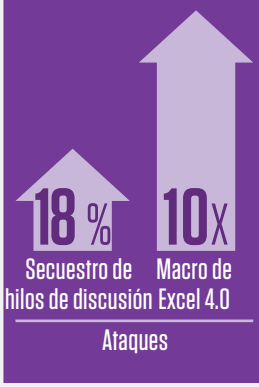
Más de **48 millones de mensajes con malware** capaces de ser **utilizados como punto de entrada para ataques de ransomware**.

En un mundo inmerso en noticias sobre la COVID-19, los ciberdelincuentes sacaron provecho de la situación. **Los señuelos relacionados con la pandemia fueron más habituales que los asociados a cualquier otro evento o noticia.** Prácticamente todos los ciberdelincuentes que supervisamos utilizaron contenido relacionado con la pandemia en algún momento de 2020.

Casi el **10 % de los mensajes de correo electrónico maliciosos relacionados con campañas** intentaron distribuir el malware Emotet. Antes de su desmantelamiento en enero de 2021 durante una redada de las fuerzas de seguridad, la infraestructura de Emotet se ofrecía en alquiler a otros grupos, que la empleaban para distribuir ransomware y otros tipos de malware.

Casi el **25 % de todas las campañas de ataque** ocultaban malware en archivos ejecutables comprimidos, que solo se ejecutaban tras la interacción de los destinatarios.

El phishing de credenciales, contra particulares o contra empresas, fue con diferencia el método más habitual de ataque, siendo responsable de casi dos tercios de todos los mensajes maliciosos, superando al resto de ataques juntos. El phishing de credenciales da lugar al compromiso de cuentas, que puede utilizarse para lanzar otros ataques, incluido el robo de datos y las estafas Business email compromise (BEC).



Las técnicas que requieren la interacción del destinatario con un adjunto o directamente con los ataques crecieron de manera considerable. **Los ataques de secuestro de hilos de discusión aumentaron un 18 %** respecto al año anterior. Los que utilizaron archivos protegidos con contraseña se multiplicaron casi por cinco. Y el volumen de ataques de **macros de Excel 4.0 creció más de 10 veces**

Más de 1 de cada 3 personas víctimas de campañas de ataques que utilizan esteganografía hicieron clic en el mensaje malicioso, la mayor tasa de éxito de todas las tácticas de ataque.

>50X

Los ataques que utilizan técnicas CAPTCHA superaron **en más de 50 veces el número de clics conseguidos** en 2020 frente al año anterior.

Las campañas de ataques lanzadas por el ciberdelincuente identificado como TA542 (el atacante vinculado con la red de bots Emotet) consiguieron persuadir al **mayor número de usuarios para que hicieran clic**. Su total refleja su eficacia y el enorme volumen de mensajes enviados en cada campaña.

Con los usuarios repentinamente confinados en sus hogares y el teletrabajo como nueva normalidad, **la visión que tienen las organizaciones de los riesgos basados en los privilegios cambió por completo. El número de organizaciones que definen alertas DLP para estas actividades aumentó de manera importante** en relación a niveles prepandemia por estas actividades:

- Uso de dispositivos USB
- Copia de un archivo o carpeta de gran tamaño (en particular a horas intempestivas)
- Evaluación de los servicios de intercambio de archivos
- Actividades que pudieran sortear la herramienta de supervisión de usuarios

TOP 5 Los controles DLP y de amenazas internas definidos por los clientes, en general, fueron:

1. Conexión a un dispositivo USB no autorizado
2. Copia de carpetas o de archivos grandes
3. Subida de un archivo sensible a la web
4. Apertura de un archivo con contraseñas en formato de texto
5. Descarga de un archivo con una extensión potencialmente dañina

Estructura del informe

En ciberseguridad, el riesgo se define como: *amenazas* x *vulnerabilidad* x *impacto* +/- *controles de seguridad*

Este informe se centra en cada una de estas facetas desde la perspectiva de nuestro modelo de riesgos asociados a los usuarios centrado en las personas —vulnerabilidad, ataques (amenazas) y privilegios (impacto)— con recomendaciones sobre las formas de mitigar cada una de ellas.

Al igual que las personas son únicas, también lo es el valor de cada uno para los ciberdelincuentes, así como el riesgo para los empresarios.

Todas tienen sus propios hábitos digitales, **vulnerabilidades** y puntos débiles. Los agresores les **atacan** de diversas formas y con distinta intensidad. Además, tienen distintos niveles de **privilegios** de acceso a los datos, sistemas y recursos.

Estos tres factores interrelacionados determinan su riesgo global.

Vulnerabilidad

La vulnerabilidad de los usuarios empieza por su comportamiento digital, es decir, cómo trabajan y dónde hacen clic.

Muchos empleados teletrabajan o acceden al correo electrónico de la empresa desde sus propios dispositivos personales. Pueden tener almacenamiento cloud para sus archivos e instalar add-ons de terceros para sus aplicaciones cloud. O pueden ser especialmente receptivos a las tácticas de phishing a través de correo electrónico.

Ataques

No todos los ciberataques se crean de la misma forma. Si bien todos son potencialmente dañinos, algunos son más peligrosos, dirigidos o sofisticados que otros.

Las amenazas indiscriminadas de bajo perfil puede que sean más numerosas que las más avanzadas, pero normalmente son menos preocupantes, ya que se conocen bien y se bloquean con más facilidad. (Sin embargo, no se equivoque, pueden causar el mismo daño).

En cambio, hay otras amenazas que aparecen solo en contados ataques y que, por su nivel de sofisticación o las personas a las que van dirigidas, son más peligrosas.

Privilegios

Los privilegios determinan todo aquello potencialmente valioso a lo que las personas tienen acceso, como datos, autoridad financiera, relaciones estratégicas, etc. Medir este aspecto del riesgo es crucial, ya que refleja la recompensa potencial para los agresores, así como el daño para las organizaciones si son víctimas del ataque.

Lógicamente, el cargo del empleado en la empresa es un factor que cuenta a la hora de determinar y calificar sus privilegios. Pero no es el único y, con frecuencia, ni siquiera es el más importante. Para los agresores, un objetivo valioso será cualquiera que les sirva como medio para conseguir su fin.

Cuando colisionan los factores de riesgo

Unos niveles de riesgo elevados de cualquiera de estas tres categorías constituyen un motivo de preocupación y, en la mayoría de los casos, requieren niveles adicionales de seguridad. Cuando dos o más factores son elevados, es señal de un problema de seguridad más urgente.

A continuación se incluyen cuatro categorías de usuarios que ponen de manifiesto cómo las combinaciones de vulnerabilidades, ataques y privilegios afectan a su nivel de riesgo general:

- **Objetivos latentes:** los usuarios con privilegios elevados que también son más vulnerables a timos de phishing son un peligro en potencia. Un usuario con privilegios elevados no siempre tiene un puesto ejecutivo. Incluso los recursos humanos júnior, empleados de instalaciones y administración pueden tener un nivel de acceso peligroso en las manos equivocadas. Puede que no estén en el radar de los atacantes ahora, pero están en el puesto perfecto para ser explotados.
- **Objetivos fáciles:** los usuarios muy atacados que son vulnerables a amenazas son presas fáciles para los ciberdelincuentes. Una respuesta y una corrección rápidas pueden contener el daño para los usuarios con pocos privilegios. Pero un ataque de éxito puede facilitar al ciberdelincuente una base para moverse hasta los usuarios con acceso a datos, sistemas y recursos más valiosos.
- **Objetivos importantes:** el riesgo que presentan los usuarios con privilegios elevados y muy atacados puede mitigarse mediante la reducción de su vulnerabilidad a través de la concienciación en materia de seguridad y una buena higiene digital. Las personas de esta categoría se enfrentarán a una enorme cantidad de ataques, y basta con que solo uno tenga éxito para provocar un daño permanente a la organización.
- **Objetivos inminentes:** los usuarios con niveles altos de los tres factores de riesgo son riesgos inmediatos y críticos. Deben tratarse como una prioridad de seguridad urgente.

SECCIÓN 1

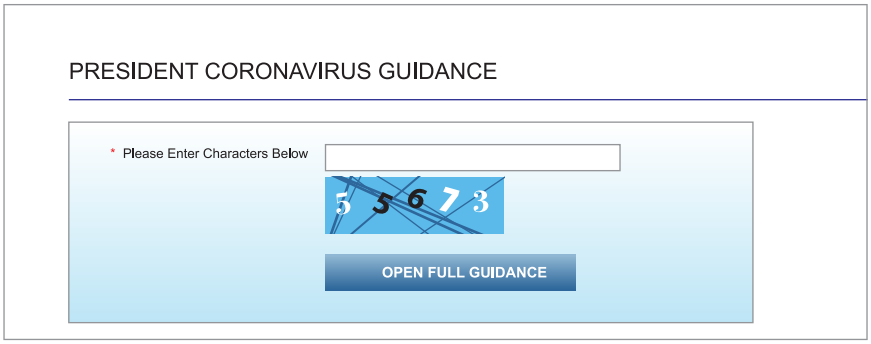
Vulnerabilidades

Otra forma de pensar sobre las vulnerabilidades es preguntarse "si mis usuarios son objeto de un ciberataque, ¿cuáles son las posibilidades de que se conviertan en víctimas?

Algunas de las técnicas de ataque de mayor éxito en 2020 fueron también las más dirigidas, y se utilizaron en campañas que en ocasiones estaban formadas por un puñado de mensajes de correo electrónico.

La **ESTEGANOGRAFÍA**, u ocultación de código malicioso en fotografías y otros tipos de archivos, se utilizó solamente en algunas campañas dirigidas. Sin embargo, la técnica demostró ser muy eficaz, consiguiendo que tres de cada ocho destinatarios hicieran clic.* Esa es la tasa de respuesta que todo ciberdelincuente (y no digamos profesional de marketing por correo electrónico) desearía.

Las técnicas **CAPTCHA**, que utilizan crucigramas visuales para distinguir a las personas de las máquinas, consiguieron superar en más de 50 veces el número de clics respecto al año anterior. Si bien la tasa de respuesta global fue un más modesto 5 % —que en cualquier caso se consideraría todo un éxito en la mayoría de las campañas de marketing por correo electrónico—, muchos usuarios sucumbieron a estas técnicas en relación a 2019.



Captura de pantalla de un desafío CAPTCHA de un ataque que utilizaba el tema de la COVID en mayo.

No está claro por qué los usuarios eran más vulnerables a una u otra técnica. Los teletrabajadores pueden haber estado más distraídos y cognitivamente mermados por el estrés de 2020. Ta vez algunos estaban incluso preparados por los nuevos controles de teletrabajo para ver la pregunta CAPTCHA como un desafío de seguridad normal.

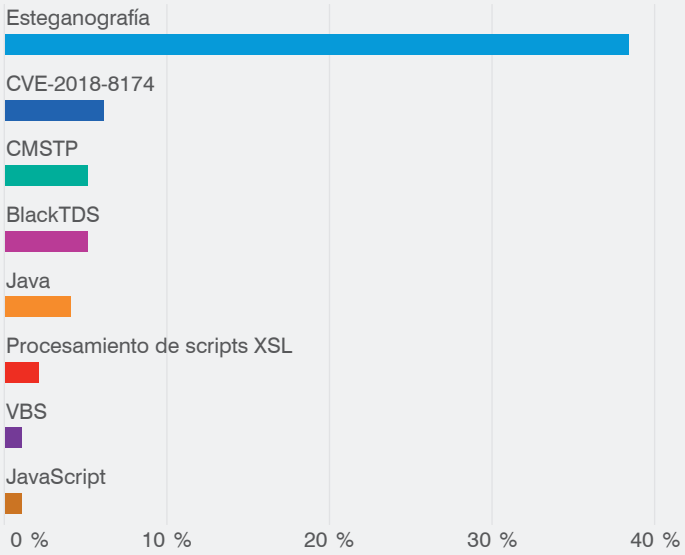
ESTEGANOGRAFÍA
Los ciberdelincuentes utilizan esta técnica para ocultar la payload maliciosa en un archivo aparentemente inofensivo, como una fotografía o un archivo de audio. Por lo general, la payload se cifra en bits de datos no utilizados que los usuarios no ven y que son muy difíciles de detectar con herramientas basadas en archivos y en entorno aislado. Tras aterrizar en las máquinas de las víctimas, los datos ocultos se codifican y se activan.

CAPTCHA
La mayoría de las veces, las técnicas CAPTCHA se utilizan como medida antifraude. Al pedir al usuario que realice una tarea que resulta muy sencilla para las personas, pero complicada para las máquinas, esta técnica ayuda a garantizar que quien está accediendo a un sitio web es una persona real (y no un robot automatizado). Los ciberdelincuentes las utilizan de manera similar, aunque más siniestra. Mediante un desafío CAPTCHA, se aseguran de que el malware está en el sistema de un usuario real, y no en un entorno aislado de seguridad que pueda supervisar su actividad maliciosa. La técnica también puede utilizarse para determinar la procedencia del usuario (en función de la dirección IP) en el caso de ataques contra personas de un país o región determinados.

*En campañas atribuidas.

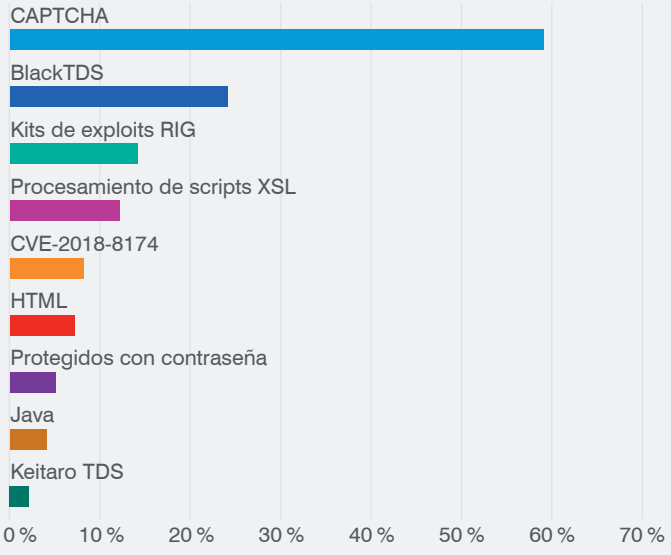
Técnicas con el mayor número de clics por mensaje*

La esteganografía demostró ser muy eficaz en las pocas campañas dirigidas en las que se utilizó esta técnica. Los ataques que aprovecharon la vulnerabilidad CVE-2018-8174 de Windows también fueron muy eficaces y se utilizaron en campañas de mayor envergadura y frecuencia.



Variación interanual (media de clics en 2020 frente a 2019)*

Las técnicas CAPTCHA, que eluden las herramientas de seguridad solicitando la intervención humana, generaron 50 veces más clics en 2020 que el año anterior. Se utilizaron en varias decenas de campañas a gran escala.



TA542

Antes de su desmantelamiento en enero de 2021, TA542 se había convertido en uno de los atacantes más prolíficos de los últimos años debido a campañas masivas que utilizan una variante de malware llamada Emotet. El grupo ha dirigido ataques contra múltiples sectores en todo el mundo, enviando cientos de miles (o incluso millones) de mensajes al día.

Emotet no solo compromete los sistemas que infecta. También utiliza estas máquinas comprometidas para lanzar nuevos ataques, incorporándolas a una red tipo zombi de más de un millón de máquinas infectadas de forma similar conocida como red de bots. Otros ciberdelincuentes utilizaron la infraestructura de red de bots de TA542 para todo tipo de ataques.

TA576

Este grupo de ciberdelincuentes se dedica principalmente a lanzar ataques con temas fiscales. Aunque solo lanzó dos campañas en 2020, ambas fueron masivas.

TA407

También conocido como Silent Librarian, Cobalt Dickens y Mabna Institute, este grupo opera en Irán. Ha atacado universidades de América del Norte y Europa en busca de propiedad intelectual. En 2018, las autoridades de EE. UU. procesaron a nueve supuestos miembros del grupo por el robo de datos valorados en 3400 millones de dólares.

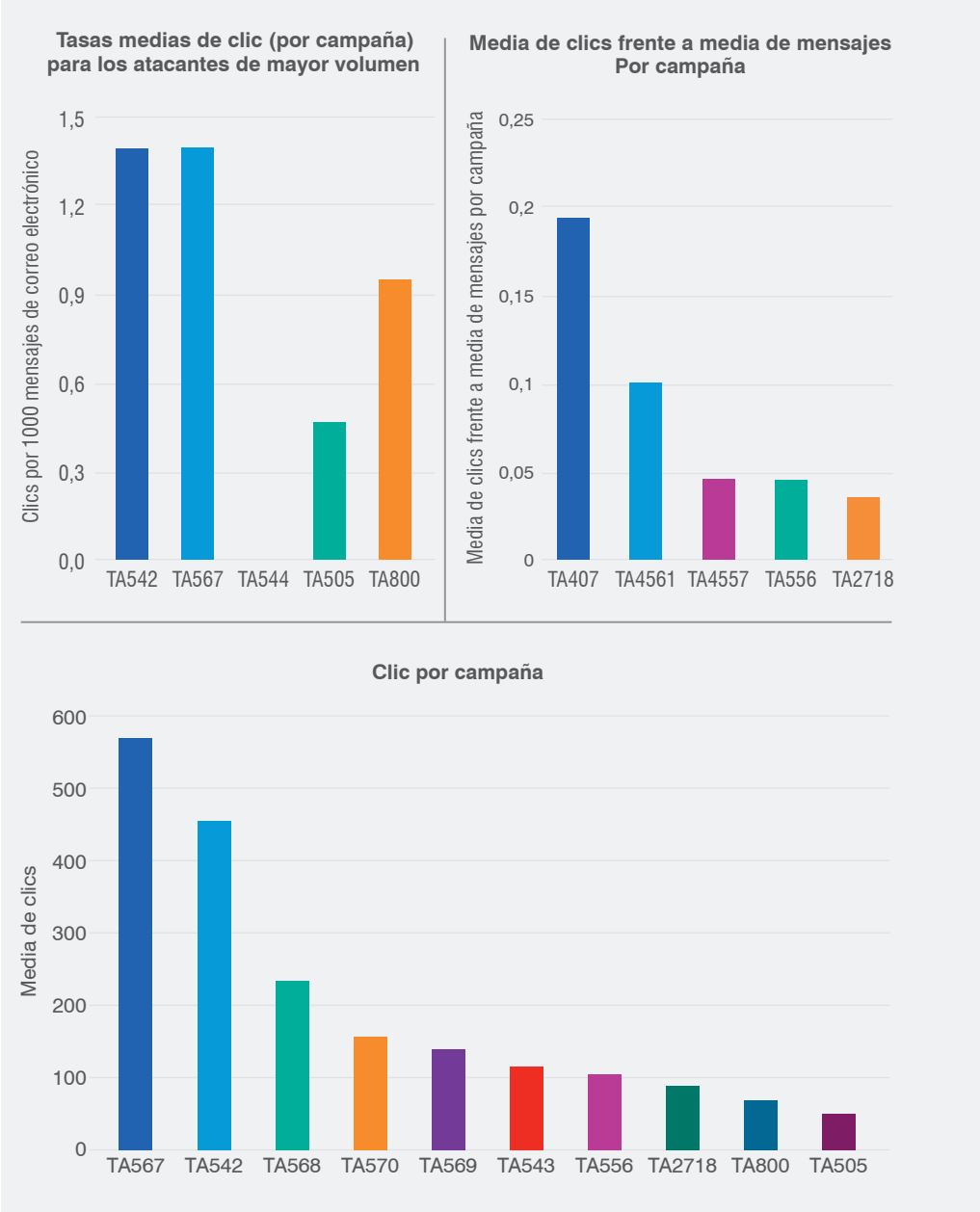
En cualquier caso, los ciberdelincuentes no tardaron en aprovecharse de los usuarios vulnerables.

Un ciberdelincuente al que hemos apodado **TA542**, el actor de amenazas con el mayor volumen de 2020, consiguió 454 clics por campaña de ataque con una tasa de éxito de aproximadamente una décima parte del 1 %. Lo que carecía en eficacia lo compensaba con el enorme volumen. (Encontrará más información sobre este infame ciberdelincuente en la **Sección 2: Ataques.**) **TA576**, otro atacante de gran volumen, consiguió 568 clics por campaña con una tasa de éxito similar.

Algunos de los atacantes más "eficaces" (los que consiguen mayores tasas de éxito) se encontraban entre los más pequeños en términos de volumen de mensajes.

Por ejemplo, un atacante al que hemos identificado como **TA407** consiguió de media un clic en cada cinco mensajes de correo electrónico que envió en 2020, una de las mayores tasas de éxito de todos los que hemos supervisado. Los ciberdelincuentes eran muy selectivos y enviaron tan solo unas decenas de mensajes en menos de 100 campañas en todo 2020.

El grupo es conocido por lo avanzado de sus técnicas de ingeniería social. Por ejemplo, sus campañas de correo electrónico utilizaban logotipos de universidades, sitios web con apariencia profesional y actividades escolares habituales (como renovaciones de bibliotecas) para engañar a las víctimas para que proporcionaran credenciales de cuentas.



Los usuarios a prueba: tasas de fallos en simulaciones de phishing

Otra forma de medir el nivel de vulnerabilidad son los ejercicios de phishing simulado. Estos simulacros de ataque pueden revelar los señuelos y tácticas que tienen más probabilidades de engañar a los usuarios en escenarios del mundo real y condiciones laborales normales.

Nuestro **informe anual State of the Phish** analizó las respuestas de los usuarios a más de 60 millones de mensajes de correo electrónico de phishing simulado en un período de 12 meses de 2020. La comparación de las tasas de fallos media (el porcentaje de usuarios que mordieron el anzuelo) muestra cómo y dónde los usuarios son más vulnerables.

Estos son solo algunos aspectos destacados:

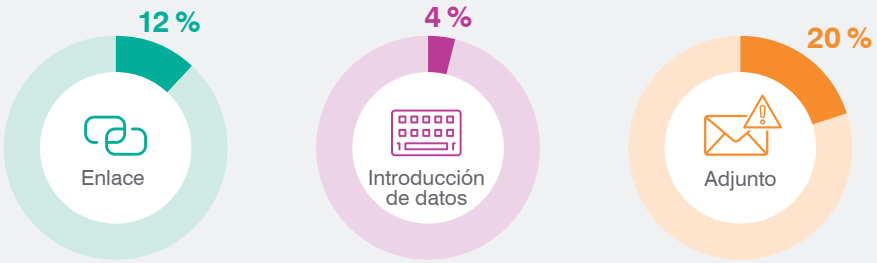
Tasas de fallos por tipo de plantilla

Cada mensaje de "phishing" se crea en base a una plantilla que permite a la organización simular una amplia variedad de estilos, temas y señuelos de ataque. Aunque las plantillas son tan variadas como las amenazas del mundo real, están organizadas en tres categorías principales:

- Basadas en enlaces (las que incluyen URL inseguras que llevan a sitios web de malware y dañinos)
- Basados en la introducción de datos (las que llevan al usuario a una página de inicio de sesión falsa para robar credenciales y otros datos personales)
- Basadas en adjuntos (las que incluyen un archivo malicioso)

Una media[2] de 1 de cada 5 usuarios hicieron clic en mensajes con adjuntos. Se trata de la mayor de los tres tipos de plantillas, una tasa de fallo que supera a los otros dos tipos combinados.

Tipos de plantillas de phishing: tasas medias de fallos



2 Para evitar la ponderación excesiva de las organizaciones más grandes, promediamos las puntuaciones por cliente en lugar de por usuarios individuales.

Tasas de fallos del sector

Sectores más vulnerables

Las tasas de fallos en ataques de phishing simulados sugieren que los usuarios de algunos sectores son más vulnerables que los de otros.

Los usuarios de empresas de ingeniería, telecomunicaciones, minería y formación, por ejemplo, fueron los más propensos a hacer clic. Al otro lado del espectro, los de los sectores de la hostelería/ocio y entretenimiento/medios de comunicación fueron los menos propensos.

(Nota: los sectores de este gráfico incluyen datos de al menos 15 organizaciones y un mínimo de 150 000 ataques simulados).

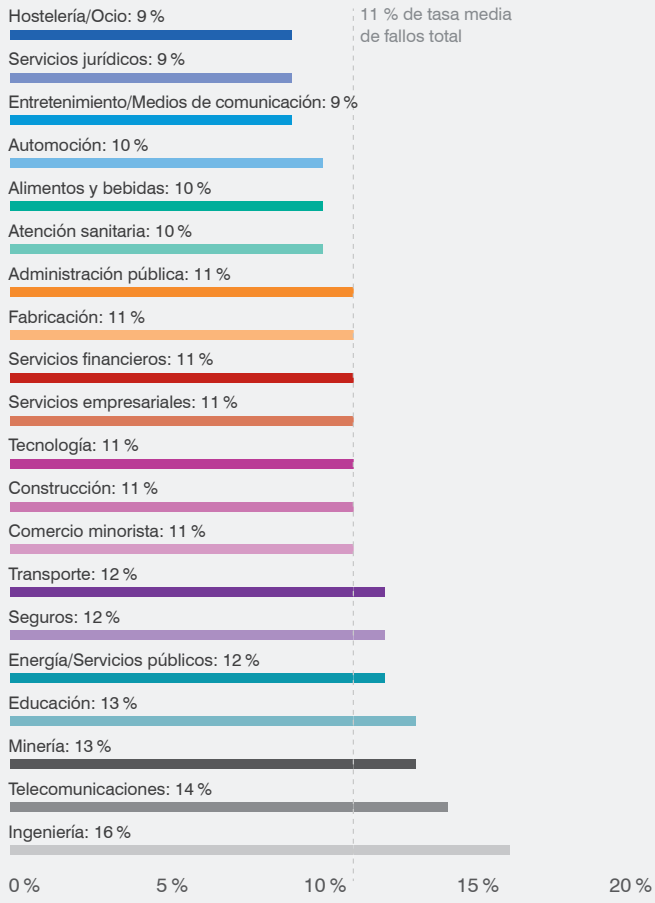
Departamentos más vulnerables

Pero las tasas de fallos por sectores por sí solas no muestran qué roles y equipos tienen las mayores dificultades. Los ciberdelincuentes a menudo atacan buzones de correo y alias de correo electrónico específicos. Las tasas de fallos por departamento a menudo ofrecen una visión más acertada de los puntos débiles potenciales.

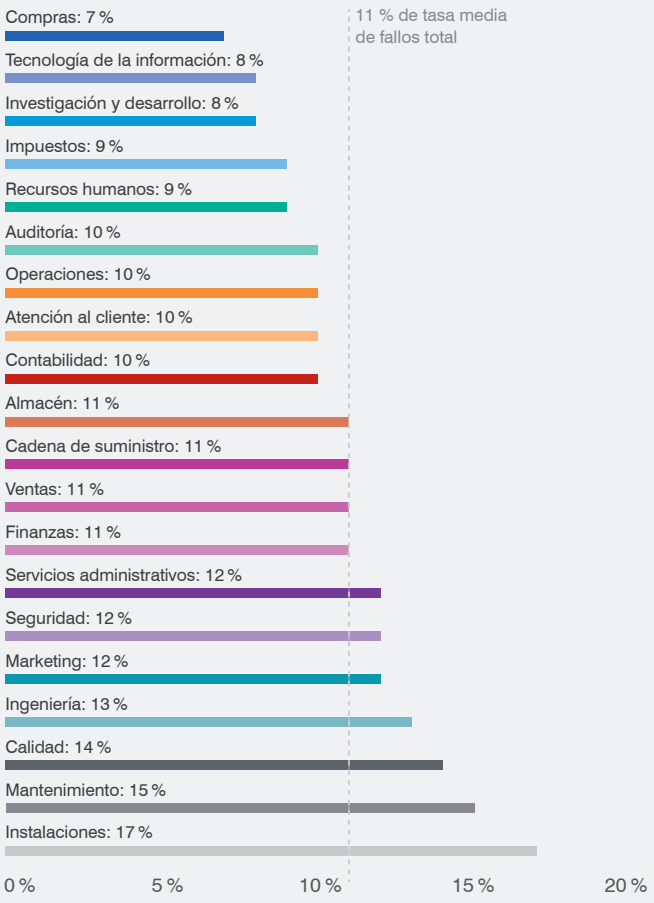
Compras, TI, investigación y desarrollo, impuestos, RR HH y auditoría fueron los departamentos menos propensos a caer en la trampa de los mensajes de phishing simulado. Instalaciones, mantenimiento, calidad e ingeniería fueron los más propensos.

(Nota: los sectores de este gráfico incluyen datos de al menos 15 organizaciones y un mínimo de 150 000 ataques simulados).

Tasa media de fallos por sector



Tasa media de fallos por departamento



SECCIÓN 2

Ataques

El ransomware va en aumento

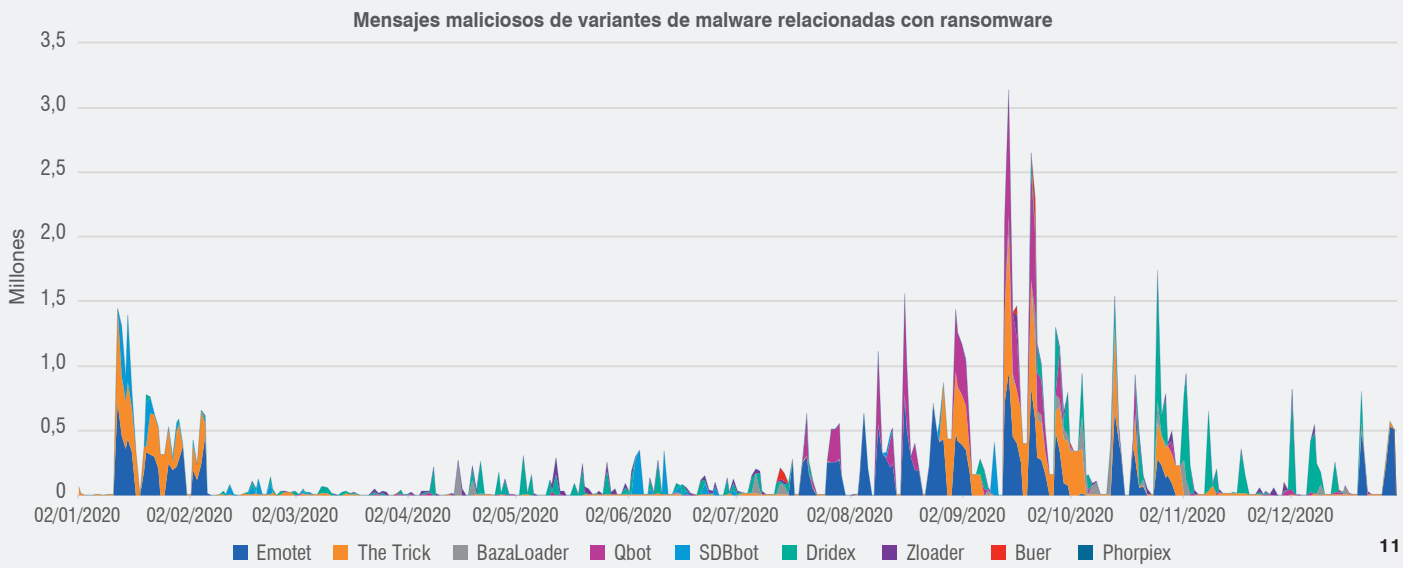
RANSOMWARE
Este tipo de malware bloquea los datos de la víctima mediante cifrado y, a continuación, exige un rescate (*ransom*, en inglés) para desbloquearlos con la clave de cifrado.

Según cifras del Gobierno de EE. UU.[3], los ataques de **RANSOMWARE** aumentaron un 300 % el año pasado. En la primera mitad de 2021, el problema había alcanzado incluso mayor prominencia con los ataques contra Colonial Pipeline, JBS Foods y el sistema público de salud de Irlanda (HSE), poniendo de manifiesto que los grupos de delincuentes responsables del ransomware provocan daño real a infraestructuras críticas en todo el mundo.

Si bien los ciberdelincuentes siguen utilizando el correo electrónico, las cosas han cambiado desde 2016, cuando Locky consiguió colarse en millones de buzones de entrada. En lugar de distribuirse como payload principal en campañas de correo electrónico malicioso, el ransomware ahora suele descargarse mediante malware ya presente en un sistema o distribuirse a través del acceso a través de un protocolo de acceso remoto (RDP) comprometido y una red privada virtual (VPN). Sin embargo, el correo electrónico sigue teniendo especial protagonismo en estos ataques, ya que es la vía a través de la cual se distribuye buena parte del malware de primera fase que se emplea para descargar el ransomware.

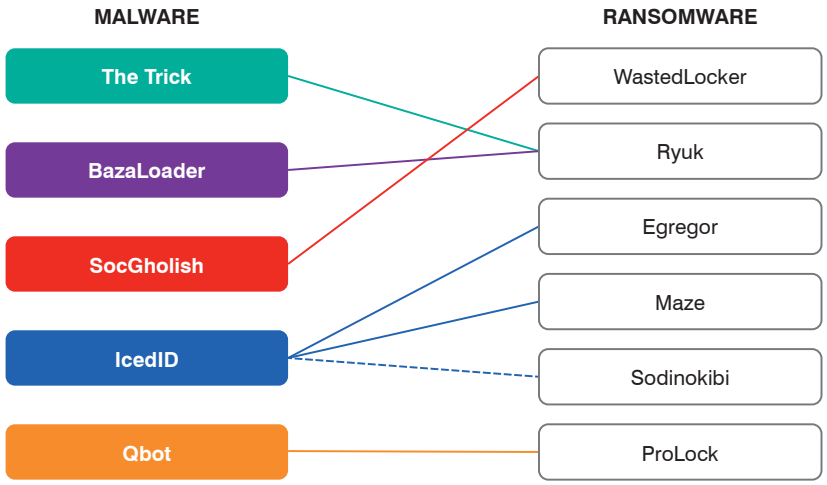
Los ciberdelincuentes encargados de estos cargadores y troyanos actúan entonces como agentes de acceso o facilitadores, y permiten a los grupos de ransomware utilizar puertas traseras para introducirse en los sistemas infectados a cambio de una parte de los beneficios. En lugar de buscar una distribución masiva y pequeños pagos, los ciberdelincuentes responsables del ransomware se embarcan ahora en campañas que se conocen como de "caza mayor", y que tienen como objetivo organizaciones de mayor tamaño con más que perder y más motivos para pagar.

3 James Rundle and David Uberti (*Wall Street Journal*). "How Can Companies Cope with Ransomware?" (¿Cómo pueden las empresas hacer frente al ransomware?) Mayo de 2021.



Este cambio de estrategia es la razón por la que no vemos grandes volúmenes de ransomware a través de nuestro gateway de correo electrónico, siendo una única variante, llamada Avaddon, responsable del 95 % de todas las payloads de ransomware de primera fase en 2020. Sin embargo, se han observado varias payloads de primera fase comunes, como The Trick, Dridex y Qbot, actuando como puntos de entrada para infecciones de ransomware posterior y, según nuestros datos, en los tres casos se encuentran entre las amenazas de mayor volumen. En total, observamos más de 48 millones de mensajes con malware capaces de descargar posteriormente ransomware u otras payloads secundarias en 2020.

Existe una relación 1:1 entre el malware de acceso inicial y la posterior variante de ransomware. Sin embargo, nuestras propias observaciones y las de otros investigadores[4] sugieren algunas asociaciones importantes.



Una muestra de las payloads de acceso inicial distribuidas por los ciberdelincuentes y el ransomware asociado desplegado como consecuencia del acceso inicial.

Si bien la red de relaciones entre grupos de ciberdelincuentes es compleja, no lo es la secuencia de eventos de un ataque de ransomware iniciado por correo electrónico: la infección inicial por un troyano bancario o cargador le sitúa en una posición de vulnerabilidad frente a cibercriminales en busca de objetivos de gran valor. Esto significa que para la mayoría de las empresas, la primera línea de defensa contra el ransomware es evitar la infección inicial.

En otras palabras, si consigue bloquear el cargador, conseguirá bloquear el ransomware.

4 Clifford Krauss (*The New York Times*). "How the Colonial Pipeline Became a Vital Artery for Fuel" (¿Cómo el oleoducto de Colonial Pipeline se convirtió en una arteria fundamental de petróleo?) Mayo de 2021.

Aunque los ciberdelincuentes no utilizaron señuelos con el tema de las elecciones hasta que estaban a pleno rendimiento en el otoño de 2020, atacaron a organizaciones relacionadas con las elecciones durante todo el año.

Estados decisivos: ataques relacionados con las elecciones en EE. UU.

La mayoría de los investigadores de seguridad anticiparon que las elecciones estadounidenses serían una oportunidad para los ciberdelincuentes. Algunos buscarían desinformar mientras que otros utilizarían las elecciones como cebo de ingeniería social en amenazas por correo electrónico.

Y eso es exactamente lo que ocurrió. Aunque los ciberdelincuentes no utilizaron señuelos con el tema de las elecciones hasta que estaban a pleno rendimiento en el otoño de 2020, atacaron a organizaciones relacionadas con las elecciones durante todo el año.

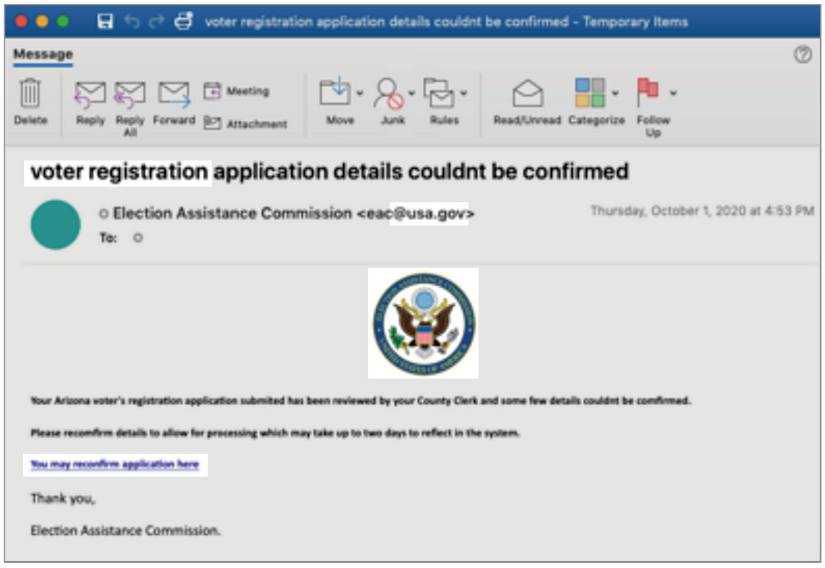
Ciberdelincuentes con motivaciones financieras y grupos financiados por estados atacaron organizaciones tanto de manera directa como periférica relacionadas con las elecciones. Esto incluyó todos los niveles gubernamentales y políticos: entidades locales, estatales y del gobierno federal, así como los comités de acción política.

Los señuelos con temas políticos y sobre las elecciones contra muchos sectores en los ataques con temas relacionados con las elecciones de EE. UU. se dispararon en octubre de 2020 y descendieron tras las elecciones el 3 de noviembre. Los temas empleados fueron:

- La salud del expresidente Donald Trump
- Comité Nacional Demócrata (DNC)
- La Comisión de Asistencia Electoral de EE. UU.
- Registro de votantes

CARACTERÍSTICAS DESTACADAS:

- Aprovecha temas que a menudo evocan fuertes sentimientos.
- Falsifica el dominio de correo de la Comisión de Asistencia Electoral de EE. UU.
- Utiliza el Sello del Presidente de EE. UU. para dar la apariencia de autoridad.
- Incluye una URL maliciosa disfrazada de un sitio web de registro.



Señuelo de correo electrónico que suplantaba a la Comisión de Asistencia Electoral.

SECUESTRO DE HILOS DE DISCUSIÓN
Tras usurpar la cuenta de correo electrónico de alguien, el atacante tiene vía libre a la bandeja de entrada de la víctima. Con ese control, el ciberdelincuente puede contestar a hilos de correo electrónico pasados o actuales con un mensaje malicioso. Como los destinatarios conocen y confían en el remitente (es más, están interactuando activamente con esa persona) esta técnica puede ser muy eficaz.

Algunas variantes de malware pueden ahora automatizar el secuestro de hilos de discusión para ingeniería social a gran escala.

EMOTET
Antes del desmantelamiento en 2021 de su infraestructura, Emotet fue el malware distribuido con más frecuencia del mundo. Se encontraba entre los primeros grupos en cambiar del robo inicial de credenciales bancarias a utilizarse como agente de acceso para otros ciberdelincuentes, incluidos los que distribuyen Dridex y Qbot.

URSNIF
Ursnif es un troyano bancario muy utilizado que evolucionó a partir de una variante de malware llamada Gozi, cuyo código fuente se filtró en 2015. Ursnif es la más popular de las muchas variantes de Gozi, que incluyen Dreambot, ISFB y Papras.

Tirando de un hilo de correo electrónico

Hubo una campaña dirigida contra funcionarios responsables de la administración de las elecciones y la planificación de la infraestructura de las elecciones. Los atacantes utilizaron un método llamado **SECUESTRO DE HILOS DE DISCUSIÓN**.

Algunas campañas de malware —como **EMOTET** y algunos ataques con **URSNIF**— se insertan automáticamente en hilos de correo electrónico activos. La técnica funciona de la forma siguiente:

1. El malware analiza los mensajes de correo electrónico en una bandeja de entrada comprometida.
2. Cuando se identifica "re:" en un asunto, crea un mensaje para enviar a otros dentro del hilo de correo electrónico, aparentando ser del usuario comprometido en el hilo.
3. Puesto que el mensaje parece proceder de alguien en quien confían los otros participantes (y sin duda con quien interactúan) los destinatarios son más propensos a caer en la trampa.

Chicos no tan orgullosos

En una campaña de amenazas por correo electrónico centrada en las elecciones poco habitual los ciberdelincuentes se hicieron pasar por el violento grupo racista de ultraderecha conocido como Proud Boys (Chicos orgullosos) y se dirigió contra votantes demócratas en Florida.

Mensajes con la línea de asunto "Vote for Trump or else!" (¡Vota a Trump o de lo contrario!) amenazaban con violencia si el destinatario no obedecía. Contenía un enlace a un vídeo con el logotipo de los Proud Boys de alguien supuestamente cumplimentando registros de votantes y votos por correo por ciudadanos de Alaska. Esta campaña contrastaba claramente actividad de ciberamenazas típica relacionada con las elecciones con flagrantes amenazas y una llamada a la acción física.

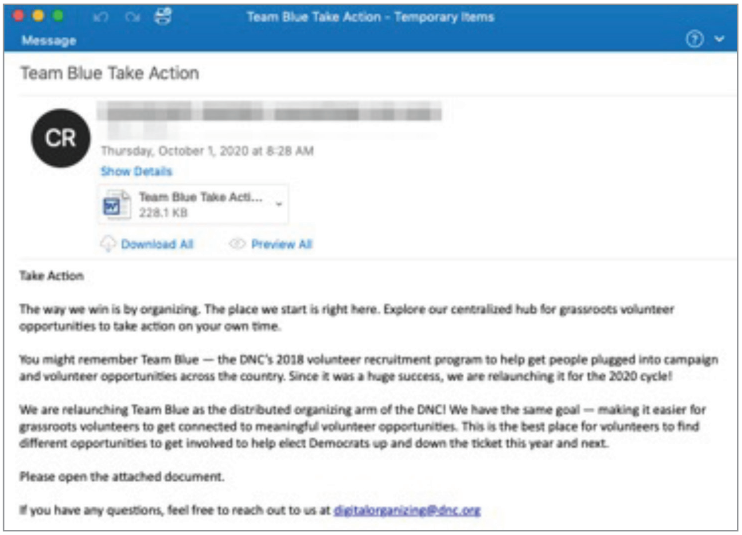
Aunque los miembros de los Proud Boys son conocidos por sus violentos ataques contra la izquierda, las autoridades y las empresas de seguridad afirman que los mensajes de correo electrónico procedían en realidad de atacantes financiados por el Estado ubicados en Irán.

Emotet hace su aparición en plena fiebre electoral

Emotet —la amenaza de mayor volumen del año— también utilizó señuelos relacionados con las elecciones a principios de octubre de 2020. TA542, el grupo detrás de Emotet, lanzó actividades relacionadas con las elecciones, como:

- **Disfrazarse** del Comité Nacional Demócrata (DNC)
- Animar a los destinatarios a presentarse voluntarios
- Apoyar la organización política

(Para obtener más información sobre Emotet, consulte **"Quién es quién en el panorama de amenazas: principales actores de amenazas", en la página 27**)



Un ataque de Emotet aprovechando las elecciones.

Emotet no dirigió ataques contra personas u organizaciones específicas implicadas en el proceso electoral. En su lugar, utilizó el interés en las elecciones y los eventos relacionados para crear señuelos y atraer a audiencias más amplias en múltiples sectores.

COVID-19: Cómo los ciberdelincuentes han aprovechado la pandemia

Para la mayoría de la gente, la COVID-19 puso patas arriba el trabajo y las rutinas domésticas. En este nuevo y extraño entorno, saber cómo son atacados sus empleados y, si es posible, quién está detrás de los ataques, son elementos fundamentales del puzle de ciberseguridad.

Los ciberdelincuentes utilizan acontecimientos de la actualidad en sus señuelos de correo electrónico todo el tiempo. Pero 2020 puede ser el primer caso en el que todos los ciberdelincuentes coincidieron en los mismos temas al mismo tiempo. Con la atención mundial sumida en noticias relacionadas con la pandemia, la totalidad del ecosistema de ciberamenazas giró en torno al mismo contenido temático al unísono.

Desde los remitentes de spam hasta los usuarios de **MALWARE COMERCIAL**, ciberdelincuentes a gran escala y las **AMENAZAS PERSISTENTES AVANZADAS** (APT), prácticamente todo el mundo cambió a la COVID-19 como opción favorita de contenido de ingeniería social. Observamos casi 250 millones de mensajes dirigidos asociados a la COVID-19, y miles de millones más de spam y ataques más generalizados.

MALWARE COMERCIAL

El malware comercial se refiere a herramientas de uso común y de disponibilidad general utilizadas por una amplia variedad de atacantes. Si bien las herramientas de seguridad deben conocer y bloquear el malware comercial, los ciberdelincuentes lo utilizan a menudo de formas muy astutas y en grandes volúmenes, y pueden ser tan dañinos como amenazas más avanzadas o dirigidas.

AMENAZAS PERSISTENTES AVANZADAS (APT)

Los ciberdelincuentes que utiliza APT por lo general llevan a cabo tareas de espionaje en nombre de un gobierno, aunque la categoría también puede incluir ciberdelincuentes avanzados. Los ataques pueden implicar el robo de propiedad intelectual, robos económicos y ataques diseñados para alterar o dañar datos y sistemas.

La apropiación de una crisis sanitaria

La pandemia de COVID-19 ha sido un buen ejemplo de cómo los ciberdelincuentes ajustan las tácticas en tiempo real para sacar provecho del miedo, incertidumbre y dudas de las víctimas.
A continuación incluimos los principales hitos de la crisis sanitaria mundial y la respuesta de los ciberdelincuentes.

Ataques destacados

19 de enero

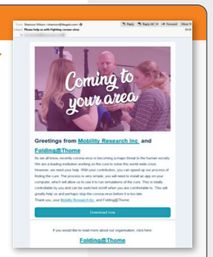
Ataques contra usuarios de Japón utilizan señuelos relacionados con la COVID-19 para conseguir que los destinatarios abran documentos de Microsoft Word infectados. Los mensajes forman parte de una campaña de mayor envergadura que distribuye la cepa de malware Emote.

10 de febrero

Mensaje de correo electrónico falso relacionado con la COVID-19 enviado a objetivos en Japón.
Mensajes de correo electrónico enviados a destinatarios en una Italia muy golpeada prometen cambios en la pandemia. Los mensajes incluyen un documento de Microsoft Word adjunto con una URL que lleva a una página de phishing que roba las credenciales.

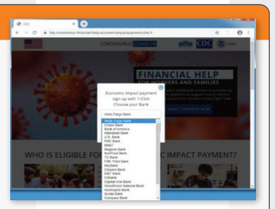
7 de marzo

Usuarios de EE. UU reciben mensajes de correo electrónico supuestamente de "Mobility Research Inc" que piden a los destinatarios que ayuden a encontrar una cura para el coronavirus participando en un proyecto Folding@Thome. El argumento imita el proyecto Folding@home legítimo, que utiliza ciclos de computación libres de los ordenadores de los usuarios para la investigación médica. Pero en lugar de ayuda en la investigación de la COVID-19 con la app Folding@Home real, los destinatarios que hacen clic en la URL se infectan con el malware RedLine, que roba las credenciales y descarga otro malware.



Abril

Residentes de EE. UU. reciben mensajes de correo electrónico de phishing del Sistema de Reserva Federal (FED), que lleva a un sitio web que parece el oficial y que pide a los destinatarios que introduzcan sus credenciales bancarias para recibir las ayudas de estímulo. Este sitio web se configuró para robar credenciales de los principales bancos de EE. UU.



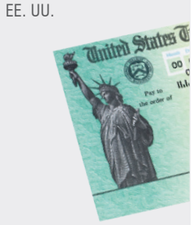
19 de enero de 2021

Mensajes de correo electrónico enviados a residentes en EE. UU. y Canadá prometen a los destinatarios dosis de la vacuna de Pfizer-BioNTech. Cuando los destinatarios hacen clic en la URL, se les dirige a una página de autenticación de Microsoft 365 falsa, diseñada para robar sus credenciales.

Volumen de mensajes de correo maliciosos relacionados con la pandemia

Hitos de la pandemia

ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE	ENERO
9 La Organización Mundial de la Salud (OMS) anuncia una misteriosa neumonía relacionada con un coronavirus en Wuhan, China.	**3** EE. UU. declara una emergencia de salud pública.	**6** 21 pasajeros de un crucero en California dan positivo.	**11** Los primeros cheques de estímulo se depositan en las cuentas bancarias de los destinatarios de EE. UU.	**1** El Remdesivir consigue la aprobación de la FDA.		**22** El Departamento de Salud y Servicios Humanos y el Departamento de Defensa de EE. UU. anuncian un acuerdo de distribución de vacunas con Pfizer y BioNTech para distribuir 100 millones de dosis de sus candidatos a vacunas de COVID-19.	**7** Se aplazan las conversaciones sobre un segundo paquete de ayudas.	**8** La Universidad de Oxford y AstraZeneca interrumpen la fase 3 de las pruebas de su vacuna debido a la sospecha de reacción adversa de uno de los participantes.	**2** El Presidente y la Primera Dama dan positivo por COVID-19; Trump ingresa en el hospital.	**16** La Administración de Medicamentos y Alimentos (FDA) de EE. UU. se compromete a actuar con diligencia para la aprobación de las vacunas de Pfizer y Moderna para uso de emergencia.	**11** La FDA aprueba la vacuna contra la COVID-19 de Pfizer-BioNTech para uso de emergencia.	
20 Tres aeropuertos (JFK, San Francisco y Los Ángeles) empiezan a realizar cribados por coronavirus a los viajeros.		**11** La OMS declara pandemia la COVID-19.		**28** Las muertes por COVID-19 en EE. UU. superan la marca de 100 000.		**27** La vacuna de Moderna entra en la fase 3 de pruebas.		**21** Johnson & Johnson comienza la fase 3 de pruebas de su vacuna.	**12** Johnson & Johnson interrumpe la fase 3 de pruebas de su vacuna tras la inexplicable enfermedad de un participante.		**14** Sandra Lindsay, una enfermera de UCI, es la primera persona en ser vacunada en EE. UU.	
21 La institución Centros para el Control y la Propagación de Enfermedades (CDC) confirma el primer caso de coronavirus en EE. UU.		**13** EE. UU. declara la COVID-19 emergencia nacional y desbloquea miles de millones de dólares en ayudas federales. Entra en vigor la prohibición de viajar para los ciudadanos no estadounidenses procedentes de Europa.	**29** Resultados prometedores en las pruebas con Remdesivir de los Institutos Nacionales de Salud (NIH).						**15** Los casos en EE. UU. vuelven a repuntar con 60 000 nuevos casos de COVID-19 comunicados, un número que no se alcanzaba desde primeros de agosto.		**18** La FDA aprueba la vacuna de Moderna para uso de emergencia.	
31 La OMS declara una emergencia de salud mundial.		**19** California declara la primera orden de confinamiento en todo un estado.							**23** En decisiones separadas, AstraZeneca y Johnson & Johnson reanudan las pruebas de sus respectivas vacunas.		**29** La segunda ronda de cheques de estímulo de EE. UU. empieza a llegar a los destinatarios.	
		26 El Congreso aprueba la CARES Act, que incluye 2 billones $ en ayudas a hospitales, pequeños negocios y gobiernos estatales y locales. Se convirtió en ley al día siguiente.										



VECTOR DE INFECCIÓN

Un vector de infección es el canal o vía de distribución del ataque. El correo electrónico es el vector de infección de la mayoría de los ciberataques modernos.

PAYLOAD

La carga maliciosa o payload es el malware que intenta introducir el atacante en el sistema de la víctima. Es distinto de cualquier código malicioso utilizado como punto de entrada inicial al sistema, técnicas de distribución o ingeniería social que intenta engañar a las personas para que lo descarguen y activen.

CARACTERÍSTICAS DESTACADAS:

- Utiliza "lookalike domains" (dominios parecidos) para parecer un comunicado de la OMS.
- El adjunto malicioso utiliza un nombre de archivo que refuerza el tema.
- Ofrece información básica sobre la COVID-19 para ayudar a legitimar el mensaje.
- Utiliza el logotipo de la OMS para ocultarse aún más.

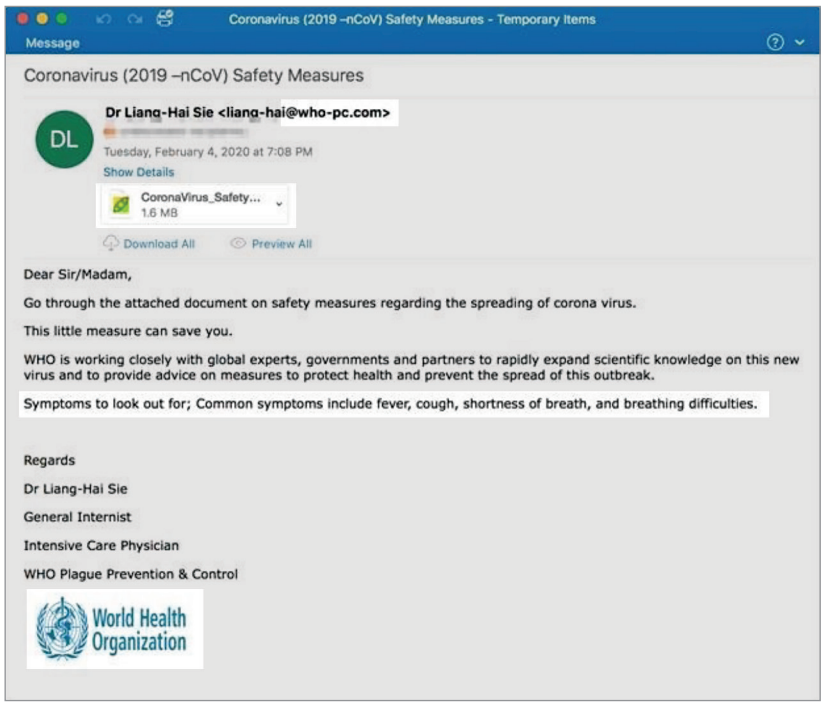
La pandemia de COVID-19 representa la mayor crisis sanitaria pública desde hace un siglo. La rápida propagación del virus por todo el planeta obligó a adaptarse a organizaciones de todo tipo. Las empresas adoptaron rápidamente nuevas políticas y tecnologías mientras se movían por la delgada línea que separa la seguridad de los trabajadores y la supervivencia de la empresa.

Los ciberdelincuentes también se adaptaron rápidamente. El miedo y la incertidumbre sobre la salud y la seguridad económica se sumaron al cambio brusco al teletrabajo, generando las condiciones ideales para que se produjeran ciberataques más eficaces. A mediados de marzo de 2020, casi el 80 % de todas las amenazas que analizamos a diario utilizaban temas relacionados con la COVID-19.

Los **VECTORES DE INFECCIÓN**, **PAYLOADS** y volumen de mensajes acumulado de estas amenazas se mantuvieron prácticamente sin cambios. Los ciberdelincuentes siguieron enviando las mismas campañas de malware y phishing. El cambio se produjo en una plantilla angustiada y en la alteración de las operaciones comerciales habituales. El resultado fue una mayor superficie de ataque y, a su vez, mayores tasas de infección.

Despertar de la primavera

En las primeras etapas de la pandemia, los señuelos se centraban en alimentar la respuesta emocional. Muchos ofrecían actualizaciones sobre cambios en la política de la empresa, las normativas oficiales o cómo estar protegido. Por ejemplo, los ciberdelincuentes se hicieron pasar por la Organización Mundial de la Salud, con la promesa de ofrecer información sobre el virus.



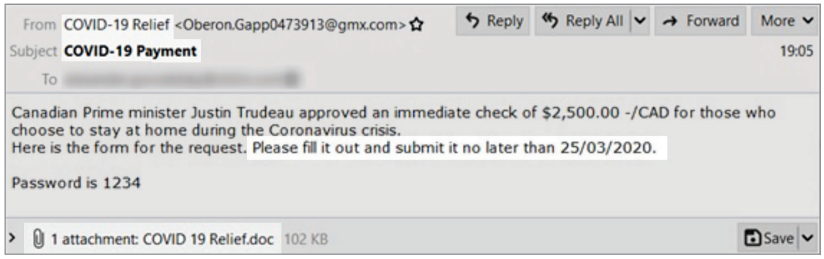
Mensajes de phishing supuestamente de la OMS

Siguiendo al dinero

A media que los gobiernos empezaron a hablar de las medidas de estímulo para evitar el colapso económico, los señuelos de los ataques empezaron a aprovechar la idea de pagos en efectivo a personas y empresas.

CARACTERÍSTICAS DESTACADAS:

- Utiliza falsificación del "display name" (nombre mostrado) y una línea de asunto para captar la atención de los destinatarios con la promesa de una ayuda financiera.
- Proporciona una fecha límite para dar la sensación de urgencia.
- El adjunto malicioso utiliza un nombre de archivo para reforzar el tema de la ayuda financiera.



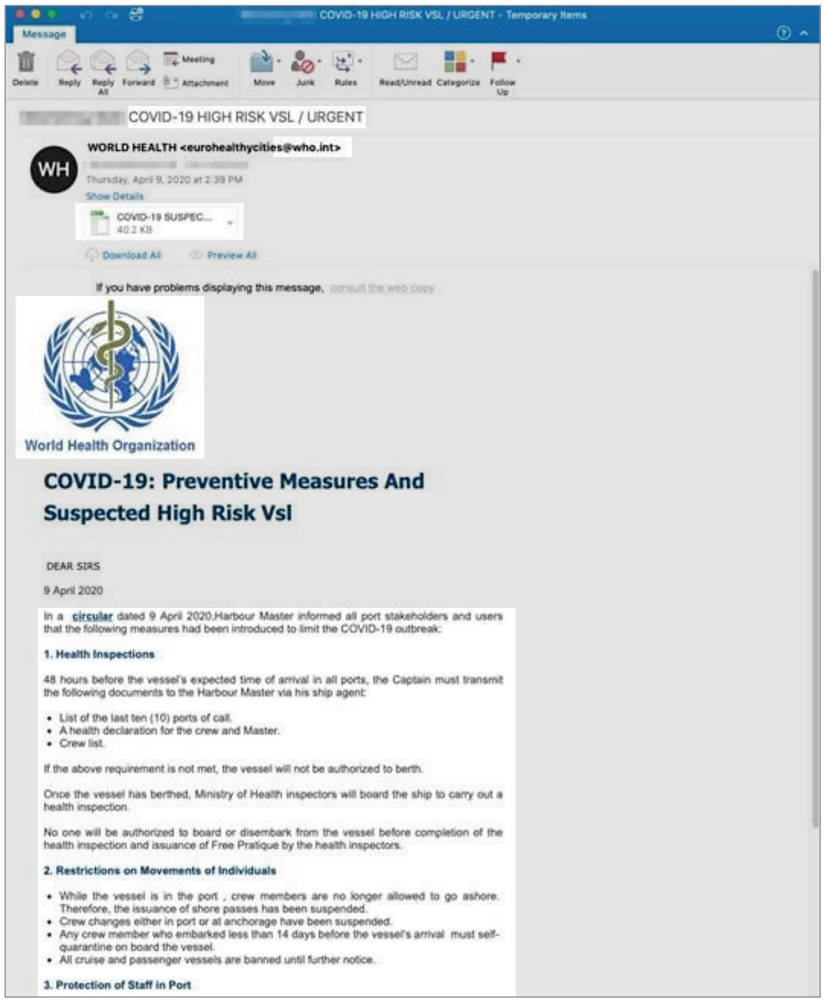
Mensajes de phishing sobre supuestas ayudas financieras por la COVID-19.

Las reglas de oro

Más adelante, a medida que los gobiernos empezaron a promulgar nuevas políticas y directrices, los señuelos comenzaron a adoptar contenido sobre cómo cumplir con ellas.

CARACTERÍSTICAS DESTACADAS:

- Transmite una sensación de urgencia y riesgo para que los lectores actúen de manera instintiva.
- Falsifica el dominio de correo electrónico de la OMS.
- El adjunto malicioso utiliza un nombre de archivo para reforzar la sensación de miedo y peligro.
- Utiliza el logotipo de la OMS para parecer oficial.
- Proporciona información real sobre la COVID-19, reforzando la aparente autoridad del mensaje.



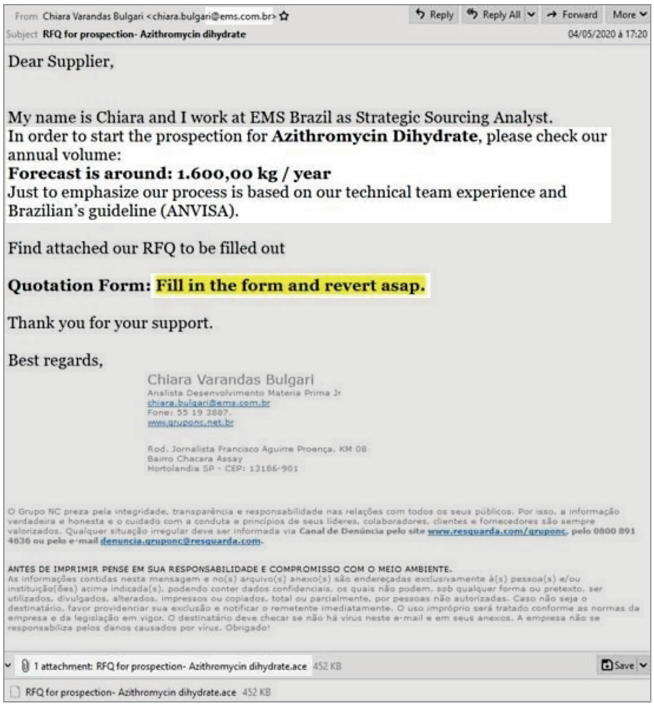
Mensajes de phishing, supuestamente de la OMS, con información detallada sobre la COVID-19.

A media que se expande el virus, también lo hacen las tácticas

La propagación de la pandemia hizo que la enfermedad acabara afectando a todas las personas en todos los rincones del planeta. Los señuelos de los atacantes aumentaron en variedad y esoterismo. Los ataques intentaban engañar a las víctimas con avisos de reparto de compras, previsiones de tratamiento de la COVID-19 y noticias sobre recortes laborales falsas.

CARACTERÍSTICAS DESTACADAS:

- Falsifica el dominio de correo electrónico de EMS, la mayor farmacéutica de Brasil.
- Utiliza temas actuales con carga emotiva para atraer la atención del lector.
- Urge al destinatario a actuar rápidamente, cortocircuitando el proceso de pensamiento deliberativo.
- Incluye un adjunto malicioso disfrazado de formulario comercial normal.


From: Chiara Varandas Bulgari <chiara.bulgari@ems.com.br>
Subject: RFQ for prospection- Azithromycin dihydrate
04/05/2020 à 17:20

Dear Supplier,

My name is Chiara and I work at EMS Brazil as Strategic Sourcing Analyst.
In order to start the prospection for **Azithromycin Dihydrate**, please check our annual volume:
Forecast is around: 1.600,00 kg / year
Just to emphasize our process is based on our technical team experience and Brazilian's guideline (ANVISA).

Find attached our RFQ to be filled out

Quotation Form: Fill in the form and revert asap.

Thank you for your support.

Best regards,

Chiara Varandas Bulgari
Analista Desenvolvimento Materia Prima Jr
chiara.bulgari@ems.com.br
Fone: 55 19 3887.
www.grupoNC.net.br

Rod. Jornalista Francisco Aguirre Proença, KM 08
Bairro Chacara Assay
Hortolandia SP - CEP: 13186-901

O Grupo NC preza pela integridade, transparência e responsabilidade nas relações com todos os seus públicos. Por isso, a informação verdadeira e honesta e o cuidado com a conduta e princípios de seus líderes, colaboradores, clientes e fornecedores são sempre valorizados. Qualquer situação irregular deve ser informada via **Canal de Denúncia pelo site www.resguarda.com/gruponc**, pelo 0800 891 4636 ou pelo e-mail denuncia.gruponc@resguarda.com.

ANTES DE IMPRIMIR PENSE EM SUA RESPONSABILIDADE E COMPROMISSO COM O MEIO AMBIENTE.
As informações contidas nesta mensagem e no(s) arquivo(s) anexo(s) são endereçadas exclusivamente à(s) pessoa(s) e/ou instituição(ões) acima indicada(s), podendo conter dados confidenciais, os quais não podem, sob qualquer forma ou pretexto, ser utilizados, divulgados, alterados, impressos ou copiados, total ou parcialmente, por pessoas não autorizadas. Caso não seja o destinatário, favor providenciar sua exclusão e notificar o remetente imediatamente. O uso impróprio será tratado conforme as normas da empresa e da legislação em vigor. O destinatário deve checar se não há vírus neste e-mail e em seus anexos. A empresa não se responsabiliza pelos danos causados por vírus. Obrigado!

1 attachment: RFQ for prospection- Azithromycin dihydrate.ace 452 KB
RFQ for prospection- Azithromycin dihydrate.ace 452 KB

Mensajes de phishing con supuesta información sobre tratamientos de la COVID-19.

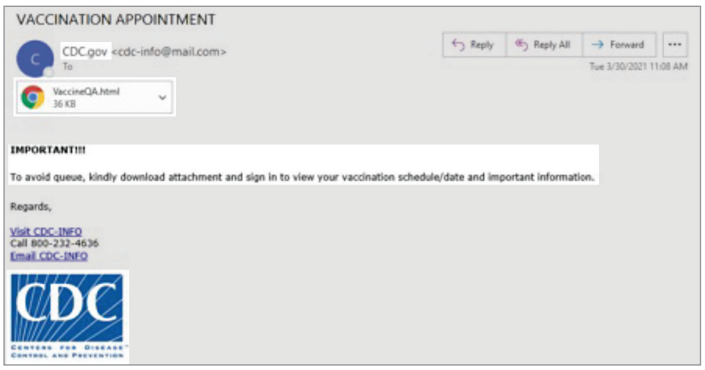
Nuevo año, temas similares

La pandemia y la respuesta global han mejorado en 2021. Y aun así, los ciberdelincuentes continúan utilizando temas relacionados con la COVID-19. Las amenazas recientes se disfrazaron de confirmación de calendarios de vacunación.

Con independencia de lo que nos tenga reservado 2021, la COVID-19 seguirá siendo un tema popular y eficaz en los ataques.

CARACTERÍSTICAS DESTACADAS:

- Utiliza "lookalike domains" (dominios parecidos) para parecer un mensaje enviado por la institución CDC.
- El archivo HTML adjunto es un sitio de phishing de credenciales.
- Promete acceso rápido a un recurso escaso (en este caso, la vacuna de la COVID-19).
- Utiliza el logotipo de CDC para reforzar la farsa.


VACCINATION APPOINTMENT
CDC.gov <cdc-info@mail.com>
To
Reply Reply All Forward
Tue 3/30/2021 11:08 AM
VaccineQA.html
36 KB

IMPORTANT!!!

To avoid queue, kindly download attachment and sign in to view your vaccination schedule/date and important information.

Regards,

Visit CDC-INFO
Call 800-232-4636
Email CDC-INFO

CDC
CENTERS FOR DISEASE CONTROL AND PREVENTION

Mensaje de phishing de robo de credenciales supuestamente de CDC.

PHISHING DE CREDENCIALES

El phishing de credenciales implica engañar a alguien para que proporcione la información de inicio de sesión de su cuenta, lo que da a los atacantes acceso a cuentas bancarias, información personal, cuentas corporativas, etc. Aunque el phishing de credenciales puede utilizar una amplia variedad de técnicas de ingeniería social, normalmente se desarrolla por correo electrónico. Haciéndose pasar por una marca o alguien de confianza de la organización de las víctimas, el atacante envía un mensaje de correo electrónico que incluye un enlace a una página de inicio de sesión falsa. Cuando el usuario introduce su nombre de usuario y contraseña, el atacante emplea la información para usurpar la cuenta de la persona.

BUSINESS EMAIL COMPROMISE (BEC)

Ataques en los que el ciberdelincuente se hace pasar por un compañero, ejecutivo o proveedor de confianza a través de una serie de técnicas de suplantación. El remitente podría pedir al destinatario que realice una transferencia bancaria, envíe un pago, desvíe la nómina, cambie los datos bancarios o envía información confidencial.

Es difícil detectar los ataques BEC porque no emplean malware ni URL maliciosas que puedan analizarse con las ciberdefensas tradicionales. En su lugar, este tipo de ataques hace uso de la suplantación de identidad y otras técnicas de ingeniería social para engañar a las personas y conseguir que realicen determinadas acciones en nombre del atacante.

Tipo de ataques

El **PHISHING DE CREDENCIALES**, tanto contra particulares como empresas, fue con diferencia el método más habitual de ataque, superando al resto de ataques combinados. Más de la mitad de las amenazas por correo electrónico en 2020 fueron intentos de phishing de credenciales.

El robo de nombres de usuario y contraseñas puede dar lugar a todo, desde fraude financiero a ciberespionaje.

Otros tipos de ataque incluyeron los dirigidos contra sistemas financieros, los que descargaban otro malware, reclutaban los sistemas infectados para redes de bots y robaban información confidencial.

BEC

BUSINESS EMAIL COMPROMISE (BEC), un tipo de estafa por correo electrónico, es una de las amenazas más dañinas desde el punto de vista financiero para empresas de todos los tamaños y sectores. Estos timos costaron a las empresas y a los particulares casi 1800 millones de dólares solamente en 2020, según el centro de denuncias de ciberdelitos (Internet Crime Complaint Center) del FBI. Esto representa el 44 % de todas las pérdidas atribuibles a la ciberdelincuencia, eclipsando a la mayoría del resto de tipos de ciberdelitos[5].

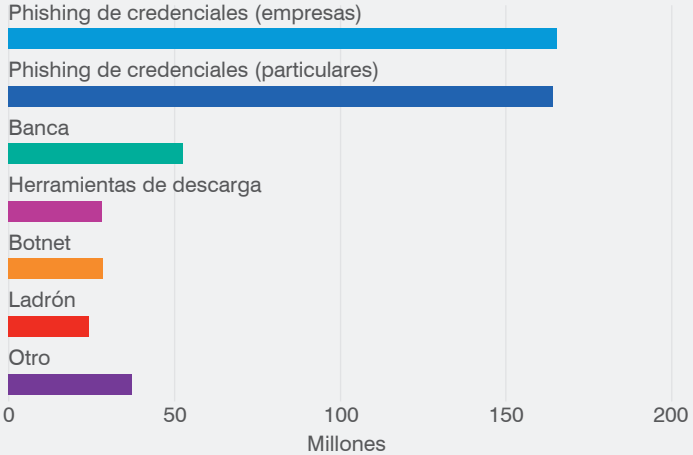
En Proofpoint llevamos el enfoque centrado a las personas a las estafas BEC, conceptualizado a través de un **marco** compuesto por tres niveles:

- Identidad: por quién se hacen pasar los ciberdelincuentes
- Engaño: las técnicas que utilizan
- Tema: la categoría de fraude que intentan

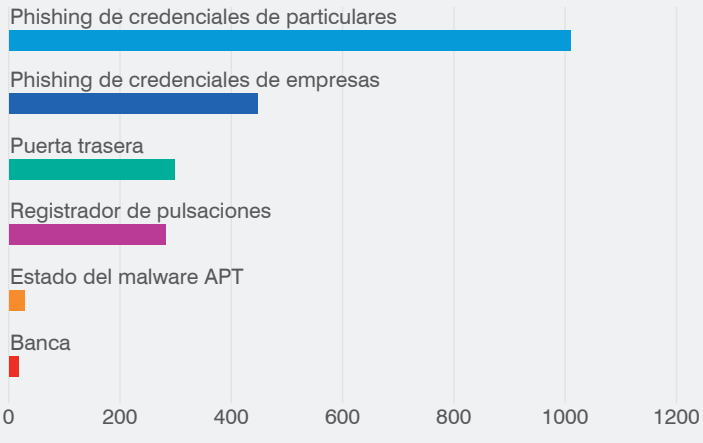
El engaño pertenece por lo general a dos categorías: técnicas de suplantación o compromiso. Definimos la suplantación como un ataque en el que el ciberdelincuente altera uno o varios de los encabezados de mensajes para enmascarar su origen. El compromiso es un ataque en el que el ciberdelincuente consigue acceder a un buzón de correo legítimo.

5 FBI. "2020 Internet Crime Report" (Informe sobre delitos en Internet de 2020). Marzo de 2021.

Tipo de ataques, por volumen de mensajes (2020)
El phishing de credenciales de particulares y de empresas fue por un amplio margen el tipo de ataque más común.



Variación (2020 frente a 2019)



Nuestro marco hace hincapié en gran medida en los temas porque genera inteligencia procesable, incluidos los distintos tipos de fraude utilizados, como **fraude de facturas**, redirección de nóminas y extorsión.

Las estafas BEC que tienen éxito emplean técnicas de ingeniería social. Esto puede producirse en forma del nombre que se muestra en el mensaje, el tono o los adjuntos utilizados para hacer que el mensaje parezca más creíble.

En uno de los intentos de fraude más elaborados observados durante 2020, un ciberdelincuente al que identificamos como TA2520 utilizó ingeniería social en varias campañas. A menudo suplantando a miembros de la dirección a través de la falsificación del "display name" (nombre mostrado), el ciberdelincuente solicitó a los destinatarios que transfieran dinero para lo que falsamente se presentó como un acuerdo de adquisición corporativa.

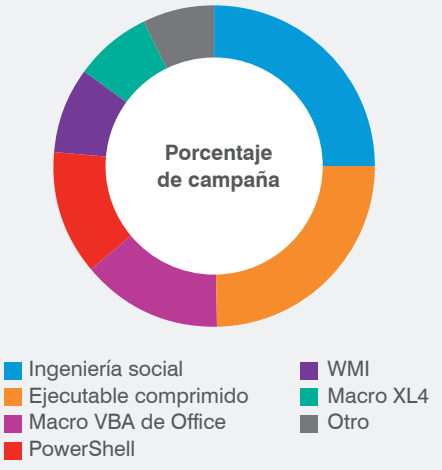
Estos intentos suponían sumas de más de 1 millón de dólares y a menudo incorporaban eventos actuales. Algunos mencionaban las restricciones de la COVID-19, por ejemplo, y estímulos para las vacunas y recuperación económica.

Otro actor de amenazas digno de mención que participó en estafas BEC en 2020 es TA2519, que lanzó ataques multifase. En la primera fase del ataque, el ciberdelincuente utilizó principalmente señuelos relacionados con la COVID-19 para robar las credenciales de las víctimas. En la segunda fase, TA2519 utilizó las credenciales robadas para secuestrar la cuenta de la víctima y usarla para facturar de manera fraudulenta a una segunda víctima, un ataque conocido como fraude de facturas de proveedores.

Una factura fraudulenta puede parecer que procede de alguien de confianza, como un compañero de trabajo o de un desconocido. Los de mayor éxito parece que aprovechan las relaciones con los proveedores, que incluyen a cualquier persona o empresa que venda productos o servicios. Estos ataques pueden terminar costando a empresas de todos los lugares de decenas de miles a varios millones de dólares.

Cuota de las campañas

Un mensaje de correo electrónico malicioso puede contener múltiples técnicas, como ingeniería social destinada a persuadir al usuario a descargar y abrir un adjunto comprometido.



Técnicas de ataque

Los ciberdelincuentes utilizan una amplia variedad de técnicas para esquivar los controles de seguridad, engañar a las víctimas para que activen el ataque e infectar los sistemas. Pero un denominador común es el uso de ingeniería social.

Utilizan líneas de asunto atractivas, reclamos convincentes y el adecuado grado de selección del objetivo para invitar al destinatario a actuar. Como se explica en **COVID-19: Cómo los ciberdelincuentes han aprovechado la pandemia, en la página 15**, la pandemia fue el tema más popular de 2020.

Estas son algunas otras tendencias importantes.

Ejecutables comprimidos

Casi 1 de cada 4 campañas de ataques utilizaron archivos ejecutables comprimidos para ocultar malware. Este método confía en que la víctima interactúe con un adjunto malicioso, como una presentación de diapositivas de PowerPoint u hoja de cálculo de Excel para ejecutar la payload (carga maliciosa). Puesto que solo se ejecuta cuando una persona desbloquea el archivo, se trata de una forma eficaz de evadir la detección de malware automatizada.

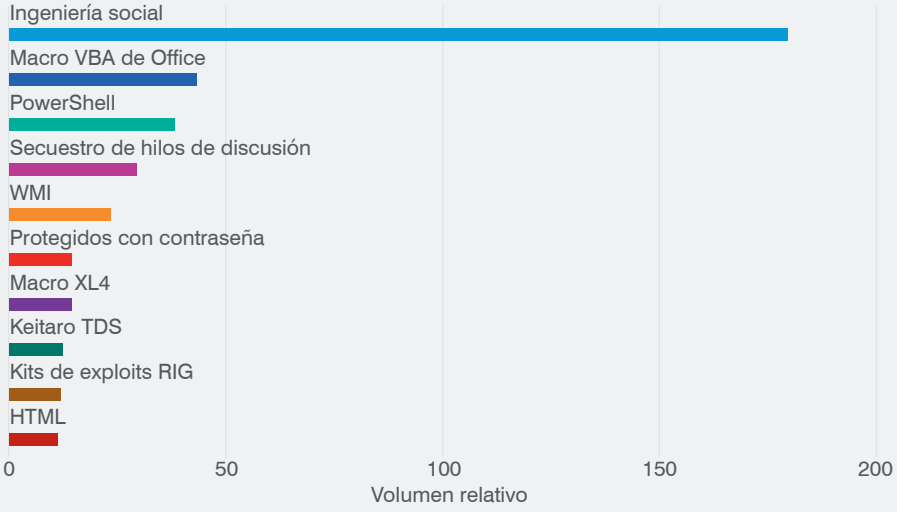
Excel 4.0

En el transcurso de 2020, los ciberdelincuentes empezaron a utilizar **cada vez más** macros de Excel 4.0 (XL4) para distribuir malware. En el proceso, se alejaron ligeramente de las macros de Office Visual Basic para Aplicaciones. (A pesar de todo, esta última sigue siendo una técnica mucho más utilizada).

Los ataques basados en XL4 aprovechan un antiguo conjunto de funciones de Excel, por lo que podría resultar sorprendente ver un repunte repentino de esta técnica. Una posibilidad: cobertura de detección limitada de XL4 en los sistemas de seguridad modernos. Aunque sigue admitiendo macros de XL4, el gigante de software ha **instado** a los clientes a migrar a la última versión de VBA.

Principales técnicas de ataque, volumen de mensajes relativo

La ingeniería social fue de lejos la técnica de ataque más empleada. Y todas las demás técnicas incluyen algún elemento de ingeniería social.



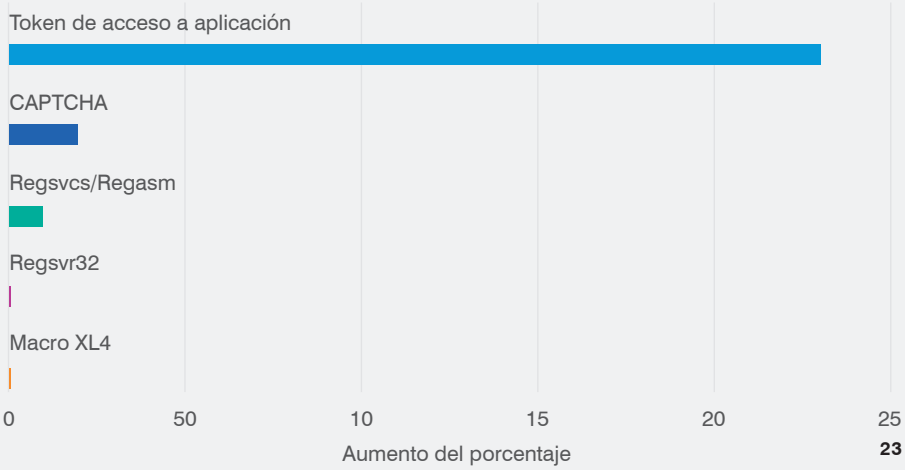
CAPTCHA

Los ataques que utilizan técnicas de CAPTCHA se dispararon en 2020. (Como se indica en la **Sección 1: Vulnerabilidades, en la página 6**, los usuarios también fueron más vulnerables a esta técnica que en 2019).

El actor de amenazas con motivaciones económicas identificado como TA564, utiliza este método en campañas de malware contra organizaciones de Canadá. Este atacante utiliza CAPTCHA para asegurarse que la víctima está ubicada en la región objetivo antes de actuar. En caso contrario, el ataque se detiene.

Aumento del porcentaje por volumen

Los ataques que hacen un uso indebido de tokens de acceso a las apps aumentaron más de un 20 %, y los ataques basados en CAPTCHA crecieron un 2 %, lo que sugiere un cambio a ataques a la nube y activados por humanos.



TROYANOS BANCARIOS
Históricamente, este tipo de malware se ha centrado en robar credenciales de inicio de sesión bancarias, por lo general redirigiendo a una versión falsa del sitio web de un banco o inyectando formularios de inicio de sesión falsos en el sitio real. Recientemente, muchos troyanos bancarios también se han utilizado como precursores de ataques de ransomware de gran repercusión.

CARGADORES/DESCARGADORES
El malware cargador o *loader* descarga código malicioso adicional alojado en Internet. Muchos tipos distintos de malware, como los troyanos bancarios y de acceso remoto, tienen ahora esta función. Los *droppers* son similares a los *loaders*, pero en lugar de descargar código adicional, cifran y ejecutan código que se incluyó en la payload de malware inicial.

DRIDEX
Dridex, el troyano bancario modular desarrollado y controlado por el grupo apodado "Evil Corp", tuvo un mal año en 2019 antes de resurgir en 2020. Este malware está estrechamente relacionado con el despliegue posterior del ransomware Bitpaymer/Doppelpaymer.

QBOT
Qbot es un troyano modular que ha visto ampliada su funcionalidad desde que apareciera en 2007. Al igual que otros troyanos bancarios incluidos aquí, Qbot es ahora principalmente un ladrón de información y un cargador de payloads de seguimiento como Cobalt Strike.

ZLOADER
Zloader es un troyano bancario más antiguo que apareció con variantes actualizadas en 2020 y sigue siendo desarrollado activamente y adoptado de forma generalizada.

TROYANOS DE ACCESO REMOTO
Los troyanos de acceso remoto ofrecen a los ciberdelincuentes control administrativo de un sistema infectado. Por lo general, cuentan con un conjunto de funciones menos sofisticado, pero conservan la capacidad para vigilar los sistemas comprometidos, así como de descargar y ejecutar malware.

Herramientas de ataque

Los **TROYANOS BANCARIOS**, que roban información financiera y pueden actuar como un **CARGADOR** para otro malware, fueron los tipos más populares de malware enviados por ciberdelincuentes. Las principales variantes son **DRIDEX**, **QBOT** y **ZLOADER**.

Aunque la actividad de la red de bots Emotet descendió bruscamente en 2020, siguió siendo uno de los grupos más activos. (Para obtener más información sobre Emotet, consulte **Caso de estudio de malware: Emotet en 2020 en la página 28** y **Metamorfosis del malware: Por qué las etiquetas ya no significan lo que antes, en la página 26**.)

Ganando la carrera RAT

Los **TROYANOS DE ACCESO REMOTO** (RAT) representaron casi un cuarto de todas las campañas que utilizaron malware. Los ciberdelincuentes pueden utilizar los RAT para hacerse con el control de la máquina de una víctima y robar datos bancarios, recopilar información y propagarse por el entorno comprometido. Ejemplos de RAT populares son: Ave Maria, NanoCore RAT y Remcos.

Aunque las campañas de RAT gozaron de popularidad en 2020, fueron menos eficaces que las campañas que utilizaron otras familias de malware. Los usuarios fueron más propensos a hacer clic o a interactuar con los mensajes de correo electrónico con Emotet, puertas traseras de malware y malware bancario.

Una lección sobre ransomware: los atacantes ponen a las escuelas en el punto de mira en el año de la educación a distancia.

Como ocurrió con las empresas, la pandemia forzó a empresas, padres, profesores y escuelas a trabajar de forma remota. Las clases se desarrollan a través de software de videoconferencia. Los estudiantes interactuaron con sus compañeros y educadores online, confiando totalmente en recursos digitales.

Los ciberdelincuentes demostraron una rápida adaptación. Aprovecharon el cambio mediante el uso de señuelos temáticos como aulas y otros recursos escolares para distribuir malware y, en muchos casos, alterar la educación online.

Una campaña de octubre de 2020 fingía proceder de un padre o tutor enviando tareas en nombre de un estudiante[6]. El correo electrónico afirmaba que el niño había tenido problemas técnicos. El documento malicioso adjunto al mensaje distribuía Cryptme, una sencilla variante de ransomware que cifra archivos del ordenador de una víctima.

6 https://www.nbcnews.com/tech/security/parents-end-chain-ransomware-hit-kids-schools-rcna646

Mensaje de correo electrónico haciéndose pasar por un progenitor.

Los ataques de ransomware contra colegios aumentaron en 2020. Con estudiantes de todo el mundo aprendiendo desde sus pantallas, dichos ataques alteraron un ya de por sí tenso entorno de trabajo.

Los colegios **siguen siendo objetivos** de los ciberdelincuentes, y prevemos que seguirá siendo así durante todo 2021.

Cobalt Strike

A menudo, los ciberdelincuentes se apropian de herramientas de software tipo RAT que tienen usos legítimos para los departamentos de TI, técnicos de pruebas de seguridad y usuarios avanzados. Algunos están incorporados en los sistemas de los usuarios, lo que permite a los atacantes aprovechar los recursos internos ("live off the land") del entorno en el que buscan habitar.

Un ejemplo es Cobalt Strike, una herramienta de seguridad comercial diseñada para ayudar a las organizaciones a probar las debilidades del sistema a través de ataques simulados. (Se conocen como ejercicios de "equipo rojo", mediante los que alguien de la organización o que trabaja para ella juega el papel de ciberintruso).

Pero cada vez más ciberdelincuentes utilizan la herramienta para ataques reales. El volumen de amenazas que distribuyen Cobalt Strike como payload principal aumentó un 161 % en 2020.

Otros investigadores de seguridad han observado las mismas tendencias a medida que más ciberdelincuentes adoptan herramientas de hackeo de código abierto. Por ejemplo, TA572 envió mensajes de correo electrónico con temas de facturas que incluían documentos de Excel y Word maliciosos utilizando macros de Microsoft Excel 4.0 (XL4) para descargar Cobalt Strike.

Metamorfosis del malware: por qué las etiquetas ya no significan lo que antes

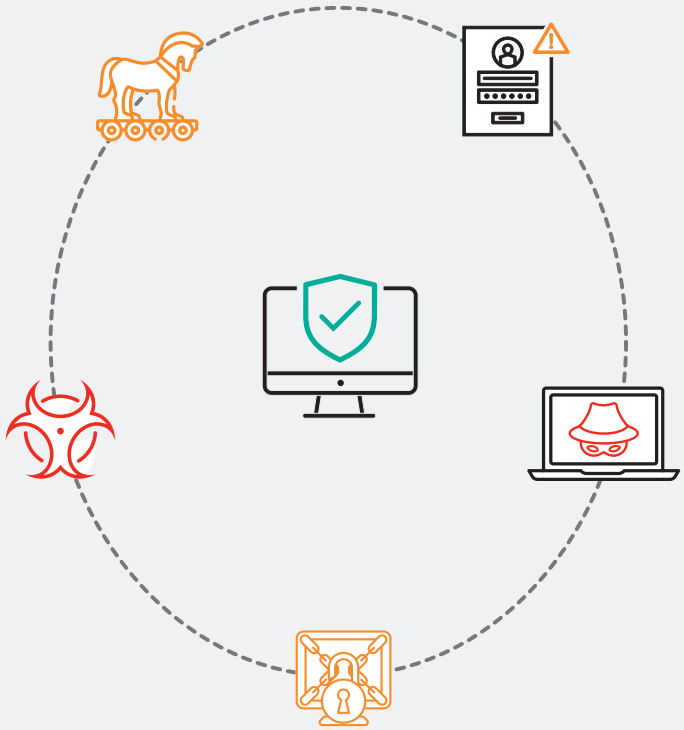
Clasificar el malware puede ser útil para comprender el ámbito y la naturaleza de las amenazas que se dirigen contra los usuarios. Pero las etiquetas no siempre dicen la verdad. Las variantes de malware mejoran y se refuerzan. Los atacantes las utilizan de formas inesperadas. Y como un grupo teatral versátil cuyos actores pueden sustituirse entre ellos cuando alguno cae enfermo, las herramientas de malware a menudo se intercambian y se utilizan en combinaciones distintas en función de las necesidades.

El uso de distintas variantes de malware conjuntamente es una práctica antigua que tiene una finalidad importante para los ciberdelincuentes. Les ofrece la flexibilidad de disponer de la herramienta adecuada para cada fase del ataque. Proporciona redundancia y permite al atacante persistir en un entorno, incluso si se detecta algún malware. Y amplía la vida del malware más antiguo que podrían detectar las gateways de seguridad, pero no como una descarga secundaria a una máquina ya infectada.

Piense en Emotet, el versátil y prolífico malware calificado como "el malware más peligroso del mundo" antes de que una redada de las fuerzas de seguridad a nivel mundial desmantelara su infraestructura en enero. Emotet apareció en 2014 como un simple troyano bancario que robaba credenciales de cuentas de un grupo reducido de objetivos en Alemania y Austria.

Rápidamente adquirió funciones de descargador, convirtiéndolo en una herramienta útil para descargar malware secundario. Con el tiempo, otras funciones lo hicieron todavía más útil para los ciberdelincuentes, más difícil de detectar y más capaz de propagarse y fácil de ampliarse.

Al final se convirtió en una red de bots versátil. Una red de máquinas infectadas que podría utilizarse como un ejército de zombis para dar cobertura a una amplia variedad de ataques en todo el mundo.



Quién es quién en el panorama de amenazas: principales actores de amenazas

Identificamos 69 actores de amenazas activos en 2020. A continuación incluimos los más activos, en base al volumen de mensajes. Como los atacantes de mayor volumen, los cinco son lo que los investigadores llaman ciberdelincuentes con motivaciones económicas, lo que quiere decir que se centran en los delitos financieros.

El arte y la ciencia de la atribución

La primera pregunta que se hace cuando ocurre cualquier delito, físico o cibernético es: *¿quién lo hizo*? Para los investigadores de seguridad, la respuesta no es siempre clara.

Cada ataque deja un rastro de migajas digitales: el malware utilizó direcciones IP de servidores de mando y control, metadatos de malware, las fuentes y los idiomas utilizados en los señuelos de correo electrónico, el comportamiento, los ajustes de configuración y otros indicios. Juntando todas estas piezas y buscando patrones entre los ataques, los investigadores consiguen un "retrato robot" de quién está detrás de un ataque. Los investigadores de amenazas llaman a este proceso "atribución".

Agrupamos los ciberdelincuentes por sus campañas y comportamientos en lugar de por nacionalidad u organización, aunque algunos son atribuidos individualmente por otros equipos de investigación y fuerzas de seguridad. Pero la atribución definitiva no siempre es posible.

La razón es porque el ecosistema de ciberdelincuentes es amplio y está muy fragmentado.

Algunas organizaciones criminales funcionan con franquicias. Un **ACTOR DE AMENAZAS** crea un "producto" de malware y configura la infraestructura como paquete o servicio fácil de utilizar. Los ciberdelincuentes de niveles inferiores pueden alquilar el servicio para sus ataques, pagar por usarlo durante un período de tiempo determinado o conseguir una parte por cada compromiso que se consiga. En otros casos, actúan como distribuidores, envían mensajes de correo electrónico con el malware y ganan una comisión por cada infección.

Puesto que ciberdelincuentes distintos pueden utilizar las mismas herramientas e infraestructura, los investigadores no siempre pueden atribuir un ataque a un ciberdelincuente específico. Pero el análisis de los ataques que pueden atribuirse a los principales autores de amenazas (como hacemos en todo el informe) sigue siendo una parte fundamental del puzle de la seguridad.

ACTOR DE AMENAZAS
Se trata de un término que los investigadores de amenazas utilizan para describir a un ciberdelincuente o grupo de ciberdelincuentes. Puede tratarse de atacantes financiados por el Estado, organizaciones cibercriminales y, en ocasiones, hacktivistas.

TA542

Este es el grupo ciberdelictivo detrás de la infame red de bots Emotet. A pesar de los cinco meses de **paréntesis** de la red de bots en 2020, las actividades del grupo fueron responsables de casi el 10 % del tráfico de correo electrónico malicioso a nivel mundial. Una redada de las fuerzas de seguridad a nivel internacional consiguió desmantelar Emotet en enero de 2021 y en ella se detuvieron a varios de los supuestos miembros del grupo. Desde entonces, las actividades del grupo se han reducido hasta casi desaparecer.

Caso de estudio de malware: Emotet en 2020

Emotet apareció por primera vez como troyano bancario en 2014 y evolucionó hasta convertirse en unas de las redes de bots más tristemente famosas de 2020.

En febrero de 2020, la actividad de Emotet se detuvo durante cinco meses antes de volver en julio. A pesar del tiempo de inactividad, Emotet continuó siendo la amenaza más prolífica de 2020.

Era conocida por su volumen y distribución masiva de mensajes de correo electrónico, utilizando señuelos de **múltiples temas** que en ocasiones coincidían con noticias y eventos mundiales como la COVID-19.

En **octubre de 2020**, un mes antes de que comenzaras las elecciones presidenciales de Estados Unidos, Emotet comenzó a utilizar temas políticos en sus señuelos de phishing. Emotet atacó a organizaciones de América del Norte, Europa, Sudeste Asiático y Oceanía. Las payloads de segunda fase incluían Qbot y The Trick.

Una vez que el grupo conseguía entrar en el entorno de una víctima, vendía el acceso a otros ciberdelincuentes o grupos, lo que aumentaba el compromiso, incluidos costosos y perturbadores ataques de ransomware.

MALVERTISING

El malvertising o publicidad maliciosa incrusta código malicioso en anuncios online. Estos anuncios a menudo aparecen en sitios web legítimos y de toda confianza, lo que los hace difíciles de bloquear en el gateway o endpoint.

TA567

Este grupo ciberdelictivo utiliza publicidad maliciosa, también conocida como **MALVERTISING**, a través de Keitaro, un sistema de distribución de tráfico (TDS) legítimo que ayuda a los anunciantes a dirigir anuncios online redirigiendo a los visitantes a los sitios web adecuados. En lugar de enviar correo electrónico malicioso, TA567 emplea el TDS Keitaro para distribuir contenido malicioso a través de publicidad legítima, que en última instancia se traduce en una amplia variedad de malware en sitios web inocentes. Los mensajes de correo electrónico inofensivos pueden contener enlaces a sitios infectados con estos bloques de anuncios comprometidos, lo que ofrece a Proofpoint visibilidad de la actividad de este atacante. Estas amenazas a menudo aprovechan técnicas de geofencing para adaptar los anuncios maliciosos a zonas geográficas específicas.

TA544

Este ciberdelincuente roba dinero a través de troyanos bancarios y otro tipo de malware. Es responsable de poco menos del 4 % del volumen total de mensajes de correo electrónico mundial. TA544 utiliza por lo general adjuntos de Microsoft Office que contienen macros maliciosas, engañando a los destinatarios para que abran el adjunto y activen la macro para descargar la payload. El ciberdelincuente ha atacado varios sectores de distintas regiones, como Italia y Japón.

THE TRICK

Desde su aparición en 2016, este troyano bancario se ha convertido en una herramienta versátil que puede descargar otro malware, propagarse a través de una red, actualizarse, etc.

BAZALOADER

Descubierto por primera vez en abril de 2020, BazaLoader se utiliza para descargar otro malware. Aunque relativamente nuevo, hemos visto al menos seis variantes del malware, un indicio de que se sigue desarrollando de forma activa.

TA505

Este influyente grupo ciberdelictivo es conocido por lanzar campañas de correo electrónico malicioso a una escala sin precedentes. El grupo cambia sus tácticas, técnicas y procedimientos (TTP) y se consideran **generadores de tendencias** en el mundo de la ciberdelincuencia. TA505 es un grupo ciberdelictivo de igualdad de oportunidades, que dirige sus ataques contra una amplia variedad de sectores y zonas geográficas. En 2020, TA505 centró principalmente sus esfuerzos en EE. UU., Canadá y zonas de Europa en las que se habla alemán. Aunque en ocasiones se ha vinculado con Evil Corp., un grupo ciberdelictivo ubicado en Rusia, lo consideramos un grupo independiente.

TA800

Este grupo distribuye malware bancario y cargadores de malware, como **THE TRICK** (también conocido como TrickBot) y **BAZALOADER**. Estos cargadores están estrechamente vinculados con ataques de ransomware de segunda fase que utilizan Conti y Ryuk, respectivamente. Fue uno de los primeros actores de amenazas que empezaron a utilizar BazaLoader en abril de 2020, meses antes que otros grupos. Dirige sus ataques contra una amplia variedad de sectores en América del Norte, siendo responsable de aproximadamente el 2 % del volumen total de correo electrónico malicioso.

SECCIÓN 3

Privilegios

Evaluar los privilegios es otra forma de determinar cuánto daño podría provocar un ataque que tuviera éxito. Comprometer a usuarios con privilegios elevados ofrece al ataque acceso a información confidencial y valiosa.

Las amenazas internas, ya surjan de usuarios maliciosos, negligentes o comprometidos, son otra forma de abuso de privilegios. Para muchas organizaciones, un cambio casi de un día para otro al teletrabajo complicó las tareas de supervisar y mitigar las amenazas internas.

Las organizaciones han examinado más de cerca los dispositivos USB, la copia de archivos o carpetas de gran tamaño (en particular a horas intempestivas), evaluando los servicios de intercambio de archivos y las actividades que pudieran sortear la herramienta de supervisión de usuarios. El número de organizaciones que definen alertas DLP para estas actividades aumentó de manera importante en relación a niveles pre-COVID-19.

Principales alertas de gestión de amenazas internas

ACCIÓN	PUESTO	VARIACIÓN DESDE 2019
Conexión de dispositivos USB no registrados	1	▲
Copia de un archivo o carpeta de gran tamaño	2	▲
Filtración de un archivo supervisado a la web mediante subida	3	▼
Apertura de un archivo con contraseñas en formato de texto no cifrado	4	▲
Descarga de un archivo con una extensión potencialmente maliciosa	5	▼
Copia de un archivo o carpeta de gran tamaño a horas intempestivas	6	▲
Filtración de un archivo a un dispositivo USB no registrado	7	▼
Instalación de herramientas de hackeo o de suplantación de identidad	8	▼
Acceso a servicios cloud de carga e intercambio	9	▲
Apertura de una carpeta de agente de ObservelT	10	▲

Conclusiones y recomendaciones

Las amenazas actuales requieren una estrategia centrada en las personas para garantizar la seguridad de los usuarios.

Los atacantes no ven el mundo como un diagrama de red. Solo ven organigramas, conexiones, relaciones y accesos.

Despliegue una solución que permita ver a quién se dirige el ataque, cómo actúa y si la víctima ha hecho clic. Tenga en cuenta el riesgo individual que representa cada usuario, por ejemplo, qué tipo de ataques recibe, a qué datos tiene acceso y si suele ser presa de los ciberdelincuentes.

Recomendamos lo siguiente para una defensa centrada en las personas.

Vulnerabilidad

La mayoría de los ciberataques no prosperan a menos que alguien caiga en ellos. La mitigación de vulnerabilidades empieza con formación para concienciar en materia de seguridad y controles basados en riesgos. Recomendamos lo siguiente:

- **Forme a los usuarios para que detecten y denuncien si hay correo electrónico malicioso.** La formación continua y los ataques simulados pueden frustrar muchos ataques y permiten identificar a las personas que son particularmente vulnerables. Las mejores simulaciones imitan las técnicas de ataque del mundo real. Busque soluciones conforme a las tendencias actuales y con la inteligencia más actualizada.
- Al mismo tiempo, **dé por hecho que en algún momento los usuarios harán clic en enlaces peligrosos.** Los atacantes siempre encontrarán nuevas formas de aprovecharse de la naturaleza humana. Encuentre una solución que neutralice las amenazas mediante la aplicación de capas de seguridad a sus usuarios más vulnerables.
- **Aísle las URL y los sitios web peligrosos.** Mantenga el contenido de los sitios web peligrosos fuera del entorno. El aislamiento web 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.

Ataques

Los ciberataques son inevitables. Pero con el enfoque, las herramientas y las políticas adecuadas, pueden ser un riesgo gestionable. Estas son nuestras recomendaciones para prevenir, detectar y responder a los ataques.

- **Construya una defensa sólida contra estafas por correo electrónico.** Detectar el fraude por correo electrónico puede ser difícil. Invierta en una solución que le permita administrar el correo electrónico con políticas personalizadas de cuarentena y bloqueo. Su solución debe analizar tanto el correo electrónico externo como el interno; los atacantes pueden utilizar cuentas comprometidas para engañar a los usuarios dentro de la misma organización.
- **Evite el ransomware evitando la infección inicial.** Los distribuidores de ransomware buscan ahora objetivos de gran valor ya infectados con un troyano o un cargador. Evite convertirse en víctima del ransomware impidiendo la entrada de estas variantes de malware más comunes.
- **Proteja las cuentas cloud de la usurpación y de las apps maliciosas.**
- **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 que aprenda de ellas.

Privilegios

El objetivo principal de todos los ciberdelincuentes es acceder a datos, sistemas y otros recursos. Cuantos más privilegios tenga la víctima, mayor será la capacidad de acceso de los atacantes, y mayor el daño que puede infringir. Para administrar los privilegios y asegurarse de que no se hacen un uso indebido de ellos, recomendamos:

- **Desplegar un sistema de gestión de amenazas internas** para impedir, detectar y responder a usuarios maliciosos, negligentes y comprometidos (los casos más habituales de abuso de privilegios) en el menor tiempo posible.
- **Responder rápidamente al abuso de privilegios potencial** con herramientas que puedan ayudarle a determinar lo que ha pasado antes, durante y después del incidente y conocer la intención del usuario, sin los falsos positivos habituales.
- **Aplicar políticas de seguridad** con formación de los usuarios, recordatorios en tiempo real y bloqueo en caso necesario.

Descubra cómo puede ayudarle Proofpoint a evaluar y mitigar la vulnerabilidad, los ataques y los privilegios con un enfoque centrado en las personas de los mayores desafíos actuales de seguridad y cumplimiento de normativas en **www.proofpoint.com/es**.

MÁS INFORMACIÓN

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

ACERCA DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentran más de la mitad del Fortune 1000, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.

©Proofpoint, Inc. Proofpoint es una marca comercial de Proofpoint, Inc. en Estados Unidos y en otros países. Todas las marcas comerciales mencionadas en este documento son propiedad exclusiva de sus respectivos propietarios.

proofpoint.

0400-005-01-01 07/21