SECURESOFT CORPORATION
e-Secure Consulting Group

Reporte Quincenal de Ciberinteligencia Securesoft

Fecha:

16 noviembre de 2021

El presente documento contiene información para la comunidad de ciberseguridad.

Equipo de Ciberinteligencia

CIB-FOR-2021-022

Índice

1. Objetivo

El presente documento de inteligencia tiene como objetivo informar sobre las principales vulnerabilidades y amenazas que se han detectado en el ciberespacio.

2. Alcance

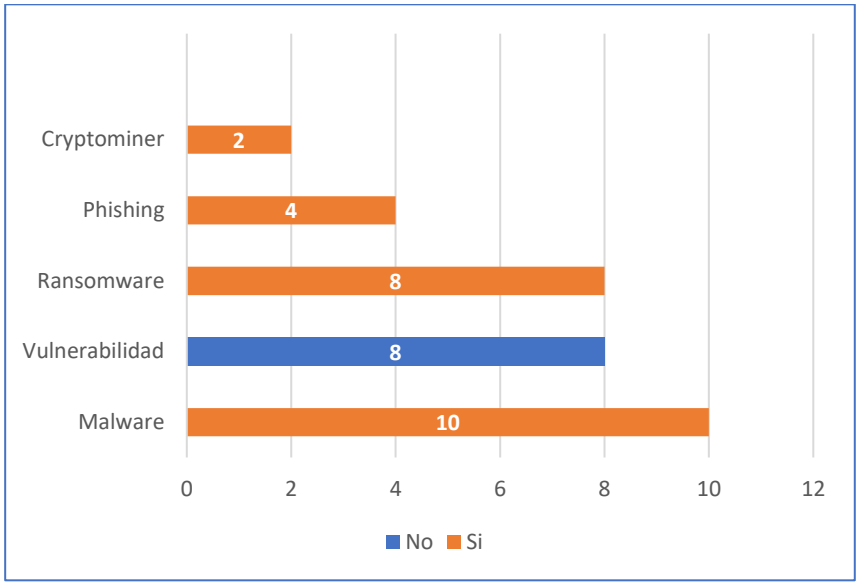
Este documento muestra el resumen, la fecha de publicación, CVE asociado y servicios afectados de vulnerabilidades y amenazas que se han hecho públicas en el transcurso del 1 de noviembre hasta el 16 de noviembre del 2021.

3. Resumen

En el presente informe se exponen 32 análisis de vulnerabilidad y amenazas, de las cuales 29 tienen severidad alta y 3 severidad crítica.

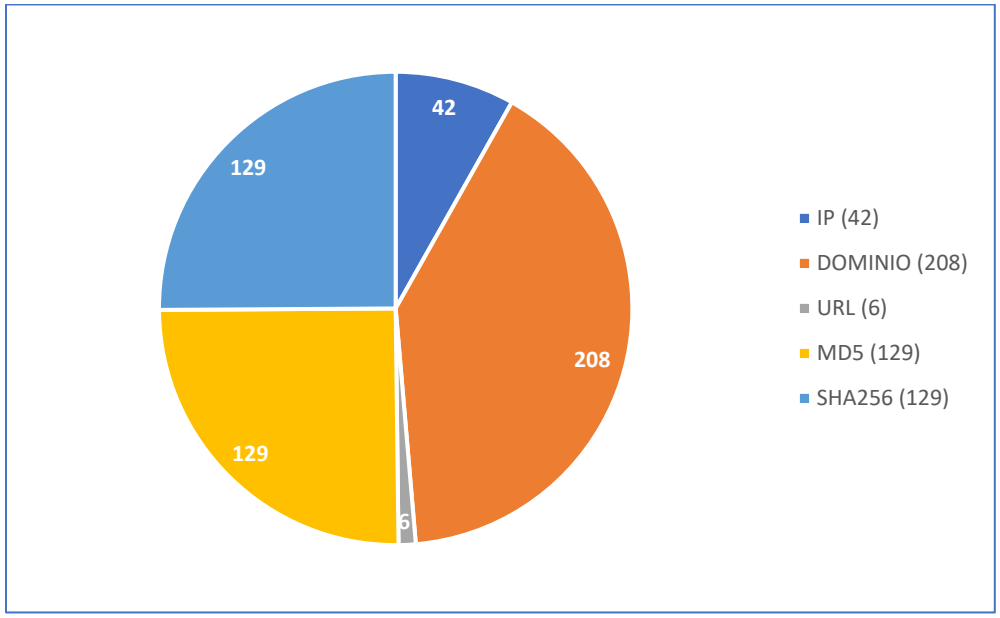
Amenazas analizadas por tipología

En las investigaciones elaboradas para el presente informe se trataron cryptominer, phishing, ransomware, vulnerabilidad y malware. Los que se detallan a continuación, separándolas de acuerdo con si contaban con indicadores de compromiso (IoC) o no.



Indicadores de Compromiso (IoC)

En las investigaciones elaboradas para el presente informe, se han distribuido 514 IoC's entre direcciones IP, Dominios, URL, MD5 y SHA256.



Tendencias en nuevas vulnerabilidades

- Recientemente se detectó una vulnerabilidad que puede provocar que los sistemas no funcionen correctamente y una campaña de phishing que involucra mensajes aparentemente enviados desde una dirección de correo electrónico de Kaspersky. Para más información leer el Boletín 2021-556.

- Cisco Systems ha publicado actualizaciones de seguridad para abordar vulnerabilidades en varios productos de Cisco que un atacante podría aprovechar para iniciar sesión como usuario raíz y tomar el control de los sistemas vulnerables. Para más información leer el Boletín 2021-558.

- Microsoft publicó el paquete de actualizaciones de seguridad correspondiente a noviembre de 2021. En esta edición la compañía corrige un total de 55 vulnerabilidades, entre estas vulnerabilidades se encuentra seis zero-day. Para más información leer el Boletín 2021-565.

- Recientemente se descubrió una vulnerabilidad afecta a los firewall PAN que utilizan GlobalProtect Portal VPN y permite la ejecución remota de código no autenticado en instalaciones vulnerables del producto. Para más información leer el Boletín 2021-572.

Tendencias en actividades maliciosas

- Recientemente se ha observado una campaña activa de phishing que se encuentra distribuyendo un backdoor bancario en América Latina, el cual tiene procesos para evitar la detección y lograr persistencia para moverse lateralmente, para más información leer Boletín 2021-544.

- Recientemente se detectó un incremento de actividades por parte del ransomware HelloKitty donde han agregado en sus métodos la capacidad de realizar ataques distribuidos de denegación de servicio (DDoS) a su arsenal de tácticas de extorsión, para más información leer Boletín 2021-551.

- Una nueva campaña de phishing que pretende ser listas de suministros infecta a los usuarios con el ransomware MirCop que encripta un sistema objetivo en menos de quince minutos, para más información leer Boletín 2021-562.

- Los ciberdelincuentes están invirtiendo en Google Ads para comprometer cuentas con billeteras falsas que roban credenciales y agotan los saldos. Se estima que han robado más de $ 500.000 dólares, para más información leer Boletín 2021-564.

4. Detalles

Vulnerabilidades

Boletín	2021-542
Asunto	ACTUALIZACIONES DE SEGURIDAD EN GOOGLE CHROME
Emisión	2/11/2021
CVE	Según lista boletín
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Según lista boletín

Descripción

Registradas como CVE-2021-38000 y CVE-2021-38003, las debilidades se relacionan con una validación insuficiente de entradas no confiables en una función llamada Intents, así como con un caso de implementación inapropiada en V8 JavaScript y motor WebAssembly. Google es consciente de que los exploits para CVE-2021-38000 y CVE-2021-38003.

Además, se aborda como parte de esta actualización de canal estable una vulnerabilidad de uso después de la liberación en el componente de transporte web (CVE-2021-38002).

Con estos parches, Google ha resuelto un total de 16 días cero en el navegador web desde principios de año:

• CVE-2021-21148 - Heap buffer overflow in V8
• CVE-2021-21166 - Object recycle issue in audio
• CVE-2021-21193 - Use-after-free in Blink
• CVE-2021-21206 - Use-after-free in Blink
• CVE-2021-21220 - Insufficient validation of untrusted input in V8 for x86_64
• CVE-2021-21224 - Type confusion in V8
• CVE-2021-30551 - Type confusion in V8
• CVE-2021-30554 - Use-after-free in WebGL
• CVE-2021-30563 - Type confusion in V8
• CVE-2021-30632 - Out of bounds write in V8
• CVE-2021-30633 - Use-after-free in Indexed DB API
• CVE-2021-37973 - Use-after-free in Portals
• CVE-2021-37975 - Use-after-free in V8
• CVE-2021-37976 - Information leak in core.

Actualización o Mitigación

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

Boletín	2021-554
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE MOZILLA FIREFOX
Emisión	5/11/2021
CVE	Según tabla boletín
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Versiones anteriores a Firefox 94 y Firefox ESR 91.3

Descripción

El CVE-2021-38503 soluciona un problema en el que las reglas de la zona de pruebas de iframe no se aplicaban correctamente a las hojas de estilo XSLT, lo que permite que un iframe omita restricciones como ejecutar scripts o navegar por el marco de nivel superior. Los ciberdelincuentes podrían manejar hojas de estilo XSLT manipuladas y ser capaces de ejecutar scripts o irrumpir en el marco principal.

Actualización o Mitigación

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

Boletín	2021-556
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE KASPERSKY
Emisión	6/11/2021
CVE	CVE-2021-35053
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

- Kaspersky Anti-Virus antes de 21.3.10.391
- Kaspersky Internet Security anterior a 21.3.10.391
- Kaspersky Total Security antes de 21.3.10.391
- Kaspersky Small Office Security antes de 21.3.10.391
- Kaspersky Security Cloud antes de 21.3.10.391
- Kaspersky Endpoint Security entre las versiones 11.1 a 11.6

Descripción

La vulnerabilidad está relacionada con Firefox y puede ser una posible denegación de servicio del sistema en caso de cambios arbitrarios en los parámetros del navegador Firefox. Un atacante podría cambiar el archivo de parámetros del navegador Firefox específico de cierta manera y luego reiniciar el sistema para que no se pueda iniciar, afecta las versiones de Windows de los productos Kaspersky Anti-Virus, Internet Security, Total Security, Small Office Security, Security Cloud y Endpoint Security. El ataque se puede hacer desde la red local. La explotación requiere una autentificación. No se conoce los detalles técnicos ni hay ningún exploit disponible. La compañía ha lanzado parches para cada uno de los productos afectados.

Por otro lado, se ha detectado un aumento de correos electrónicos de spearphishing diseñados para robar las credenciales de Office 365. Estos intentos de phishing se basan en un kit de phishing que denominamos "lamtheboss" y que se utiliza junto con otro kit de phishing conocido como "MIRCBOOT". La actividad puede estar asociada con múltiples ciberdelincuentes. Los correos electrónicos de phishing generalmente llegan en forma de "notificaciones por fax" y atraen a los usuarios a sitios web falsos que recopilan credenciales para los servicios en línea de Microsoft, para mayor información revisar el Boletín SecureSoft-Nro. 2021-463. Estos correos electrónicos tienen varias direcciones de remitente incluidas, como noreply@sm[.]kaspersky[.]com.

Durante la investigación de esta actividad de phishing, se determinó que algunos correos electrónicos se enviaron utilizando el Simple Email Service (SES) de Amazon y el token SES legítimo. Este token de acceso se emitió a un contratista externo durante la prueba del sitio web 2050.earth. El sitio también está alojado en la infraestructura de Amazon. Tras el descubrimiento de estos ataques de phishing, el token de SES fue revocado de inmediato. No se encontró ningún compromiso del servidor, acceso no autorizado a la base de datos o cualquier otra actividad maliciosa en 2050.earth y servicios asociados.

Actualización o Mitigación

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

Boletín	2021-557
Asunto	ACTUALIZACIÓN DE SEGURIDAD DEL KERNEL DE LINUX
Emisión	6/11/2021
CVE	CVE-2021-43267
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Kernel de Linux desde la versión 5.10-rc1 hasta 5.14.16

Descripción

La vulnerabilidad rastreada como CVE-2021-43267 se puede aprovechar tanto de forma local como remota. Si bien la explotación local es más fácil debido a un mayor control sobre los objetos asignados en el montón del Kernel, la explotación remota se puede lograr gracias a las estructuras que admite TIPC.

TIPC es un protocolo de capa de transporte diseñado para que los nodos que se ejecutan en entornos de clúster dinámicos y se comuniquen de manera confiable entre sí de una manera más eficiente y tolerante a fallas similar a otros protocolos como TCP. La vulnerabilidad identificada tiene que ver con una validación insuficiente de los tamaños proporcionados por el usuario para un nuevo tipo de mensaje llamado "MSG_CRYPTO " que se introdujo en septiembre de 2020 y permite que los nodos pares del clúster envíen claves criptográficas.

Si bien el protocolo tiene verificaciones para validar dichos mensajes después del descifrado logrando garantizar que el tamaño del payload real de un paquete no exceda el tamaño máximo del mensaje de usuario y que este último sea mayor que el tamaño del encabezado del mensaje, no se encontraron restricciones en la longitud de la clave (también conocido como 'keylen'), lo que da como resultado un escenario en el que "un atacante puede crear un paquete con un tamaño de cuerpo pequeño para asignar memoria de pila y luego usar un tamaño arbitrario en el atributo 'keylen' para escribir fuera de los límites de esta ubicación".

No hay evidencia de que se haya explotado la falla hasta la fecha, y luego de la divulgación responsable del 19 de octubre el problema se ha abordado en la versión 5.15 del Kernel de Linux.

Actualización o Mitigación

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

Boletín	2021-558
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE CISCO
Emisión	6/11/2021
CVE	CVE-2021-34739, CVE-2021-34741, CVE-2021-34795, CVE-2021-40112, CVE-2021-40113 y CVE-2021-40119
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

- Cisco Policy Suite versión 21.2.0 y posteriores
- Cisco Small Business Series y Cisco AsyncOS
- Catalyst PON Switch CGP-ONT-1P
- Catalyst PON Switch CGP-ONT-4P
- Catalyst PON Switch CGP-ONT-4PV
- Catalyst PON Switch CGP-ONT-4PVC
- Catalyst PON Switch CGP-ONT-4TVCW

Descripción

Rastreada como CVE-2021-40119, la vulnerabilidad ha sido calificada con una severidad de 9.8 sobre un máximo de 10 en el sistema de puntuación CVSS y se debe a una debilidad en el mecanismo de autenticación SSH de Cisco Policy Suite, un exploit exitoso podría permitir que un atacante inicie sesión en un sistema afectado como usuario root.

También se abordó tres vulnerabilidades críticas a las que se les han asignado los identificadores CVE-2021-34795 (puntuación CVSS: 10,0), CVE-2021-40113 (puntuación CVSS: 10,0) y CVE-2021-40112 (Puntuación CVSS: 8,6) que afectan la interfaz de administración basada en web de la Terminal de red óptica (ONT) de switches de la serie de redes ópticas pasivas (PON) Cisco Catalyst que podrían permitir que un atacante remoto no autenticado inicie sesión utilizando una cuenta de depuración inadvertida existente en el dispositivo y tomar el control, realizar una inyección de comando y modificar la configuración del dispositivo.

Por último, se ha corregido dos fallas más de alta gravedad en los switches Cisco Small Business Series y Cisco AsyncOS. Rastreados como CVE-2021-34739 (puntuación CVSS: 8.1) y CVE-2021-34741 (puntuación CVSS: 7.5), podrían permitir que adversarios remotos no autenticados obtengan acceso no autorizado a la interfaz de administración basada en web de los switches y lleven a cabo una denegación de servicio (DoS).

Actualización o Mitigación

- Mantener el conocimiento situacional de las últimas amenazas y zonas vulnerables de la organización.

Boletín	2021-565
Asunto	MICROSOFT CORRIGE 55 VULNERABILIDADES EN EL PARCHE DE SEGURIDAD DE NOVIEMBRE
Emisión	12/11/2021
CVE	Según tabla boletín
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Según lista boletín

Descripción

En octubre, Microsoft ha publicado 55 correcciones de seguridad, incluido seis Zero-Day en los cuales se observaron que 2 vulnerabilidades Zero-Day se encuentran siendo explotados activamente en Microsoft Exchange y Microsoft Excel.
Las vulnerabilidades explotadas activamente solucionadas este mes están siendo rastreadas como CVE-2021-42292 y CVE-2021-42321. La vulnerabilidad de Microsoft Exchange (CVE-2021-42321) es un error de ejecución de código remoto autenticado. En conjunto la vulnerabilidad de Microsoft Excel (CVE-2021-42292) se ha utilizado activamente en ataques maliciosos según Microsoft.

Actualización o Mitigación

• Implementar la actualización que corresponda a cada producto según la información proporcionada por Microsoft en la sección de "Security Updates" accediendo por medio del hipervínculo de la columna de "Actualización" de la "Tabla 1" del presente boletín de acuerdo a cada vulnerabilidad mencionada.

Boletín	2021-566
Asunto	CITRIX PUBLICA ACTUALIZACION DE SEGURIDAD
Emisión	12/11/2021
CVE	CVE-2021-22955 y CVE-2021-22956
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

- Citrix ADC y Citrix Gateway 13.0 antes de 13.0-83.27
- Citrix ADC y Citrix Gateway 12.1 antes de 12.1-63.22
- Citrix ADC y NetScaler Gateway 11.1 antes de 11.1-65.23
- Citrix ADC 12.1-FIPS antes de 12.1-55.257
- Modelos 4000-WO, 4100-WO, 5000-WO y 5100-WO
- Versión 11.4 antes de 11.4.2
- Versión 10.2 antes de 10.2.9c

Descripción

El primer error rastreado como CVE-2021-22955 permitiría la denegación de servicio (DoS) no autenticada debido al consumo de recursos no controlados. Esta falla afectaría a dos productos Citrix (anteriormente NetScaler ADC y Gateway) se utilizan para la gestión del tráfico con reconocimiento de aplicaciones y el acceso remoto seguro. Para este caso, el ataque solo puede iniciarse dentro de la red local y la explotación no requiere ningún tipo de autenticación. La manipulación con una entrada desconocida conduce a una vulnerabilidad de denegación de servicio, lo cual tendría un impacto en la disponibilidad.

El segundo error, registrado como CVE-2021-22956, permite la interrupción temporal de la GUI de administración de un dispositivo. Afecta a los dos productos anteriores, así como al dispositivo Citrix SD-WAN WANOP Edition. Este último proporciona optimización para las implementaciones de Citrix SD-WAN, que permiten una conectividad segura y un acceso perfecto a las aplicaciones virtuales, en la nube y de software como servicio (SaaS) en las empresas y sucursales.

La interrupción de cualquiera de los dispositivos podría evitar el acceso remoto y de sucursales a los recursos corporativos y el bloqueo general de la nube y los activos y aplicaciones virtuales.

En el caso del primer error de Citrix ADC y Gateway, los dispositivos deben configurarse como un servidor virtual VPN o AAA para que sean vulnerables. En el caso del segundo error, los dispositivos deben tener acceso a NSIP o SNIP con acceso a la interfaz de administración.

Actualización o Mitigación

- Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-572
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE PALO ALTO NETWORKS
Emisión	14/11/2021
CVE	CVE-2021-3064
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• GlobalProtect Portal VPN versiones de PAN-OS 8.1 y anteriores a PAN-OS 8.1.17

Descripción

El problema afecta a múltiples versiones de PAN-OS 8.1 antes de la 8.1.17 y se ha encontrado numerosas instancias vulnerables expuestas en activos conectados a Internet, más de 10.000 activos.

Un equipo desarrolló un exploit que permite obtener una shell en el objetivo afectado, acceder a datos de configuración confidenciales, extraer credenciales y mucho más. Una vez que un atacante logra el control sobre el firewall, tendrá visibilidad de la red interna y podrá moverse lateralmente.

CVE-2021-3064 es un desbordamiento de búfer que se produce mientras se analiza la entrada proporcionada por el usuario en una ubicación de longitud fija en la pila. El código problemático no es accesible externamente sin utilizar una técnica de smuggling HTTP. La explotación de estos juntos produce la ejecución remota de código bajo los privilegios del componente afectado en el dispositivo de firewall.

El smuggling de solicitudes HTTP es una técnica para interferir con la forma en que un sitio web procesa secuencias de solicitudes HTTP que se reciben de los usuarios. Este tipo de vulnerabilidades son a menudo de naturaleza crítica, lo que permite a un atacante eludir los controles de seguridad, obtener acceso no autorizado a datos confidenciales y comprometer directamente a otros usuarios de la aplicación.

Para aprovechar esta vulnerabilidad, un atacante debe tener acceso de red al dispositivo en el puerto de servicio GlobalProtect (puerto predeterminado 443). Como el producto afectado es un portal VPN, a menudo se puede acceder a este puerto a través de Internet. En dispositivos con ASLR habilitado (que parece ser el caso en la mayoría de los dispositivos de hardware), la explotación es difícil pero posible.

En dispositivos virtualizados (firewalls de la serie VM), la explotación es significativamente más fácil debido a la falta de ASLR. El código de explotación disponible públicamente no existe en este momento, pero es probable que el código de explotación pública aparezca pronto.

En un esfuerzo por evitar permitir el uso indebido, los detalles técnicos relacionados con CVE-2021-3064 no se divulgarán públicamente durante un período de 30 días a partir de la fecha. En ese momento se dará a conocer más información.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Amenazas

Boletín	2021-543
Asunto	NUEVO RANSOMWARE SPOOK
Emisión	2/11/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows.

Descripción

El ransomware Spook inició sus actividades desde septiembre de 2021 y sigue el modelo de extorsión de múltiples frentes, en el cual las víctimas se ven afectadas por la amenaza de destrucción de datos, así como por la filtración de datos públicos.
Aparentemente Spook es una variante del ransomware Prometheus y cuenta con un cifrado AES, junto con una nota de amenaza de filtrar los datos de las víctimas al público. El malware tiene la capacidad de cifrar los dispositivos de destino sin necesidad de conexión a Internet. El cifrado de un disco completo puede ocurrir en solo unos minutos, momento en el cual la nota de rescate se muestra en el escritorio (RESTORE_FILES_INFO.HTA).
El malware también realiza una serie de cambios para garantizar que las notificaciones de rescate se muestren de manera destacada después del reinicio (a través del menú Inicio lnk, Reg). Luego el proceso WinLogon se modifica (a través del registro) para mostrar el texto de la nota de rescate al iniciar sesión en dispositivos comprometidos.
Además, Spook intentará terminar los procesos y detener los servicios de cualquier cosa que pueda inhibir el proceso de cifrado. Luego ejecutará un conjunto de procesos para la verificación y eliminación del proceso anti-ransomware Raccine que algunas organizaciones implementan en un esfuerzo por proteger los dispositivos. Tras la infección, se indica a las víctimas que accedan al portal de pago ubicado en la darkWeb para que se pueda negociar el rescate de sus archivos.

Actualización o Mitigación

• Bloquear los indicadores de compromisos (IOC) mostrados en el boletín, en los dispositivos de seguridad de su infraestructura.

Boletín	2021-544
Asunto	NUEVA CAMPAÑA DE PHISHING DISTRIBUYE BACKDOOR BANCARIO
Emisión	2/11/2021
CVE	No
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Aparentemente esta campaña se ha mantenido activa desde el 2020. Los ciberdelincuentes parecían no dejarse intimidar por la exposición de avisos de seguridad y han implementado nuevos indicadores de compromiso (IOC) con el fin de mantener activa su campaña que distribuye un backdoor bancario.

En una investigación adicional respecto a esta campaña se observó que se estaban haciendo intentos para descargar un archivo sospechoso llamado mpr.dll en dispositivos de la víctima. En conjunto se observó que se descargaron cinco archivos, cuatro de los cuales estaban firmados y parecían ser archivos DLL legítimos, pero el archivo llamado mpr.dll no estaba firmado y era sospechosamente grande para un solo archivo DLL de 588 MB. Los sectores a los que se dirigió esta actividad incluyeron tecnología de la información, servicios profesionales, manufactura, servicios financieros y gobierno.

Actualmente no se tiene información de cuál fue el vector de infección inicial en esta campaña, pero aparentemente fue una URL maliciosa propagada a través de campañas de phishing o publicidad maliciosa, que suele ser el primer paso en las campañas de troyanos bancarios de América Latina. Luego, las víctimas son redirigidas a una URL de Amazon Web Services (AWS), que parece que los ciberdelincuentes abusaron para usar como servidor de comando y control (C&C). Luego un archivo ZIP que contiene un archivo de Microsoft Software Installer (MSI) se descarga de la infraestructura de AWS. Si la víctima hace doble clic en el archivo MSI dentro del ZIP descargado, ejecutará msiexec.exe, que luego se conecta a un servidor C&C secundario para descargar otro archivo ZIP que contiene el payload (mpr.dll), junto con otro archivo ejecutable portátil legítimo (PE).

El archivo ZIP extraído contiene una aplicación legítima de Oracle renombrada: VBoxTray.exe. Esto se ejecuta para ejecutar el payload(mpr.dll) mediante el secuestro del orden de búsqueda de DLL. El secuestro del orden de búsqueda de DLL aprovecha la forma en que Windows maneja los DLL para permitir que un atacante cargue código malicioso en un proceso legítimo. El archivo mpr.dll también tiene un tamaño superior a 100 MB para evitar el envío a los servicios de seguridad, que tienden a no procesar archivos por encima de ese tamaño. Luego, se crea la persistencia para el proceso VBoxTray.exe, de modo que mpr.dll podrá utilizar la técnica de movimiento lateralmente a través del Registro de Windows o Windows Management Instrumentation (WMI) para infectar a toda una empresa.

Actualización o Mitigación

• Bloquear los indicadores de compromisos (IOC) compartidos en el boletín, en los dispositivos de seguridad de su infraestructura.

Boletín	2021-545
Asunto	NUEVO MALWARE ABSTRACTEMU
Emisión	2/11/2021
CVE	CVE-2019-2215, CVE-2020-0041, CVE-2020-0069
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Android

Descripción

El nuevo malware de Android puede rootear los dispositivos infectados para tomar el control total y modificar silenciosamente la configuración del sistema, así como evadir la detección mediante la abstracción de código y las comprobaciones anti-emulación. El malware, denominado AbstractEmu, se incluyó con 19 aplicaciones de utilidad distribuidas a través de Google Play y tiendas de aplicaciones de terceros (incluidas Amazon Appstore, Samsung Galaxy Store, Aptoide y APKPure).

Las aplicaciones que agrupaban el malware incluían administradores de contraseñas y herramientas como ahorradores de datos e instaladores de aplicaciones, todos ellos brindando la funcionalidad que prometieron para evitar levantar sospechas. Las aplicaciones maliciosas se eliminaron de Google Play Store. Sin embargo, es probable que las otras tiendas de aplicaciones sigan distribuyéndolas. AbstractEmu no tiene ninguna funcionalidad sofisticada de explotación remota de clics utilizados en amenazas avanzadas de estilo APT. Se activa simplemente cuando el usuario abre la aplicación. Como el malware se disfraza de aplicaciones funcionales, es probable que la mayoría de los usuarios interactúen con ellas poco después de la descarga. Una vez instalado, AbstractEmu comenzará a recopilar y enviar información del sistema a su servidor de comando y control mientras el malware espera más comandos. Para rootear los dispositivos Android que infecta, AbstractEmu tiene múltiples herramientas a su disposición en forma de exploits dirigidos a varias vulnerabilidades, incluida la vulnerabilidad registrada como CVE-2020-0041. El malware también utiliza un exploit para atacar a la vulnerabilidad CVE-2020-0069 encontrada en los chips MediaTek utilizados por docenas de fabricantes de teléfonos inteligentes que han vendido colectivamente millones de dispositivos. Los atacantes detrás de AbstractEmu también tienen suficientes habilidades y conocimientos técnicos para agregar soporte para más objetivos al código disponible públicamente para los exploits CVE-2019-2215 y CVE-2020-0041. Al utilizar el proceso de rooteo para obtener acceso privilegiado al sistema operativo Android, el ciberdelincuente puede otorgarse silenciosamente permisos o instalar malware adicional, pasos que normalmente requerirían la interacción del usuario. AbstractEmu esperará los comandos de su servidor comando y control que puede indicarle que recolecte y exfiltre archivos en función de qué tan nuevos son o coinciden con un patrón dado, rooteen dispositivos infectados o instalen nuevas aplicaciones. Las acciones adicionales que AbstractEmu puede realizar después de rootear un dispositivo infectado van desde monitorear notificaciones, realizar capturas de pantalla y grabar la pantalla hasta bloquear el dispositivo e incluso restablecer la contraseña.

Actualización o Mitigación

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

Boletín	2021-546
Asunto	NUEVA BOTNET PINK CON MÁS DE 1 MILLÓN DE BOTS
Emisión	2/11/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows y Linux

Descripción

Rastreado como Pink, la botnet es capaz de insertar anuncios arbitrarios legítimos y opera principalmente en China. Además, es la botnet más grande detectada desde 2015, con escaneos identificados de hasta 1,963,000 direcciones IP activas asociadas con esta infraestructura maliciosa en un día. Por otro lado, a principios de 2020 se informó que las direcciones IP de los nodos bot asociados a esta botnet superan los 5 millones. Las direcciones IP domésticas se asignan dinámicamente, por lo que el tamaño real de los dispositivos infectados detrás de estos datos no se puede calcular con precisión, aunque es seguro que se trata de millones de dispositivos.

A diferencia de otras botnets que vemos comúnmente, Pink actualizará el firmware original del router después de infectarlo para mantener controles absolutos. En el firmware reescrito, se incluyen el descargador de PinkBot y el bootloader compatible.

Pink utiliza la red peer to peer para distribuir información de comandos en tiempo real. Con esta función, se pudo evaluar la cantidad de infecciones de PinkBot a nivel mundial. El principal proveedor ha estado explorando todos los métodos posibles para eliminar los dispositivos infectados y el número de infecciones se ha reducido significativamente. Si bien, al mismo tiempo, todavía hay una buena cantidad de unidades infectadas con un promedio de 103024 IP activas diarias.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-547
Asunto	NUEVO RANSOMWARE DECAF
Emisión	3/11/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Recientemente se ha observado un nuevo ransomware escrito en el lenguaje de programación Golang, el cual durante su ciclo de infección se configuran los datos necesarios para la actividad maliciosa del ransomware. Este ransomware comienza ejecutando un argumento de línea de comandos, --path, que representa el directorio raíz donde el ransomware comenzará a cifrar archivos mediante la siguiente estructura de un encryptor:

•Prefijo de archivo cifrado: cada encabezado de archivo cifrado comienza con un prefijo especial "magic", 0xDADFEEDBABEDECAF

•Extensión de archivo [.]decaf

•Establece una clave pública de encriptación PKCS1

Se observó que este ransomware antes de empezar el ciclo de cifrado averigua qué directorios debe cifrar en los dispositivos comprometidos. Luego comprueba si --path tiene valor, caso contrario llama a la función FileUtils[.]ListDriverRootPaths(). Luego para terminar esta fase el ransomware crea un objeto WMI para usarlo más adelante.

En conjunto este ransomware utiliza la función main_EncWorker_func1, el cual, será responsable de gestionar nuevas rutas de archivo, llamar a la función de cifrado de archivos y eliminar el archivo original. Una vez cifrado crea un archivo README[.]txt dentro de cada directorio el cual se observa como una nota de rescate con los contactos de los ciberdelincuentes.

Además, se observó que el ransomware DECAF utiliza c con una clave de cifrado generada aleatoriamente, cifrando cada archivo con una clave de cifrado simétrica diferente utilizando una clave pública de los ciberdelincuentes. Luego del cifrado de archivos el ransomware utilizará el objeto creado WMI creado en la fase de inicialización con el fin de ejecutar comandos adicionales y eliminar la capacidad de recuperación en los sistemas comprometidos mediante el proceso cipher[.]exe. Adicionalmente, se observó que los ciberdelincuentes del ransomware DECAF utilizan el método multi-goroutine, el cual, le permite crear varias rutinas de cifrado que esperan mensajes del ciclo de infección inicial.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-548
Asunto	NUEVA CAMPAÑA DE SPEAR PHISHING DISTRIBUYE EL MALWARE DRIDEX
Emisión	3/11/2021
CVE	No
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Recientemente se ha observado que el grupo de ciberdelincuentes conocidos como TA575, propagaba el malware Dridex utilizando señuelos. A finales de octubre de 2021, se observó miles de correos electrónicos dirigidos a todas las industrias principalmente en los Estados Unidos.

Los correos electrónicos pretenden engañar a la víctima completando un documento adjunto para obtener acceso a una plataforma de streaming. Los archivos adjuntos son documentos de Excel con macros que, si están habilitados, descargarán payloads del backdoor bancario Dridex.

Dridex es un backdoor bancario distribuido por múltiples afiliados que puede provocar el robo de datos y la instalación de malware de seguimiento como el ransomware. TA575 es un afiliado de Dridex, el cual distribuye malware a través de URL maliciosas, archivos adjuntos de Microsoft Office y archivos protegidos con contraseña. En promedio, TA575 envía miles de correos electrónicos por campaña que impactan a cientos de organizaciones. TA575 también utiliza la red de distribución de contenido Discord (CDN) para alojar y distribuir Dridex.

Actualización o Mitigación

• Considerar deshabilitar macros en archivos de Office, evitando que pueda ser aprovechado por softwares maliciosos.

Boletín	2021-549
Asunto	NUEVA INFORMACIÓN DEL RANSOMWARE BLACKMATTER
Emisión	3/11/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

BlackMatter está vinculado al grupo de ciberdelincuentes Coreid, que anteriormente era responsable del ransomware Darkside. Durante los últimos 12 meses, los ciberdelincuentes del ransomware Blackmatter han sido uno de los grupos de ransomware con mayor actividad de ciberataques y sus herramientas se han utilizado en una serie de ataques, entre los que destaca el ataque de Darkside de mayo de 2021 en Colonial Pipeline que interrumpió el suministro de combustible. Este grupo de ransomware opera bajo un modelo RaaS, trabajando con afiliados para realizar ataques de ransomware y luego tomando una parte de las ganancias. Actualmente se ha observado que Blackmatter ha implementado entre sus herramientas Exmatter con el propósito de exfiltrar datos.

La herramienta Exmatter se ejecuta como un ejecutable .NET y se ofusca, cuando se ejecuta, comprueba los argumentos de la línea de comandos para las siguientes cadenas: "nownd" y "-nownd". Si se encuentra alguno, intenta ocultar su propia ventana llamando a la API "ShowWindow" con la siguiente función:

•ShowWindow (Process.GetCurrentProcess (). MainWindowHandle, 0);

Con el fin de identificar los archivos para su exfiltración, recuperará los nombres de todas las unidades lógicas en el dispositivo infectado y recopilará todos los nombres de las rutas de los archivos, sin tener en cuenta todo lo que se encuentre en los directorios.

En conjunto excluirá archivos de menos de 1024 bytes de tamaño y archivos con los siguientes atributos:

•FileAttributes.System

•FileAttributes.Temporary

•FileAttributes.Directory

Los archivos que coinciden con los criterios se cargaran en un servidor SFTP remoto. Luego cuando ha terminado de filtrar los datos, Exmatter inicia el siguiente proceso para eliminar cualquier rastro de sí mismo ejecutando comandos en PowerShell.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-550
Asunto	NUEVA CAMPAÑA PROPAGA MALWARE INFOSTEALER APARENTANDO SER UNA APLICACIÓN DE WINDOWS
Emisión	3/11/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Durante un análisis se observó una nueva campaña que propagan malware Infostealer pretendiendo ejecutar códigos maliciosos para robar información confidencial de dispositivos infectados, los ciberdelincuentes que se encuentran propagando esta campaña utilizaron PowerShell, generado por un archivo ejecutable malicioso conocido como HoxLuSfo.exe, con el propósito de intentar realizar una omisión UAC. El proceso HoxLuSfo.exe fue generado por sihost.exe, el cual es un proceso en segundo plano que inicia y mantiene los centros de notificación y acción de Windows.

El propósito de ejecutar comandos en PowerShell es intentar realizar una omisión de UAC a través del software conocido como Disk Cleanup utility, que viene incluido en los sistemas Windows, aparentemente intentando explotar vulnerabilidades, en dispositivos que tienen versiones de Windows 10. En algunos dispositivos, es posible que la utilidad de Disk Cleanup utility se ejecute a través de la tarea programada nativa "SilentCleanup" que, cuando se activa, ejecuta el comando %windir%\system32\cleanmgr.exe/autoclean/d %systemdrive% con privilegios escalados. El comando de PowerShell aprovechó el uso de la variable de entorno %windir% en la ruta especificada en la tarea programada "SilentCleanup" alterando el valor establecido para la variable de entorno %windir%.

Por lo tanto, el reemplazo de la variable de entorno configuró la tarea programada "SilentCleanup" para ejecutar el comando %LOCALAPPDATA%\Microsoft\OneDrive\setup\st.exe REM\system32\cleanmgr.exe /autoclean /d %systemdrive%.

Actualización o Mitigación

• Bloquear los indicadores de compromisos (IOC) compartidos en el boletín asociado, en los dispositivos de seguridad de su infraestructura.

Boletín	2021-551
Asunto	NUEVA ACTIVIDAD DEL RANSOMWARE HELLOKITTY
Emisión	3/11/2021
CVE	CVE-2021-20016, CVE-2021-20021, CVE-2021-20022, CVE-2021 -2002
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows y Linux

• SonicWall SSLVPN SMA100

• SonicWall Email Security versión 10.0.9.x

• MySQL Server versiones anteriores a 8.0.22

Descripción

HelloKitty también es conocido por robar documentos confidenciales de los servidores comprometidos de las víctimas antes de cifrarlos. Los archivos exfiltrados se utilizan más tarde para presionar a las víctimas de pagar el rescate bajo la amenaza de filtrar los datos robados en línea en un sitio de filtración de datos. En algunos casos, si la víctima no responde rápidamente o no paga el rescate, los actores de amenaza pondrá en marcha una denegación de servicio distribuido (DDoS) en el sitio web del lado público de la empresa víctima.

Los operadores de ransomware del grupo utilizarán varios métodos para comprometer las redes de los objetivos, incluidas las credenciales vulneradas y las fallas de seguridad parcheadas recientemente en los productos SonicWall (CVE-2021-20016, CVE-2021-20021, CVE-2021-20022, CVE-2021 -2002). El ransomware HelloKitty o sus variantes también se han utilizado con otros nombres, incluidos DeathRansom y Fivehands.

Desde julio de 2021, la banda de ransomware también se observó utilizando una variante de Linux que apunta a la plataforma de máquina virtual ESXi de VMware y servidores Linux después de que los objetivos empresariales hayan migrado para un uso más eficiente de los recursos y una administración de dispositivos más fácil.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-552
Asunto	NUEVA ACTIVIDAD DEL MALWARE SNAKE
Emisión	4/11/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

• Telegram

• Navegadores basados en Chromium

• Navegadores basados en Gecko

Descripción

Snake es un malware que roba información con muchas funciones y se implementa en el lenguaje de programación .NET. Cuenta con registro de pulsaciones de teclas, así como datos del portapapeles, captura de pantalla y capacidades de robo de credenciales de más de 50 aplicaciones. Snake puede filtrar datos robados a través de una variedad de protocolos, como FTP, Protocolo simple de transferencia de correo (SMTP) y Telegram.

Snake ha estado presente en el panorama de amenazas desde noviembre de 2020 y ha sido una amenaza constante para la privacidad y seguridad de los usuarios desde entonces. Se observó un aumento en las infecciones con el malware Snake a fines de agosto de 2021 sin una tendencia específica en la industria o las ubicaciones geográficas de las víctimas objetivo.

Los ciberdelincuentes distribuyen Snake como archivos adjuntos a correos electrónicos de phishing como solicitudes de pago.

Los archivos adjuntos suelen ser archivos de almacenamiento con extensiones de nombre de archivo como img, zip, tar y rar, y almacenan un ejecutable .NET que implementa el malware Snake. Los usuarios primero deben descomprimir y luego iniciar el ejecutable .NET para infectar sus sistemas. El ejecutable pone en escena las características de robo de información del malware Snake en sistemas comprometidos y establece la persistencia. Snake es casi idéntico a dos programas de malware de robo de información comunes, FormBook y Agent Tesla.

Actualización o Mitigación

• Bloquear los indicadores de compromisos (IOC) compartidos en el boletín, en los dispositivos de seguridad de su infraestructura.

Boletín	2021-553
Asunto	NUEVA ACTIVIDAD DEL GRUPO HIVE RANSOMWARE
Emisión	5/11/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Linux y FreeBSD.

Descripción

Hive es una organización de ransomware que ha comenzado a atacar los sistemas Linux cuando sus objetivos corporativos comenzaron a cambiar a máquinas virtuales (VM) para facilitar las copias de seguridad, la administración de dispositivos y la utilización eficiente de los servicios.
Las nuevas herramientas de cifrado de Hive ransomware se encuentran actualmente en la etapa de desarrollo y aún carecen de funcionalidad. Se conoce que en la versión de Linux el cifrado no funcionaba correctamente cuando el virus se ejecutaba con una ruta exacta.
Esta variante de Linux del ransomware tampoco se encripta cuando se realiza sin privilegios de root porque intenta dejar caer la nota de rescate en los sistemas de archivos raíz de los dispositivos dañados. Esta versión admite un único parámetro de línea de comando (-no-wipe). Y al igual que la versión de Windows, esta variante está escrita en Golang.
Por otro lado, se conoce que la versión de Windows de Hive tiene hasta cinco opciones de ejecución, que incluyen finalizar procesos y omitir la limpieza del disco, además de ignorar archivos poco interesantes y documentos más antiguos.

Actualización o Mitigación

• Bloquear los indicadores de compromisos (IOC) compartidos en el boletín, en los dispositivos de seguridad de su infraestructura.

Boletín	2021-555
Asunto	NUEVA VARIANTE DEL RANSOMWARE HIVE
Emisión	5/11/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Linux.
• Sistemas Operativos FreeBSD.

Descripción

Los ciberdelincuentes del ransomware Hive , se ha mantenido activo desde al menos junio de 2021, actualmente se ha observado que este grupo de ciberdelincuentes han comprometido a más de 30 organizaciones. El grupo es conocido por usar correos electrónicos de phishing con archivos adjuntos maliciosos para obtener acceso a las redes de las víctimas. Una vez dentro de la red, utilizan RDP para moverse lateralmente a través de la red.

Recientemente se observó que esta variante, al momento de ejecutarse en una ruta explícita, el proceso de cifrado no funciona correctamente. Además, la versión de Linux no puede inicializar el proceso de cifrado cuando no se ejecuta con privilegios de root, esto demuestra que esta variante aún se encuentra en desarrollo. Al igual que la versión de Windows, estas variantes están escritos en Golang, pero las cuerdas, los nombres de paquetes y nombres de funciones se han ofuscado, probablemente con gobfuscate.

Adicionalmente se observó que la variante para Linux y FreeBSD tienen soporte para un solo parámetro de línea de comando (-no-wipe), mientras que la variante de Windows equivalente tiene cinco opciones de ejecución.

Actualización o Mitigación

• Bloquear los indicadores de compromisos (IOC) compartidos en el boletín, en los dispositivos de seguridad de su infraestructura.

Boletín	2021-559
Asunto	NUEVA CAMPAÑA DEL RANSOMWARE BABUK
Emisión	8/11/2021
CVE	CVE-2021-34473, CVE-2021-34523, CVE-2021-31207 y CVE-2021-36942
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

- Sistemas Operativos Windows
- Microsoft Exchange Server

Descripción

El ataque de ransomware Babuk se inicia con un archivo DLL o con un ejecutable .NET que se basa en el servidor de Exchange utilizando la vulnerabilidad ProxyShell. La versión ejecutable .NET del descargador inicial es una variante ligeramente modificada del exploit EfsPotato utilizado para descargar y ejecutar la siguiente etapa. EfsPotato es un exploit que intenta escalar los privilegios del proceso utilizando una vulnerabilidad en el sistema de archivos cifrados (CVE-2021-36942).

El módulo ejecutable de .NET inicial se ejecuta como un proceso secundario de w3wp.exe e invoca el shell de comandos para ejecutar un comando en PowerShell. El comando de PowerShell invoca una solicitud web para conectarse a un repositorio malicioso usando el comando Invoke-WebRequest y certutil.exe para descargar el módulo del principal y guardarlo como tortilla.exe para que luego sea ejecutado por el descargador.

El exploit enumera los privilegios del usuario actual y accede al token de usuario y modifica el nivel de acceso del token a MaximumAllowed, por lo que mejora los privilegios y llama a la función CreateProcessAsUser para ejecutar el cargador de la etapa 2 como un nuevo proceso dentro del contexto de seguridad especificado en el token del usuario de la víctima. Los ciberdelincuentes ejecutan una omisión de AMSI y deshabilita la supervisión en tiempo real de Windows Defender, el análisis de secuencias de comandos y la supervisión del comportamiento mediante la ejecución del comando Set-MpPreference.

Actualización o Mitigación

- Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-560
Asunto	NUEVA VARIANTE DEL MALWARE SNAKE KEYLOGGER
Emisión	8/11/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Snake Keylogger es un malware que se ha desarrollado utilizando .NET, este malware apareció por primera vez a fines de 2020 y se centró en robar información confidencial del dispositivo de la víctima, incluidas las credenciales guardadas, las pulsaciones de teclas de la víctima, las capturas de pantalla de la pantalla de la víctima y los datos del portapapeles. En julio de 2021, Snake Keylogger ingresó por primera vez en un informe de las 10 familias de malware más populares, lo que significa que la familia Snake Keylogger está aumentando su influencia e impactando los dispositivos y datos confidenciales de más empresas.

Recientemente se observó que el malware se encuentra propagándose mediante un archivo adjunto dentro de un correo electrónico, el cual contiene código macro VBA malicioso. Una vez que la víctima habilita el contenido, el código VBA malicioso se ejecuta en segundo plano. El proyecto de macro malicioso que contiene el código VBA malicioso está protegido con contraseña para que el analizador no pueda verlo. Al revisar su código, se llama a la función "Workbook_Activate ()" cuando se abre el documento. Luego escribe un fragmento de código de PowerShell de una variable local en un archivo BAT. El código de PowerShell descarga un archivo en el dispositivo de la víctima y lo coloca en "% AppData% \ Wheahmnfpgaqse.exe" llamando a "DownloadFile ()" y lo ejecuta llamando a "Start-Process ()", después, el descargador invoca una función llamada "Consturctor ()". Luego invoca otra función "Program.List_Types ()", donde descarga el módulo Snake Keylogger, desde un enlace malicioso, que es un archivo DLL encriptado RC4. A continuación, llama a la función "ToRc ()" para que RC4 lo descifre utilizando una clave de descifrado "Dllzjn".

Luego procede a cargar el módulo Dll descifrado (conocido como "Huzeigtmvaplpinhoo.dll"), y enumera sus funciones de exportación para encontrar "G6doICqoMU ()", que se invoca ejecutando "type.InvokeMember en la función Consturctor (). El módulo Dll ("Huzeigtmvaplpinhoo.dll") implementa Snake Keylogger en el dispositivo de la víctima y lo configura como un programa de ejecución automátic, para extraer un archivo PE ejecutable en la memoria desde el directorio de recursos y luego realiza un proceso de vaciado que inyecta el archivo PE ejecutable en un proceso recién creado y lo ejecuta.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-561
Asunto	NUEVA INFORMACION DEL MALWARE SQUIRRELWAFFLE
Emisión	8/11/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

En septiembre de 2021, se observó por primera vez una nueva familia de malware conocida como SquirrelWaffle, este malware se propagó a través de documentos maliciosos de Microsoft Office adjuntos en correos electrónicos.

Recientemente se observaron nuevos indicadores de compromisos (IOC) en los documentos que distribuían SquirrelWaffle, entre estos documentos encontramos un documento de Microsoft Word y una hoja de cálculo de Microsoft Excel.

En el documento Microsoft Word imita un documento de DocuSign, pidiendo a la víctima que haga clic en "Habilitar edición" y "Habilitar contenido" para ver el contenido. El archivo contiene varias macros de VBA, la rutina principal se encuentra en una función llamada "eFile", que es ejecutada por la funcionalidad "AutoOpen". El segundo documento es un archivo malicioso de Microsoft Excel, que contiene un mensaje falso que también intenta engañar a la víctima para que haga clic en los botones "Habilitar edición" y "Habilitar contenido". Este documento de igual manera utiliza macros de Excel 4.0 (XML), para mayor información revisar el Boletín SecureSoft-Nro. 2021-530.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-562
Asunto	NUEVA CAMPAÑA DE PHISHING PROPAGA RANSOMWARE MIRCOP
Emisión	9/11/2021
CVE	No
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

El ataque comienza enviando un correo electrónico no solicitado a la víctima, supuestamente siguiendo un arreglo previo sobre una orden. El cuerpo del correo electrónico contiene un hipervínculo a una URL de Google Drive que, si se hace clic, descarga un archivo MHT (archivo de página web) en la máquina de la víctima.

Google Drive sirve para dar legitimidad al correo electrónico y se alinea muy bien con las prácticas comerciales cotidianas.

Los usuarios que abren el archivo solo pueden ver una imagen borrosa de lo que supuestamente es una lista de proveedores, sellada y firmada para darle un toque extra de legitimidad. Cuando se abre el archivo MHT, descargará un archivo RAR que contiene un descargador de malware .NET de "hXXps: // a [.] Pomf [.] Cat / gectpe.rar". El archivo RAR contiene un archivo EXE, que utiliza scripts VBS para colocar y ejecutar el payload de MirCop en el sistema infectado. El ransomware se activa inmediatamente y comienza a tomar capturas de pantalla, bloquea archivos, cambia el fondo a una horrible imagen con temática de zombies y ofrece a las víctimas instrucciones sobre qué hacer a continuación de acuerdo a los atacantes. El usuario solo puede abrir navegadores web específicos para comunicarse con los ciberdelincuentes y organizar el pago del rescate. Los actores de la amenaza no están interesados en comprometer la máquina de la víctima de manera sigilosa o permanecer allí por mucho tiempo para realizar ciberespionaje o robar archivos para extorsión. Por el contrario, el ataque se desarrolla rápidamente y la fuente del problema se vuelve rápidamente evidente para la víctima.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-563
Asunto	NUEVA ACTIVIDAD DEL RANSOMWARE HIVE
Emisión	11/11/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Recientemente una empresa sufrió un ataque de ransomware, en el cual se afectaron servidores y estaciones de trabajo, provocó el cierre de los sistemas de TI para evitar la propagación del ataque. Si bien las ventas en línea de la empresa afectada continúan funcionando como se esperaba, las cajas registradoras no pueden aceptar tarjetas de crédito ni imprimir recibos en las tiendas afectadas. La interrupción del sistema también impide las devoluciones debido a la imposibilidad de buscar compras anteriores.

Según BleepingComputer se ha confirmado que la operación Hive Ransomware está detrás del ataque e inicialmente exigió un monto de rescate de $ 240 millones para recibir un descifrador de archivos. Sin embargo los ciberdelincuentes de ransomware suelen exigir grandes rescates al principio para dejar espacio para la negociación y, por lo general, reciben una fracción de la demanda inicial. Sin embargo, según BleepingComputer se redujo casi automáticamente a una cantidad mucho menor.

Si bien no está claro si se han robado datos no cifrados como parte del ataque, se sabe que el ransomware Hive roba archivos y los publica en su sitio de filtración de datos 'HiveLeaks' si no se paga un rescate.

El ransomware Hive es una operación relativamente nueva lanzada en junio de 2021 que se sabe que infringe las organizaciones a través de campañas de phishing con malware. Una vez que obtienen acceso a una red, los ciberdelincuentes se propagarán lateralmente a través de una red mientras roban archivos no cifrados para usarlos en demandas de extorsión. Cuando obtienen acceso de administrador en un controlador de dominio de Windows, implementan su ransomware en toda la red para cifrar todos los dispositivos. Hive también ha creado variantes que se utilizan para cifrar servidores Linux y FreeBSD, comúnmente utilizados para alojar máquinas virtuales, para mayor información revisar el Boletín SecureSoft-Nro. 2021-555.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-564
Asunto	CIBERDELINCUENTES UTILIZAN GOOGLE ADS PARA ROBAR CREDENCIALES Y VACIAR CUENTAS
Emisión	12/11/2021
CVE	No
Categoría	Cryptominer
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

• Google Ads

Descripción

Algunos anuncios en la web están vinculados para descargar billeteras criptográficas asociadas a Phantom y MetaMask, pero se detectó que ciberdelincuentes comenzaron a utilizar Google Ads para buscar posibles víctimas. Al momento de que un usuario accede a uno de estos anuncios comprometidos es redirigido a un sitio web malicioso que ha sido manipulado para que parezca el sitio de billetera Phantom (u ocasionalmente MetaMask). Luego se le pide al objetivo que registre una nueva cuenta con una "Frase de recuperación secreta". También se les solicita que creen una contraseña para la supuesta cuenta (que es recolectada por los atacantes). Después de eso, los visitantes reciben un atajo de teclado para abrir la billetera y luego se les conduce al sitio auténtico de Phantom.

Si el usuario agrega la pestaña de la billetera de Chrome a su navegador e inserta la frase de recuperación recién creada por el atacante, en realidad inicia sesión en la billetera del atacante en lugar de crear una nueva. Esto significa que, si transfieren fondos, el atacante los obtendrá de inmediato.

Los estafadores utilizarán la Búsqueda de Google como vector de ataque principal para llegar a las billeteras criptográficas, en lugar del tradicional phishing a través del correo electrónico, cada anuncio tenía una selección cuidadosa de mensajes y palabras clave para destacar en los resultados de búsqueda. Los sitios web de phishing a los que se dirigía a las víctimas reflejaban copias e imitaciones meticulosas de los mensajes de la marca de billetera. Y lo más alarmante es que varios grupos de estafadores están pujando por palabras clave en Google Ads, lo que probablemente sea una señal del éxito de estas nuevas campañas de phishing que están orientadas a robar carteras criptográficas.

Actualización o Mitigación

• Bloquear los indicadores de compromisos (IOC) compartidos en el boletín asociado, en los dispositivos de seguridad de su infraestructura.

Boletín	2021-567
Asunto	NUEVA CAMPAÑA DE COMPROMISO DE CORREO ELECTRÓNICO EMPRESARIAL (BEC) DIRIGIDA A USUARIOS DE MICROSOFT 365
Emisión	12/11/2021
CVE	No
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Correos electrónicos Microsoft 365.

Descripción

Esta campaña fue descubierta por primera en septiembre y fue denominada One Font, debido a la forma en que oculta el texto en un tamaño de fuente de un punto dentro de los mensajes. Para este caso, los ciberdelincuentes ocultan enlaces dentro de las hojas de estilo en cascada (CSS) en sus correos electrónicos de phishing.

La campaña One Font también incluye mensajes con enlaces codificados dentro de la etiqueta <font> que, en combinación con las otras técnicas de ofuscación, también destruyen la efectividad de los filtros de correo electrónico que dependen del lenguaje natural para su análisis.

La campaña reciente es similar a una llamada ZeroFont, descubierta en 2018, que utilizó tácticas similares para superar la PNL de Microsoft en sus protecciones de seguridad de Office 365. Esta campaña insertó texto oculto con el tamaño de fuente cero dentro de los mensajes para activar los escáneres de correo electrónico que dependen del lenguaje natural para eliminar los correos electrónicos maliciosos.

Al igual que la campaña ZeroFontr, One Font también se dirige a las organizaciones de Office 365 y puede conducir a BEC y, en última instancia, poner en peligro la red corporativa si los mensajes no se marcan y los usuarios son engañados para que inserten sus credenciales.

Una vez que llega a las bandejas de entrada que parecen ser un mensaje legítimo, la campaña One Font utiliza tácticas típicas de ingeniería social de phishing para llamar la atención de la gente. Los ciberdelincuentes presentan lo que parece un aviso de caducidad de contraseña, utilizando mensajes urgentes para estimular a una víctima potencial a hacer click en un enlace malicioso. Este enlace los lleva a una página de phishing donde parecen estar ingresando sus credenciales para que puedan cambiar sus contraseñas y mediante esto, los ciberdelincuentes están sustrayendo sus credenciales para usarlas en otras actividades delictivas cibernéticas.

Actualización o Mitigación

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

Boletín	2021-568
Asunto	NUEVA CAMPAÑA DEL MALWARE BAZARLOADER UTILIZA EL INSTALADOR DE APLICACIONES DE WINDOWS
Emisión	12/11/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows.

Descripción

BazarLoader (también conocido como BazarBackdoor, BazaLoader, BEERBOT, KEGTAP y Team9Backdoor) es un backdoor que se usa comúnmente para comprometer las redes de objetivos de alto valor y vender acceso a activos comprometidos a otros ciberdelincuentes. También se ha utilizado para entregar payloads adicionales, como beacon Cobalt Strike que ayudan a los ciberdelincuentes a acceder a la red de sus víctimas y, en última instancia, implementar ransomware. En la campaña recientemente observada, utilizan correos electrónicos propagados por ciberdelincuentes que inducen una sensación de urgencia al hacerse pasar por un gerente de la empresa que solicita más información sobre una queja de un cliente sobre el destinatario del correo electrónico. Esta queja está supuestamente disponible para su revisión como PDF desde un sitio alojado en el propio almacenamiento en la nube de Microsoft, el cual en realidad descarga el backdoor BazarLoader utilizando un subdominio de adobeview que agrega aún más credibilidad al esquema.

Los ciberdelincuentes utilizaron dos direcciones web diferentes para alojar esta página falsa de 'descarga de PDF', ambas páginas se alojaron en el almacenamiento en la nube de Microsoft, lo que quizás le dé una sensación de autenticidad, y los archivos .appinstaller y .appbundle se alojaron en la raíz del almacenamiento de cada página web. Sin embargo, en lugar de apuntar a un documento PDF, el botón "Vista previa de PDF" en el sitio de aterrizaje de phishing abre una URL con un prefijo ms-appinstaller. Al hacer clic en el botón, el navegador primero mostrará una advertencia que le preguntará a la víctima si desea permitir que el sitio abra el Instalador de aplicaciones. Una vez ejecutado, App Installer primero comenzará a descargar el archivo .appinstaller malicioso de los ciberdelincuentes y un archivo .appxbundle que contiene el payload final llamada Security.exe dentro de una subcarpeta UpdateFix . El payload descarga y ejecuta un archivo DLL adicional que se inicia y genera un proceso secundario que, a su vez, genera otros procesos secundarios, y finalmente termina la cadena con la inyección del código malicioso en un proceso de navegador Edge basado en Chromium. Después de implementarse en el dispositivo comprometido, BazarLoader comenzará a recolectar información del sistema (por ejemplo, disco duro, procesador, placa base, RAM, hosts activos en la red local con direcciones IP públicas). Esta información se envía al servidor de comando y control, camuflada como cookies entregadas a través de los encabezados HTTPS GET o POST.

Actualización o Mitigación

• Bloquear los indicadores de compromisos (IOC) compartidos en el boletín, en los dispositivos de seguridad de su infraestructura.

Boletín	2021-569
Asunto	NUEVO GRUPO DE CIBERDELINCUENTES VOID BALAUR
Emisión	12/11/2021
CVE	No
Categoría	Cryptominer
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

El grupo ruso conocido como Void Balaur, también conocido bajo el nombre de Rockethack, ha sido identificado como un grupo de ciberdelincuentes, que se ofrece para ser contratado para ingresar en el correo electrónico y las cuentas de redes sociales de objetivos de alto perfil y alto riesgo en todo el mundo.

Durante una investigación por Trend Micro se observó que el grupo Void Balaur busca los datos más privados y personales de empresas e individuos y luego vende esos datos a quien quiera pagar por ellos. Por una tarifa premium, el grupo a menudo puede proporcionar copias totales de los buzones de correo, robados sin la ayuda del usuario objetivo, informó.

El grupo de ciberdelincuentes también ha lanzado ataques contra los intercambios de criptomonedas como EMXO, que según el informe ha sido victimizado varias veces por Void Balaur. En septiembre, el grupo apuntó al jefe de la agencia de inteligencia, los ministros del gobierno y los dos miembros de un parlamento de Europa del Este, Void Balaur también está activo en los EE. UU., Israel y Japón.

El grupo parece estar dispuesto a trabajar en casi cualquier sector que ofrezca una gran cantidad de datos valiosos, incluidas las telecomunicaciones, las comunicaciones por radio y por satélite, la banca, la aviación, los seguros médicos, entre otros.

Actualización o Mitigación

• Bloquear los indicadores de compromisos (IOC) compartidos en el boletín, en los dispositivos de seguridad de su infraestructura.

Boletín	2021-570
Asunto	NUEVO MALWARE BOTENAGO
Emisión	12/11/2021
CVE	CVE-2015-2051, CVE-2020-9377, CVE-2016-11021, CVE-2016-1555, CVE-2017-6077, CVE-2016-6277, CVE-2017-6334, CVE-2019-19824, CVE-2017-18368, CVE-2020-9054, CVE-2020-10987, CVE-2014-2321 y CVE-2020-8958.
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Según lista boletín

Descripción

BotenaGo fue escrito en Golang (Go), ha ido ganando popularidad en los últimos años y los autores de malware lo adoran por crear payloads que son más difíciles de detectar y realizar ingeniería inversa. Se descubrió que la botnet se dirige a millones de dispositivos con funciones que aprovechan las vulnerabilidades. A continuación, se muestran los más populares:

• CVE-2015-2051, CVE-2020-9377, CVE-2016-11021: routers D-Link

• CVE-2016-1555, CVE-2017-6077, CVE-2016-6277, CVE-2017-6334: dispositivos Netgear

• CVE-2019-19824: routers basados en Realtek SDK

• CVE-2017-18368, CVE-2020-9054: routers Zyxel y dispositivos NAS

• CVE-2020-10987: Productos Tenda

• CVE-2014-2321: módems ZTE

• CVE-2020-8958: Guangzhou 1GE ONU

Una vez instalado, el malware creara dos puertos de backdoor (31412 y 19412), donde espera que se le envíe una dirección IP de la víctima. Una vez que se recibe uno, el bot explotará cada vulnerabilidad en esa dirección IP para obtener acceso. Una vez que BotenaGo obtenga acceso, ejecutará comandos de shell remotos para reclutar el dispositivo en la botnet. Según el dispositivo al que se dirija, el malware utiliza diferentes enlaces para obtener un payload coincidente. Aún no está claro qué actor de amenaza está detrás del malware y la cantidad de dispositivos infectados.

Actualización o Mitigación

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

Boletín	2021-571
Asunto	NUEVO MALWARE ABCBOT DIRIGIDO A LINUX
Emisión	13/11/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Linux

Descripción

Si bien la primera versión de la botnet se remonta a julio de 2021, las nuevas variantes observadas tan recientemente como el 30 de octubre han sido equipadas con actualizaciones adicionales para atacar servidores web Linux con contraseñas débiles y que son susceptibles a vulnerabilidades de días cero, también una implementación personalizada de DDoS, lo que indica que el malware está en continuo desarrollo. Hasta la fecha, se han observado un total de seis versiones de la botnet.

Una vez instalado en un host comprometido, el malware desencadena la ejecución de una serie de pasos que dan como resultado que el dispositivo infectado se reutilice como servidor web, además de informar la información del sistema a un servidor de comando y control, propagándose el malware a nuevos dispositivos mediante la búsqueda de puertos abiertos y la actualización automática a medida que sus operadores ponen a disposición nuevas funciones.

En el análisis se observó que Abcbot informa repetidamente la información del dispositivo local, no registra los nombres de dominio DGA, excluye irrazonable los servidores de recursos TOR y Github, y la funcionalidad del servidor web no está realmente habilitada, lo que indica que los autores de Abcbot están probando varias tecnologías.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

Boletín	2021-573
Asunto	NUEVA CAMPAÑA DE PHISHING PROPAGA MALWARE QBOT
Emisión	15/11/2021
CVE	No
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

DatopLoader (también conocido como Squirrelwaffle) compromete a las víctimas a través de una campaña de malspam y proporciona a los actores de amenazas un punto de apoyo inicial en los sistemas y entornos de red de las víctimas. Esto se puede usar para facilitar más compromisos o infecciones de malware adicionales.

Se detecto un archivo de Excel malicioso que intentaba ejecutar tres archivos diferentes usando regsvr32[.]exe. A primera vista, este archivo de Excel contiene una hoja que guía al usuario para habilitar la macro, lo que conduce a una conexión de red y finalmente a la entrega de QakBot. Se reviso en modo desarrollador en Excel y se verifico el proyecto VBA de este archivo encontrando 3 hojas en modo oculto que contenían Excel Macro 4 que crean una nueva carpeta usando kerner32[.]dll!CreateDirectoryA. el cual descarga 3 archivos de dominios diferentes. Se descubrió que los tres archivos descargados eran DLL de troyanos bancarios Qakbot del cual se trata de un troyano bancario diseñado para robar las credenciales de las cuentas y la información de las sesiones bancarias en línea, lo que lleva al fraude por adquisición de cuentas.

Actualización o Mitigación

• Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.

5. Recomendaciones

- Leer los boletines citados en las amenazas que tengan uno asociado, esto con la finalidad de encontrar más información de la amenaza como: Una mayor descripción, Indicadores de compromiso, recomendaciones personalizada y fuentes por amenaza.
- Considerar deshabilitar PowerShell y Macros de Microsoft, evitando que pueda ser aprovechado por softwares maliciosos.
- Utilizar una política de uso de contraseñas seguras considerando la complejidad, el cambio de credenciales por defecto y la no reutilización de las mismas.
- Mantener un protocolo estricto para realizar copias de seguridad de los activos de información de mayor criticidad.
- Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.
- Bloquear los indicadores de compromisos (IOC) compartidos en el boletín asociado, en los dispositivos de seguridad de su infraestructura.
- Verificar la información de la cuenta que envía el correo, el nombre y la dirección del destinatario para identificar si son sospechosas.
- No abrir correos electrónicos de dudosa procedencia (remitente desconocido), ni dar clic en enlaces, ni descargar archivos adjuntos desconocidos.
- Escanear todo el software descargado de Internet antes de la ejecución.
- De detectar un correo spam, phishing o cualquier actividad anómala reportarlo. inmediatamente a los encargados de seguridad de la información de su institución.

* Antes de realizar el bloqueo de IoC's es importante que previamente en ambiente de desarrollo se valide y confirme a nivel de sus servicios internos y externos, con el propósito de aplicar los cambios de manera controlada.

** Es importante que previamente en ambiente de desarrollo se valide y confirme a nivel de los servicios, con el propósito de aplicar los cambios de manera controlada.