HP WOLF SECURITY

Informe de amenazas. Tipos y estadísticas.

CUARTO TRIMESTRE DE 2022

Panorama de amenazas

Te presentamos la edición del cuarto trimestre de 2022 del informe sobre amenazas de HP Wolf Security

Cada trimestre, nuestros expertos en seguridad destacan campañas, tendencias y técnicas notables de malware que HP Wolf Security identifica. Al aislar las amenazas que han evadido las herramientas de detección y han llegado a los dispositivos, HP Wolf Security ofrece una visión de las últimas técnicas que utilizan los ciberdelincuentes, dando a los equipos de seguridad el conocimiento necesario para combatir las amenazas emergentes y mejorar sus posturas de seguridad.[1]

Resumen

Amenazas por correo electrónico que eludieron la seguridad de la puerta de enlace

Un 13 %

- Por tercer trimestre consecutivo, los archivos comprimidos han sido el tipo de archivo más utilizado para distribuir malware (42 %). El malware de archivos comprimidos ha aumentado un 20 % desde el primer trimestre de 2022, ya que los atacantes se alejan de los formatos de archivo de Office hacia alternativas que no dependan de macros, como los archivos de imagen de disco (IMG e ISO).
- En el cuarto trimestre, una oleada de atacantes imitaron proyectos de software conocidos para engañar a los usuarios y que estos infectaran sus ordenadores con malware. Los ataques ocurren cuando los usuarios hacen clic en anuncios de buscadores que conducen a sitios web maliciosos casi idénticos a los sitios web legítimos.
- Los atacantes eluden los controles de seguridad de la red perimetral, como los escáneres de puerta de enlace de correo electrónico, al incluir enlaces maliciosos en archivos PDF. El 13 % de las amenazas por correo electrónico identificadas por HP Wolf Security había evadido uno o varios escáneres de puerta de enlace de correo electrónico, poniendo de relieve las limitaciones de los controles de seguridad basados en la detección.
- Los responsables de las amenazas experimentan con códigos QR en sus señuelos para robar datos de las tarjetas de crédito y débito de las víctimas. En este tipo de ataque, es más probable que las víctimas accedan a sitios web maliciosos desde sus teléfonos móviles, que pueden carecer de protección frente a la suplantación de identidad.

Amenazas notables

Los atacantes utilizan señuelos en formato PDF para distribuir malware y eludir la seguridad del correo electrónico

Debido al declive de documentos y hojas de cálculo de Office como método para distribuir malware a los ordenadores, observamos que los atacantes experimentaban con técnicas alternativas, como el contrabando de HTML y los archivos de acceso directo maliciosos (LNK). El contrabando de HTML es eficaz cuando se trata de eludir la seguridad de la puerta de enlace de correo electrónico, porque los atacantes pueden cifrar su malware dentro de los archivos adjuntos en HTML, evitando que los escáneres inspeccionen el contenido malicioso. A pesar de que seguimos observando cómo este método se utiliza ampliamente, los atacantes siempre están probando técnicas nuevas para evadir la detección. Una técnica que cobró impulso en diciembre fueron los documentos PDF. HP Wolf Security observó un aumento del 38 % en el malware en formato PDF en el cuarto trimestre en comparación con el trimestre anterior.

La cadena de infección comienza con un atacante que envía un documento PDF a una víctima por correo electrónico. Al igual que con el contrabando de HTML, los atacantes imitan marcas conocidas para captar la atención del destinatario. La imagen 1 muestra un ejemplo de un visualizador de documentos online falso observado en el cuarto trimestre, una conocida plantilla de señuelo. El documento PDF contiene un enlace que lleva a un archivo ZIP alojado en un servidor web. Como el archivo PDF adjunto no contiene ningún código ejecutable, es menos probable que lo detecten las puertas de enlace de correo electrónico. Para aumentar la probabilidad de evadir la detección, los atacantes también cifran el archivo comprimido y proporcionan la contraseña y las instrucciones en el documento PDF que envían al destinatario.

A menudo, el archivo ZIP que se descarga contiene un archivo de imagen de disco (.ISO o .IMG) que a la vez contiene un archivo de acceso directo. El destinatario tiene que abrir el archivo de acceso directo para desencadenar la infección. Hemos visto cómo utilizan esta técnica para distribuir familias de malware, incluidos QakBot e IcedID, ambos conocidos precursores de ataques de ransomware operados por humanos.[2,3]

El número de pasos para desencadenar una infección a través de archivos adjuntos maliciosos PDF y HTML es mayor que el número de documentos de Office habilitados con macros. Pero a pesar de que se requiere una mayor interacción por parte del usuario para ejecutar el malware, los atacantes siguen poniendo en peligro las redes porque los usuarios caen en estas trampas.

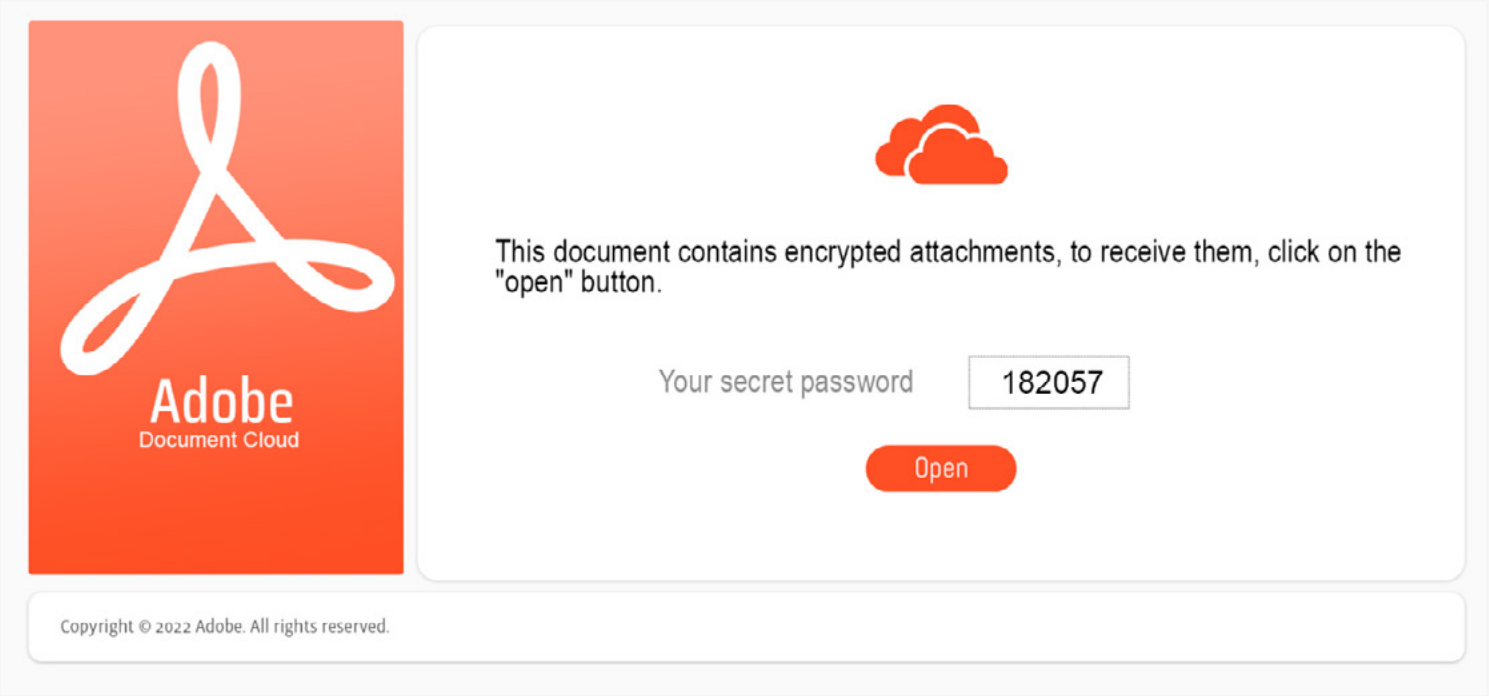


Imagen 1: Visualizador de documentos falso utilizado para engañar a las víctimas con el fin de que infecten sistemas con QakBot.

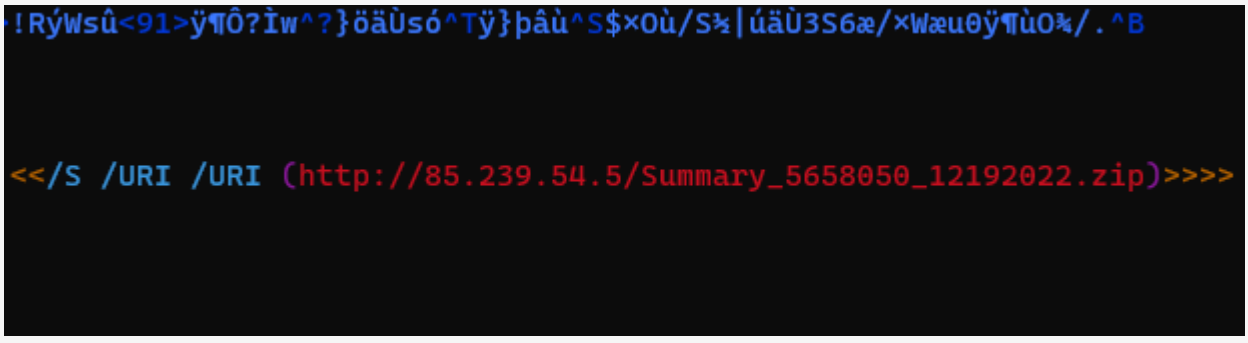


Imagen 2: Enlace integrado en un archivo PDF que descarga un archivo comprimido malicioso al hacer clic en él.

Los atacantes experimentan con códigos QR para robar información confidencial

A finales de noviembre de 2022, detectamos una campaña inusual de suplantación de identidad en chino que abusaba de los códigos QR para robar datos de tarjetas de crédito y otra información confidencial.[4] Descubrimos la campaña a través de nuestro sistema de análisis interno, que compara imágenes utilizadas en incidentes de suplantación de identidad y malware. En esta campaña, los atacantes utilizaron un código QR para atraer al usuario a un sitio web malicioso.

El ataque comienza cuando se envía un documento de Word a un destinatario por correo electrónico. El documento asegura que el destinatario tiene derecho a una subvención del gobierno y cumple con los elementos clásicos de un engaño de suplantación de identidad eficaz: la confianza en la autoridad, la urgencia y un incentivo financiero para actuar.

Para recibir la subvención, se le pide al destinatario que escanee el código QR con WeChat, una famosa aplicación de mensajería instantánea, redes sociales y pagos móviles y, posteriormente, que siga las instrucciones en el sitio web.

El uso de códigos QR es una forma eficaz de forzar a la víctima a cambiar de un ordenador a un dispositivo móvil, que posiblemente esté protegido por mecanismos de protección y detección de suplantación de identidad más débiles. Los códigos QR también benefician a los atacantes porque es menos probable que las puertas de enlace de correo electrónico inspeccionen las direcciones web de destino a las que llevan los códigos, lo que significa que los mensajes de correo electrónico de suplantación de identidad tienen una mayor probabilidad de llegar a las bandejas de entrada de los usuarios en comparación con los hipervínculos normales.

Imagen 3: Documento trampa que solicita al usuario que actualice los campos del documento.

Desde finales de octubre, hemos observado estas campañas de suplantación de identidad casi a diario a un ritmo acelerado. Los atacantes modifican los engaños en los documentos y los dominios todos los días. Si bien no podemos declarar con certeza el tamaño de estas campañas, la elección por parte del atacante de un marco de suplantación de identidad dinámico indica que se pretendía la escalabilidad. No es de extrañar que estas campañas se distribuyan en grandes volúmenes. La estructura del kit de suplantación de identidad permite que el contenido y el tema de una campaña sean fácilmente intercambiables.

También hemos visto códigos QR utilizados en campañas de suplantación de identidad en inglés que se hacen pasar por empresas de entrega de paquetes solicitando pagos. Por consiguiente, tanto los individuos como las organizaciones deben estar atentos a dichas campañas.

Imagen 4: Sitio web de suplantación de identidad que solicita los datos de la tarjeta de crédito de la víctima.

Aumento de publicidad maliciosa de software

Cuando configuramos un ordenador nuevo, muchos de nosotros tenemos paquetes de software que nos gusta instalar. Pero si no tienes cuidado, podrías terminar instalando malware que se haga pasar por tu software favorito. Desde noviembre, hemos observado un aumento significativo de las campañas que utilizan publicidad maliciosa para distribuir malware a víctimas desprevenidas.[5]

La publicidad maliciosa se lleva a cabo cuando los responsables de las amenazas compran anuncios en los resultados de los buscadores y redirigen a los usuarios a sitios web que alojan malware. La compra de anuncios permite a los atacantes conseguir una clasificación más alta en los buscadores para sus sitios web maliciosos que contienen consultas relacionadas con el software. En algunos ejemplos que analizamos, los atacantes imitaron conocidos proyectos de código abierto, como Audacity, Blender y GIMP. Un usuario que busque uno de estos paquetes de software, puede recibir un anuncio que lo lleve a un sitio web malicioso.

La imagen 5 muestra un ejemplo de un enlace patrocinado falso. Si observas detenidamente, verás que el nombre de dominio del anuncio difiere del sitio web genuino del proyecto de software. Pero la diferencia entre los dominios es sutil y resulta fácil no darse cuenta. Al hacer clic en el anuncio, se accede a un sitio web falso que copia el diseño del sitio web legítimo de Audacity.

Número de proyectos de software imitados en campañas de publicidad maliciosa desde noviembre de 2022

24

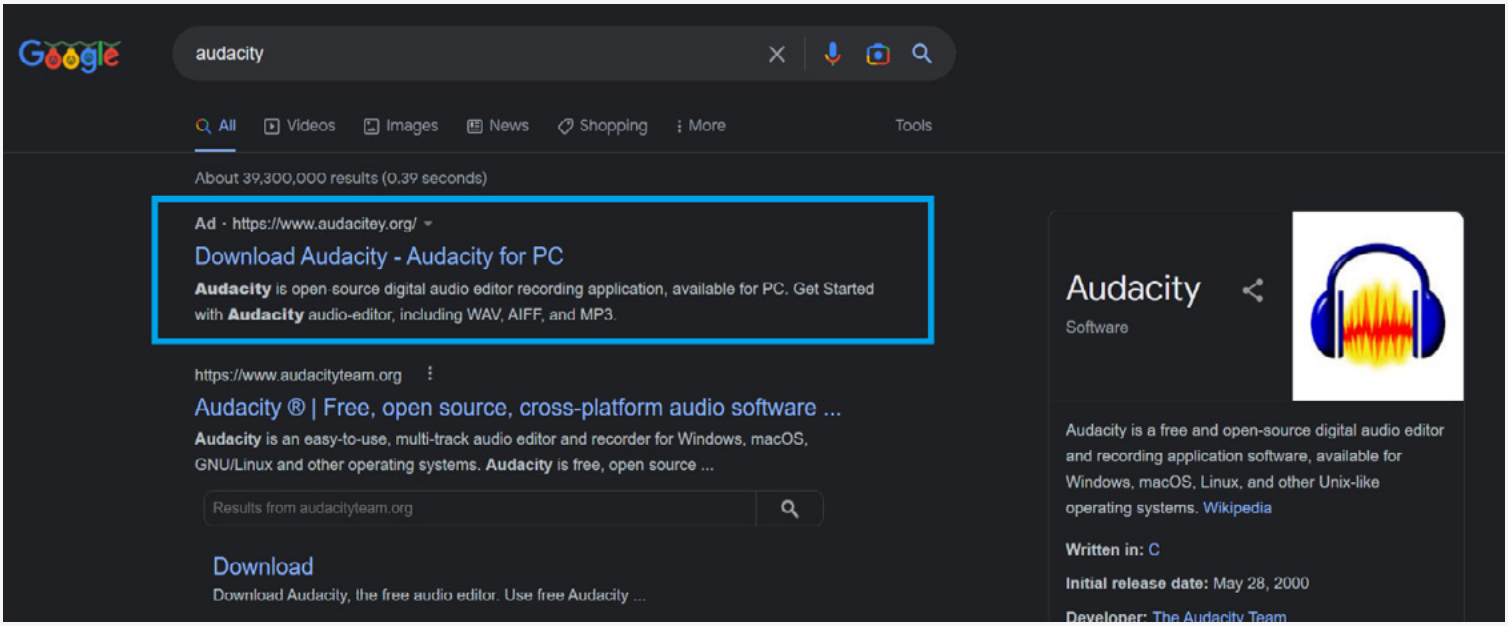


Imagen 5: Anuncio de buscador que lleva a un sitio web malicioso que distribuye malware.

El sitio web falso es casi idéntico al real, lo que dificulta al usuario detectar que es falso (Imagen 6). Cuando el usuario hace clic en el botón de descarga, se facilita un archivo .exe que se hace pasar por un instalador, en este caso, «audacity-win-x64.exe». Este ejemplo hace referencia a Vidar Stealer, un ladrón de información.[6] Vidar Stealer no es la única familia que se distribuye a través de publicidad maliciosa. También hemos visto cómo se utiliza este tema falso de publicidad maliciosa de software para propagar al menos ocho familias de malware, incluidos algunos ladrones de información, como Rhadamanthys Stealer y BatLoader, entre otros.[7,8] Sin embargo, desde mediados de noviembre, las campañas más importantes que hemos visto que utilizan este enfoque de distribución son las que propagan el troyano IcedID.

Al igual que con Vidar Stealer, los atacantes imitan los sitios web legítimos de los proyectos de software para propagar malware. Los atacantes tienden a no cambiar las propiedades de los dominios en las campañas, lo que permite identificar los sitios web falsos en función del registrador de dominios, servidores de nombres y nombres de dominio.

Durante dos meses, nuestra búsqueda identificó 92 dominios que imitan 24 proyectos de software diferentes que se han utilizado o podrían todavía utilizarse para distribuir malware a través de publicidad maliciosa (Imágenes 7 y 8). Creemos que esta tendencia continuará creciendo a medida que los responsables de las amenazas diversifiquen sus métodos de distribución de malware.

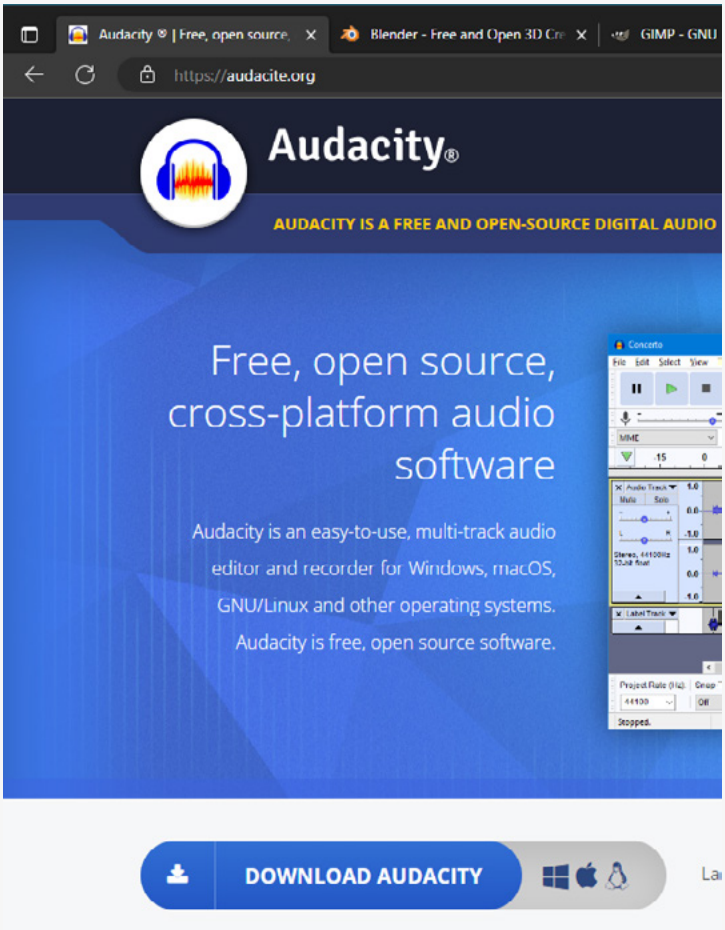


Imagen 6: Sitio web falso de Audacity que distribuye Vidar Stealer.

Domain	Registrar	Created	Name Server
www-irs-forms.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 29, 2022, 4:12 p.m.	a.dnspod.com c.dnspod.com
vvv-discord.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 29, 2022, 10:49 a.m.	a.dnspod.com c.dnspod.com
mlcrosofteams.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 29, 2022, 10:49 a.m.	a.dnspod.com c.dnspod.com
wvvw-citrix.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 28, 2022, 9:42 a.m.	a.dnspod.com c.dnspod.com
www-adobe.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 28, 2022, 9:42 a.m.	a.dnspod.com c.dnspod.com
vwvv-discord.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 28, 2022, 9:42 a.m.	a.dnspod.com c.dnspod.com
www-microsofteams.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 27, 2022, 1:44 p.m.	a.dnspod.com c.dnspod.com
vwv-discord.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 27, 2022, 1:44 p.m.	a.dnspod.com c.dnspod.com
www-onenote.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 26, 2022, 10:27 a.m.	a.dnspod.com c.dnspod.com
www-microsoftteams.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 26, 2022, 10:11 a.m.	a.dnspod.com c.dnspod.com

Imagen 7: Dominios con errores tipográficos registrados en diciembre de 2022.

Campaign date	Imitated software		Malware family
December 2021	Discord		Redline Stealer
February 2022	Windows 11 OS upgrade		Redline Stealer
November 2022 – ongoing	Audacity	Thunderbird	IcedID
	Blender	Fortinet	Vidar Stealer
	GIMP	Webex	Rhadamanthys Stealer
	Notepad++	Sandboxie Plus	BatLoader
	Microsoft Teams	Docker	Redline Stealer
	Citrix	Basecamp	Aurora Stealer
	Adobe	VMWare	Gozi
	OneNote	OBS	Raccoon Stealer
	LibreOffice	WhatsApp	
	Slack	Tor Browser	
	TeamViewer	Crypto Browser	
	Any Desk	Brave Browser	

Imagen 8: Tabla que resume las campañas de publicidad maliciosa de software falso.

Los distribuidores de Emotet trabajan en torno a una estricta política de macros de Office para infectar los ordenadores

No se realizaron muchas campañas de Emotet en el cuarto trimestre.[9] Sin embargo, del 2 al 11 de noviembre, el malware volvió con nuevas campañas de correo no deseado después de una pausa de varios meses. El malware se distribuía como de costumbre a través de hojas de cálculo de Excel maliciosas habilitadas con macros y adjuntas a mensajes de correo electrónico. Sin embargo, detectamos un cambio en el diseño de los documentos.

Después de años de sufrir abusos de atacantes, en febrero de 2022 Microsoft deshabilitó de forma predeterminada Visual Basic para macros de aplicaciones en muchos formatos de archivo de Microsoft Office descargados de la web.[10] Este cambio ha contribuido a la tendencia actual de diversificación de tipos de archivos de ataque. Curiosamente, en lugar de alejarse de las macros, los distribuidores de Emotet intentaron esquivar la política.

Imagen 9: Imagen de ingeniería social utilizada en la campaña Emotet en noviembre de 2022.

Cuando el destinatario abre la hoja de cálculo, se le muestra una imagen de ingeniería social que se hace pasar por un banner de Office. Las instrucciones indican al usuario que para ver el contenido de la hoja de cálculo, debe copiar el archivo en una de las carpetas indicadas en la imagen y, posteriormente, volver a abrirlo. Al igual que el contrabando de HTML y la distribución de malware en formato PDF, este método requiere un alto nivel de interacción del usuario para desencadenar la infección. Antes del cambio de la política de Office, los usuarios podían activar involuntariamente la ejecución del malware con dos clics.

Si el usuario sigue las instrucciones, se ejecuta la macro maliciosa. El código guarda cuatro archivos DLL con nombres distintos en el directorio del usuario y, a continuación, los ejecuta con regsvr32.exe (T1218.010), lo que deriva en la ejecución de la carga útil Emotet.[11] Debido a la complejidad de las instrucciones de usuario, es posible que esta campaña fuera una prueba para comparar la tasa de infección de esta técnica de distribución con otros métodos.

Aumento del malware de imágenes de disco durante el tercer trimestre

31 %

Vectores principales de ataque

77 %

Correo electrónico

14 %

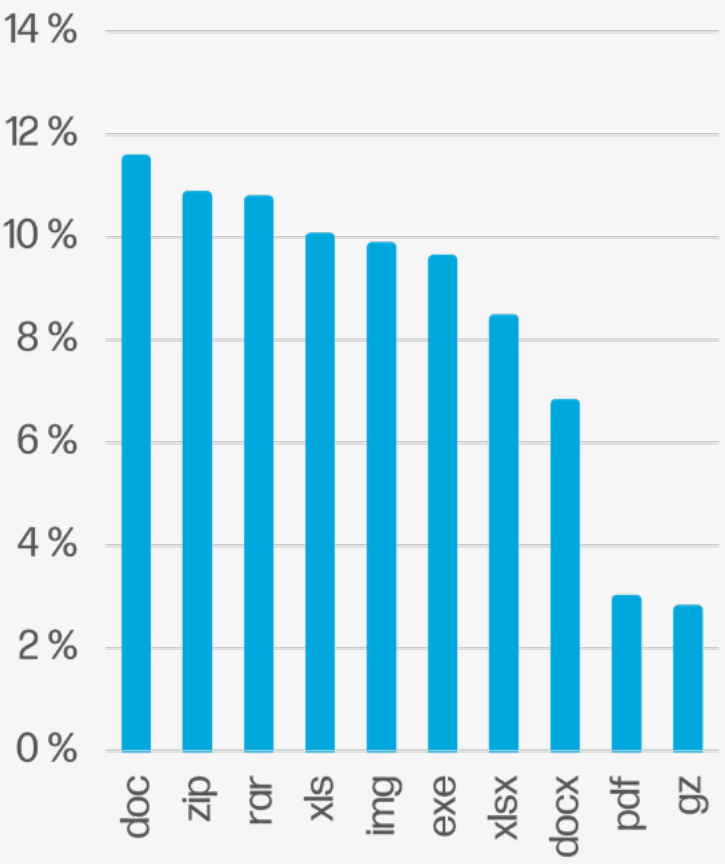
Descargas desde el navegador

9 %

Otros

Tendencias destacadas

Principales extensiones de archivos de malware



Por tercer trimestre consecutivo, los archivos comprimidos siguen siendo el tipo de archivo de distribución de malware más conocido.

En el cuarto trimestre, el 42 % del malware se distribuyó en formatos de archivo comprimido, como ZIP y RAR. Los archivos comprimidos continuaron siendo el grupo de formatos de archivo de malware más conocido durante el tercer trimestre, superando los formatos de Office (38 %). La popularidad de los archivos comprimidos ha aumentado un 20 % desde el primer trimestre de 2022, ya que los responsables de las amenazas prefieren cada vez más las secuencias de comandos para ejecutar sus cargas útiles.

Cuatro de las 10 principales extensiones de archivos de malware eran formatos de archivos comprimidos (ZIP, RAR, IMG y GZ). Cabe destacar que se produjo un aumento del 31 % en el malware de imagen de disco (IMG) en comparación con el tercer trimestre, y el formato subió dos puestos para convertirse en el quinto tipo de archivo de malware más conocido en el cuarto trimestre. Los atacantes están abusando de la función de montaje automático de Windows que permite a las víctimas montar y acceder fácilmente al malware almacenado dentro de los archivos IMG haciendo doble clic en ellos.

RAR, otro tipo de archivo comprimido, también subió en la clasificación al tercer puesto, dado que un 11 % del malware utiliza este formato de archivo. En general, los 10 formatos de archivo principales representaron el 83 % del malware aislado que HP Wolf Security ha detectado.

A los responsables de las amenazas les atraen los archivos comprimidos porque se cifran fácilmente, lo que dificulta la detección de malware por parte de proxies web, entornos aislados y escáneres de correo electrónico. Muchas organizaciones utilizan archivos comprimidos cifrados por razones legítimas, lo que dificulta el rechazo mediante una directiva de los archivos adjuntos de correo electrónico cifrados.

Aumento de amenazas de HTML durante el tercer trimestre

44 %

Las amenazas de HTML crecen en el cuarto trimestre

Las amenazas de HTML, incluido el contrabando de HTML, aumentaron un 44 % en el cuarto trimestre y se convirtieron en el decimoquinto formato de malware más conocido (dos puestos más que el decimoséptimo puesto del tercer trimestre), lo que indica la creciente popularidad de esta técnica entre los responsables de las amenazas para propagar malware.

Mantente al día

El informe de amenazas de HP Wolf Security es posible gracias a que la mayoría de nuestros clientes optan por compartir telemetría de amenazas con HP. Nuestros expertos en seguridad analizan tendencias de amenazas y campañas de malware significativas, anotan alertas con información y las comparten con los clientes.

Recomendamos que los clientes sigan los siguientes pasos para poder sacarle el máximo partido a sus implementaciones de HP Wolf Security:[a]

▪ Habilita los servicios de inteligencia de amenazas y el reenvío de amenazas en tu controlador de HP Wolf Security para beneficiarte de las anotaciones, la clasificación y el análisis de MITRE ATT&CK de nuestros expertos.[b] Para obtener más información, lee nuestros artículos de la base de conocimientos.[12, 13]

▪ Mantén actualizado tu controlador de seguridad de HP Wolf para recibir nuevos paneles y plantillas de informes. Consulta las notas de la versión y las descargas de software más recientes en el portal del cliente.[14]

▪ Actualiza tu software de dispositivos de HP Wolf Security para mantenerte al día con las reglas de anotación de amenazas que nuestro equipo de investigación añade.

El equipo de investigación de amenazas de HP publica periódicamente indicadores de compromiso (IOC) y herramientas para que los equipos de seguridad puedan defenderse de las amenazas. Puedes acceder a estos recursos en el repositorio GitHub de HP Threat Research.[15] Para conocer las últimas investigaciones de amenazas, visita el blog de HP Wolf Security.[16]

Acerca del informe de amenazas de HP Wolf Security

Las empresas corren mayor riesgo cuando los usuarios abren archivos adjuntos de correo electrónico, hacen clic en hipervínculos de mensajes de correo electrónico y descargan archivos de la web. HP Wolf Security protege a la empresa aislando la actividad de riesgo en las micromáquinas virtuales, lo que garantiza que el malware no infecte el servidor central ni se propague a la red corporativa. HP Wolf Security utiliza la introspección para recopilar datos forenses valiosos y ayudar a nuestros clientes a comprender las amenazas a las que se enfrentan sus redes con el fin de reforzar su infraestructura. El informe de amenazas de HP Wolf Security destaca campañas de malware notables que nuestro equipo de investigación de amenazas ha analizado para que nuestros clientes estén al tanto de las amenazas emergentes y puedan adoptar medidas para proteger sus entornos.

Acerca de HP Wolf Security

HP Wolf Security es un nuevo tipo[c] de seguridad de dispositivos. La cartera de servicios de seguridad de HP basados en hardware y centrados en dispositivos se ha diseñado para que las organizaciones puedan proteger a los ordenadores, impresoras y personas de los depredadores cibernéticos que les rodean. HP Wolf Security brinda una protección y resiliencia completas para los dispositivos que comienza en el hardware, y se amplía a través del software y los servicios.

Referencias

[1] https://hp.com/wolf.

[2] https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot.

[3] https://malpedia.caad.fkie.fraunhofer.de/details/win.icedid.

[4] https://threatresearch.ext.hp.com/chinese-phishing-campaign-abuses-qr-codes-to-steal-credit-card-details/.

[5] https://threatresearch.ext.hp.com/adverts-mimicking-popular-software-leads-to-malware/.

[6] https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar.

[7] https://malpedia.caad.fkie.fraunhofer.de/details/win.rhadamanthys.

[8] https://malpedia.caad.fkie.fraunhofer.de/details/win.bat_loader.

[9] https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet.

[10] https://attack.mitre.org/techniques/T1218/010/.

[11] https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked.

[12] https://enterprisesecurity.hp.com/s/article/Threat-Forwarding.

[13] https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence.

[14] https://enterprisesecurity.hp.com/s/.

[15] https://github.com/hpthreatresearch/.

[16] https://threatresearch.ext.hp.com/blog.

OBTÉN MÁS INFORMACIÓN EN HP.COM

HP WOLF SECURITY

a. HP Wolf Enterprise Security es un servicio opcional y puede incluir ofertas, como HP Sure Click Enterprise y HP Sure Access Enterprise. HP Sure Click Enterprise requiere Windows 8 o 10 y es compatible con Microsoft Internet Explorer, Google Chrome, Chromium o Firefox. Los archivos adjuntos admitidos incluyen archivos de Microsoft Office (Word, Excel y PowerPoint) y PDF, siempre que se haya instalado Microsoft Office o Adobe Acrobat. HP Sure Access Enterprise requiere Windows 10 Pro o Enterprise. Los servicios de HP se rigen por los términos y condiciones del servicio de HP aplicables proporcionados o indicados al cliente en el momento de la compra. El cliente puede tener derechos adicionales de acuerdo con las leyes locales aplicables y estos derechos no están afectados de ninguna forma por los términos y condiciones del servicio de HP o la garantía limitada de HP proporcionada con su producto HP. Para conocer todos los requisitos del sistema, visita www.hpdaas.com/requirements.

b. El controlador de HP Wolf Security requiere HP Sure Click Enterprise o HP Sure Access Enterprise. El controlador de HP Wolf Security es una plataforma de gestión y análisis que proporciona datos críticos acerca de dispositivos y aplicaciones, y no se vende como un servicio independiente. El controlador de HP Wolf Security sigue las estrictas normas de privacidad del RGPD y cuenta con las certificaciones ISO27001, ISO27017 y SOC2 Tipo 2 para la seguridad de la información. Se requiere acceso a Internet con conexión a HP Cloud. Para conocer todos los requisitos del sistema, visita http://www.hpdaas.com/requirements.

c. HP Security es ahora HP Wolf Security. Las funciones de seguridad varían en función de la plataforma. Consulta la ficha técnica del producto para obtener más información.

Los servicios de HP se rigen por los términos y condiciones del servicio de HP aplicables proporcionados o indicados al cliente en el momento de la compra. El cliente puede tener derechos adicionales de acuerdo con las leyes locales aplicables y estos derechos no están afectados de ninguna forma por los términos y condiciones del servicio de HP o la garantía limitada de HP proporcionada con su producto HP.