SECURESOFT CORPORATION
e-Secure Consulting Group

Reporte Semanal de Ciberinteligencia Securesoft

Fecha:

03 Agosto de 2020

El presente documento contiene información para la comunidad de ciberseguridad.

Equipo de Ciberinteligencia

CIB-FOR-2020-002

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

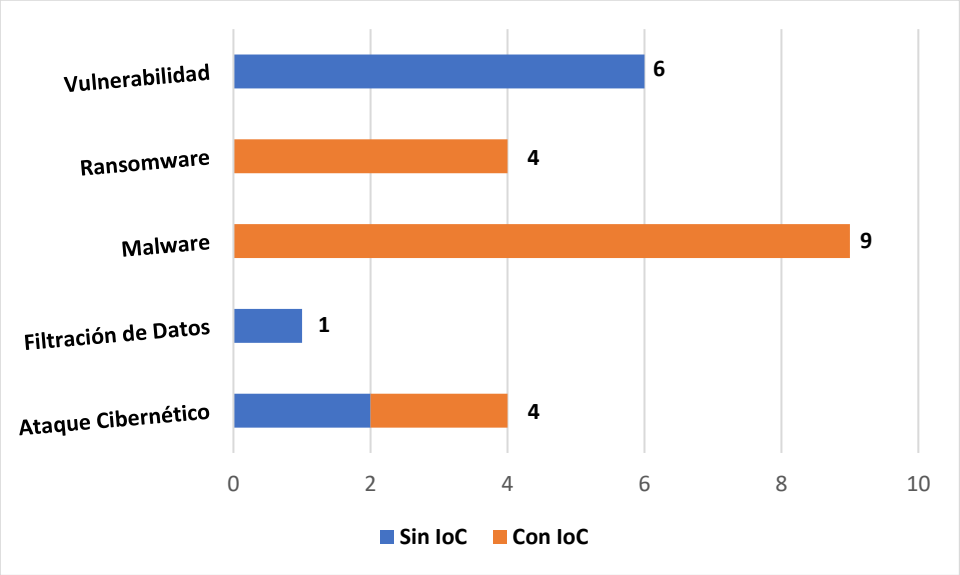
Este documento muestra el resumen, la fecha de publicación, CVE asociado y servicios afectados de vulnerabilidades y amenazas que se han hecho públicas en el transcurso del 14 de julio hasta el 02 de agosto del 2020.

3. Resumen

En el presente informe se exponen 24 análisis de vulnerabilidad y amenazas, de las cuales 4 han sido consideradas como críticas mientras que 20 como altas.

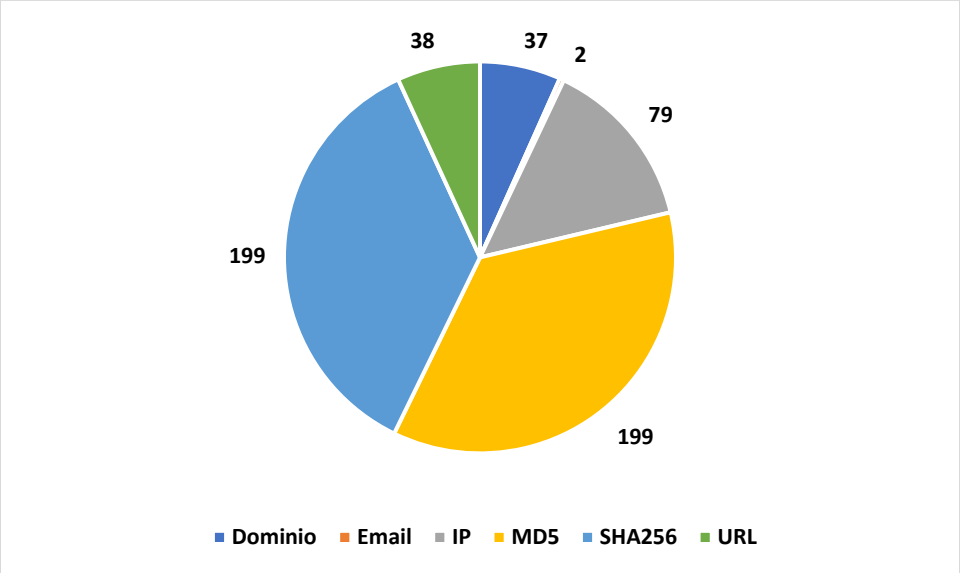
Amenazas analizadas por tipología

En las investigaciones elaboradas para el presente informe se trataron vulnerabilidades, malware, ataques cibernéticos y ransomware. 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 554 IoC entre Dominios, Email, IP, MD5, SHA256 y URL's.



Tendencias en nuevas vulnerabilidades críticas

- De acuerdo con nuestras fuentes de inteligencia la nueva vulnerabilidad asignada al CVE-2020-1350 está siendo explotada por los cibercriminales. Esta vulnerabilidad afecta a las versiones de Windows Server desde la 2003 hasta la 2019. Para más información leer el Boletín 2020-220, en la cual podrá encontrar la actualización para esta vulnerabilidad.

- Otra vulnerabilidad que es tendencias es la CVE-2020-6287, del componente de SAP, para más información se sugiere leer el resumen que se encuentra en este informe y el Boletín 2020-219. Esta es una vulnerabilidad crítica. Durante los últimos días se ha registrado muchas actividades que se relacionan con la vulnerabilidad.

Actividades maliciosas asociadas a grupo de cibercriminales

- Durante las últimas se ha detectado que el grupo de cibercriminales Lazarus ha estado ejecutando múltiples ataques. Destaca el uso del framework MATA por parte de este grupo, el cual es usado para afectar a víctimas que usan los sistemas operativos: Linux, MacOS y Windows. Para más información se sugiere leer el resumen que se encuentra en este reporte o ver el Boletín 2020-230.

4. Detalles

Vulnerabilidades

Boletín	2020-215
Asunto	ZOOM RECIBE ACTUALIZACIÓN DE SEGURIDAD PARA MITIGAR VULNERABILIDAD DE DÍA CERO
Emisión	10/07/2020
CVE	No tiene
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

Aplicación Zoom para Windows 7 y sistemas operativos anteriores de Microsoft sin soporte

Descripción

La vulnerabilidad está presente en cualquier versión de Zoom compatible con Windows, se sospecha que los atacantes desconocen de su existencia. Para que la vulnerabilidad pueda ser explotada es necesario que se cumplan unos factores. En primer lugar, la vulnerabilidad solo puede ser explotada en Windows 7 y sistemas Windows antiguos, que estén al final de su vida útil y ya no reciban soporte por parte de Microsoft. En segundo lugar, es necesario que la víctima realice una acción como abrir un archivo malicioso, el cual funciona como exploit.

Zoom fue notificado de la existencia de dicha vulnerabilidad, recibió documentación en la cual se exponían diversos escenarios que hacían posible la explotación de esta. Es así como se confirmó la existencia de la vulnerabilidad. El cliente de Zoom tiene una funcionalidad de actualización automática, por lo que la actualización será recibida por la mayoría de los usuarios de manera automática.

Actualización o Mitigación

Aplicar las actualizaciones para estas vulnerabilidades proporcionadas por Zoom. Para ello haga clic aquí.

Imagen 1. Imagen de referencia del producto afectado

Boletín	2020-219
Asunto	VULNERABILIDAD EN UN COMPONENTE DE SAP - CRÍTICA
Emisión	14/07/2020
CVE	CVE-2020-6287
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

Soluciones de SAP que usan el componente SAP NetWeaver AS Java de la 7.30 a la 7.50

Descripción

RECON, es la abreviatura de código remotamente explotable en NetWeaver, esta tiene el puntaje máximo en la escala de CVSS, por lo que puede ser explotado remotamente por atacantes no autenticados para comprometer los sistemas SAP vulnerables. RECON está identificada con el CVE-2020-6287.

Esta vulnerabilidad se debe a la falta de autenticación en un componente web de SAP NetWeaver AS Java, la cual permite realizar actividades de alto privilegio en sistemas SAP afectados. La explotación exitosa permite crear un nuevo usuario de SAP con máximos privilegios, omitiendo todos los controles de acceso y autorización, obteniendo control total sobre todo el sistema SAP. Esto a su vez permite leer, modificar y eliminar cualquier registro, archivo o informe sobre el sistema comprometido.

Un ataque exitoso también les permitiría cambiar los datos bancarios de una empresa comprometida (número de cuenta, IBAN, etc.), leer información de identificación personal (PII, por sus siglas en inglés), realizar acciones sin restricciones a través de la ejecución de comandos del sistema operativo y tomar el control de la administración de los procesos de compra.

Actualización o Mitigación

Aplicar las actualizaciones proporcionadas por Cisco. Para ello haga clic aquí.

Imagen 2. Imagen de referencia de la marca de los productos afectados

Boletín	2020-220
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE MICROSOFT - JULIO 2020 - CRÍTICA
Emisión	15/07/2020
CVE	Varios
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

Sistema operative Windows

Descripción

Microsoft ha publicado actualizaciones para 123 vulnerabilidades. De las cuales 18 son consideradas como críticas y 105 como importantes.

En este paquete de actualizaciones, la vulnerabilidad corregida más destacada es una que se encuentra presente en el Servidor DNS de Windows server 2003, 2008 y 2019. La cual permite la ejecución de código remoto. Esta fue asignada al CVE-2020-1350 y denominada con el nombre SigRed. La vulnerabilidad se debe a un desbordamiento de buffer, el cual se da cuando se procesa una consulta SIG grande, mayor a 64 KB.

Actualización o Mitigación

Se recomienda leer el boletín que se encuentra citado en la primera fila de la tabla de esta hoja. Ahí se encontrarán más vulnerabilidades junto a su actualización.

Imagen 3. Imagen de referencia de la marca de los productos afectados

Boletín	2020-222
Asunto	CISCO PUBLICA ACTUALIZACIÓN DE SEGURIDAD - CRÍTICA
Emisión	16/07/2020
CVE	Varios
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Software Cisco PLM versiones 10.5 SU9 y anteriores, y 11.5 SU6 y anteriores
• RV110W Wireless-N VPN Firewall
• RV130 VPN Router
• RV130W Wireless-N Multifunction VPN Router
• RV215W Wireless-N VPN Router

Descripción

• CVE-2020-3140: Permite a un atacante no autenticado obtener acceso al dispositivo afectado. Esta se debe a una validación incorrecta del usuario en la interfaz de administración web. Para obtener la actualización para esta vulnerabilidad haga clic aquí.

• CVE-2020-3144: Permite a un atacante no autenticado evitar la autenticación y ejecutar comandos arbitrarios en el dispositivo afectado. Esta se debe a una gestión de sesión incorrecta. Para obtener la actualización para esta vulnerabilidad haga clic aquí.

• CVE-2020-3323: Permite a un atacante no autenticado ejecutar código remoto de manera arbitraria en un dispositivo afectado. Esta se debe a una validación incorrecta en la interfaz de administración web, para aprovecharse de esta vulnerabilidad se tiene que enviar solicitudes HTTP maliciosas. Para obtener la actualización para esta vulnerabilidad haga clic aquí.

• CVE-2020-3330: Permite a un atacante no autenticado tome el control total del dispositivo mediante una cuenta con privilegios elevados. Esta se debe a que una cuenta del sistema tiene una contraseña predeterminada y estática. Para obtener la actualización para esta vulnerabilidad haga clic aquí.

• CVE-2020-3331: Permite a un atacante no autenticado ejecutar código remoto de manera arbitraria en un dispositivo afectado. Esta se debe a una validación incorrecta en la interfaz de administración web. Cabe resaltar que esta vulnerabilidad es parecida a la CVE-2020-3323, sin embargo, afecta a menos dispositivos. Para obtener la actualización para esta vulnerabilidad haga clic aquí.

Actualización o Mitigación

Aplicar las actualizaciones para cada vulnerabilidad, accediendo a está a través del link proporcionado en cada vulnerabilidad.

Boletín	2020-232
Asunto	CISCO PUBLICA ACTUALIZACIÓN DE SEGURIDAD
Emisión	24/07/2020
CVE	CVE-2020-3452
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

Software ASA y FTD

Descripción

La vulnerabilidad ha sido asignada al CVE-2020-3452. Si un atacante no autenticado explota con éxito esta vulnerabilidad puede acceder a archivos confidenciales en sistemas afectados a través de ataques transversales de directorio.

CVE-2020-3452 es causado por una validación incorrecta de URL en las solicitudes HTTP que permite al atacante explotar la vulnerabilidad mediante el envió de solicitudes especialmente diseñadas con secuencias de caracteres transversales de directorio.

Los atacantes pueden aprovecharse de esta vulnerabilidad para obtener acceso remoto y leer archivos de manera arbitraria de los dispositivos destino, los cuales están almacenados dentro del sistema de archivos del servicio web que solo está habilitado cuando se encuentra configurado con las funciones AnyConnect o WebVPN.

Actualización o Mitigación

Aplicar las actualizaciones recomendadas por Cisco de acuerdo con el producto afectado. Para ello haga clic aquí.

Imagen 4. Imagen de referencia de la marca de los productos afectados

Boletín	2020-236
Asunto	CISCO PUBLICA ACTUALIZACIÓN DE SEGURIDAD - CRÍTICA
Emisión	24/07/2020
CVE	CVE-2020-3452
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

Software ASA y FTD

Descripción

La vulnerabilidad asignada al CVE-2020-3382 es de omisión de autenticación, tiene una puntuación de 9.8 de 10 en la escala de CVSS. Esta se encuentra en la API REST de Cisco DCNM. Si un atacante explota exitosamente esta vulnerabilidad puede omitir la autenticación y ejecutar de forma remota acciones arbitrarias en dispositivos vulnerables con privilegios administrativos, a través de la API REST.

CVE-2020-3382 afecta a todos los modos de implementación de todos los dispositivos Cisco DCNM instalados con instaladores .ova o .iso y software Cisco DCNM. Cisco confirmó que la vulnerabilidad no afecta a las instancias de Cisco DCNM instaladas en sistemas operativos Windows o Linux.

La vulnerabilidad asignada al CVE-2020-3374 es de omisión de autorización, posee una puntuación de 9.9 de en la escala de CVSS. Permite a un atacante autenticado omitir la autorización, accediendo a información confidencial, modificar la configuración del sistema, o afectar la disponibilidad del sistema afectado.

La vulnerabilidad asignada al CVE-2020-3375 es de desbordamiento de búfer. La cual permite a un atacante remoto no autenticado obtener acceso a información, realizar cambios en el sistema y ejecutar comandos de manera arbitraria.

Cisco también corrigió otras 5 vulnerabilidades de severidad alta y 3 vulnerabilidades de severidad baja. Para ver información de estas vulnerabilidades acceda al boletín de esta noticia.

Actualización o Mitigación

Aplicar las actualizaciones recomendadas por Cisco de acuerdo con el producto afectado. Para ello haga clic aquí.

Amenazas

Boletín	2020-214
Asunto	NUEVO ATAQUE DE REVIL RANSOMWARE
Emisión	10/07/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Las víctimas de este grupo de cibercriminales son empresas y los clientes de estos últimos, los ataques que realizan tienen por objetivo robar información financiera.

Los ataques inician con correos electrónicos de spearphishing que contienen archivos .LNK que fingen ser una imagen o un documento. Cuando la víctima lo abre, se ejecuta un componente JavaScript malicioso. La función del componente JavaScript es la de implementar otro malware como el módulo de espionaje Evilnum, malware de Golden Chickens MaaS y múltiples herramientas basadas en Python. También se detectó otro componente malicioso desarrollado en C#, el cual tienen funciones similares al del componente JavaScript.

En las operaciones realizadas por este grupo de atacantes, varios componentes se ejecutan de forma independiente y se conectan a diferentes servidores de comando y control (C2, abreviado en inglés) para recibir comandos y herramientas.

Las herramientas y la infraestructura de Golden Chickens MaaS son utilizadas por grupos como FIN6 y Cobalt, y TrickBot.

Se detectó que Evilnum utiliza ampliamente las herramientas de Golden Chickens. Entre los payloads usados por estos se encuentran TerraStealer, TerraTV y TerraPreter. Luego usan herramientas basadas en Python para obtener una shell inversa, proxy SSL, entre otros. El conjunto de herramientas se completa con scripts de PowerShell para eludir controles de seguridad y utilidades de NirSoft para extraer contraseñas de clientes de correo electrónico y licencias de Microsoft Office y Windows.

La mayoría de los servidores C2 utilizados por los atacantes no tienen un nombre de dominio, solo se identifican por una dirección IP. Las direcciones se obtienen de las páginas GitHub, GitLab y Reddit.

Boletín	2020-216
Asunto	CONTI RANSOMWARE
Emisión	13/07/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Se sospecha que los atacantes detrás de Ryuk ransomware, decidieron hacer una transición a Conti, el cual posee código basado en Ryuk, por lo que parece una nueva versión de este. Además de esto se ha observado que la nota de rescate que deja Conti es similar a la que utiliza Ryuk. Por otro lado, también se identificó que la infraestructura utilizada por Trickbot y Ryuk es usada por Conti para realizar sus ataques.

Debido a lo anteriormente mencionado, se cree que Conti está vinculado al mismo grupo de desarrolladores de Ryuk.

Conti al infectar la computadora de la víctima la prepara para el cifrado, es así como detendrá 146 servicios de Windows relacionados con soluciones de seguridad, respaldo, base de datos y correo electrónico.

Al encriptar una computadora, el ransomware agregará la extensión .CONTI a los archivos encriptados y colocará una nota de rescate llamada CONTI_README.txt en cada carpeta afectada. Se ha detectado que utiliza una clave de cifrado AES-256 única por archivo, que luego se cifra con una clave de cifrado pública RSA-4096. Esta clave RSA es única por víctima.

Al cifrar archivos, Conti usa una API de Windows llamada “Administrador de reinicio de Windows” que terminará los procesos o servicios de Windows que mantienen un archivo abierto durante el cifrado.

Imagen 5. Imagen de referencia de la amenaza

Boletín	2020-217
Asunto	TRICKBOT ADVIERTE POR ERROR A SUS VÍCTIMAS
Emisión	13/07/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

En una versión reciente analizada del malware TrickBot, se detectó que los atacantes distribuyen por error una versión de prueba del módulo grabber.dll que roba contraseñas. Cuando este módulo se carga, muestra una advertencia en el navegador que indica que está recopilando información.

El módulo grabber.dll, se encarga de recolectar credenciales y cookies guardadas en los navegadores Chrome, Edge, Internet Explorer y Firefox. Estas credenciales y cookies robadas se pueden usar para iniciar sesión en las cuentas de la víctima.

Durante el análisis se encontró documentación con algunas de las funcionalidades del malware, las cuales son: Guardar los archivos flash comunes, mostrar solo los errores críticos, mostrar información de la versión y salir, mostrar ayuda y salir, entre otros.

Se sospecha que este módulo ha sido codificado por los mismos desarrolladores de TrickBot, ya que esta codificado de forma similar que otros módulos del este mismo malware. El mensaje que se muestra es de pruebas y los atacantes olvidaron de eliminarlo de la versión que se publicó.

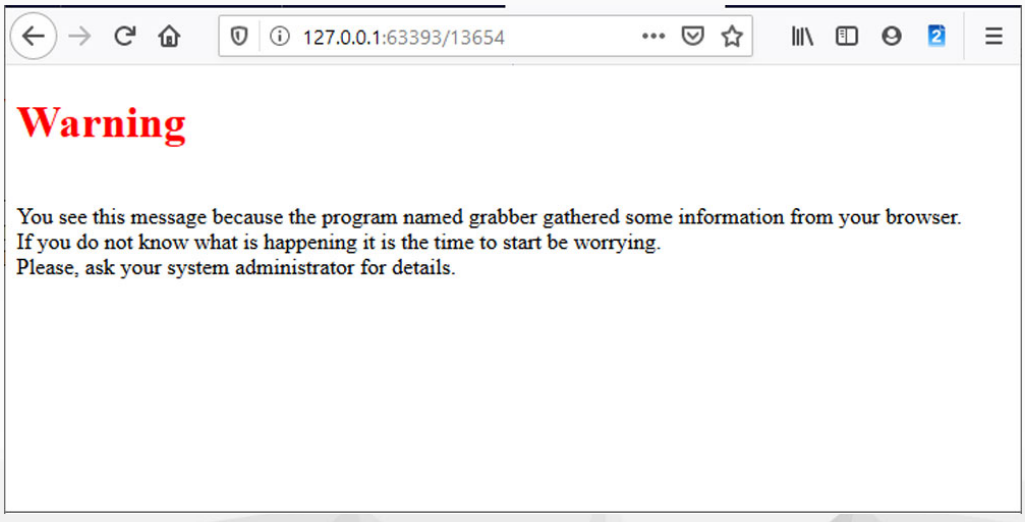


Imagen 6. Imagen de referencia del mensaje que deja la amenaza

Boletín	2020-218
Asunto	NUEVA VARIANTE MIRAI
Emisión	14/07/2020
CVE	CVE-2020-10173
Categoría	Malware
Severidad	Alta

Servicios Afectados

Cámaras IP, televisores inteligentes y routers, entre otros

Descripción

Esta variante de Mirai combina vulnerabilidades antiguas y nuevas, que le permiten afectar a diferentes dispositivos conectados. Estas afectan a cámaras IP, televisores inteligentes y enrutadores, entre otros.

La vulnerabilidad más notable que está aprovechando Mirai es la CVE-2020-10173, esta permite inyección de comandos en el router Comtrend VR-3033. Lo cual permite a los atacantes comprometer la red administrada por el router afectado. Hasta el momento solo se ha publicado una prueba de concepto (PoC, por sus siglas en inglés) para esta vulnerabilidad, sin ningún exploit reportado hasta antes de esta variante Mirai.

Una característica distintiva de las variantes de Mirai es el uso de ataques de fuerza bruta Telnet y Secure Shell (SSH, por sus siglas en inglés). En la muestra analizada se observa que se utiliza el cifrado XOR para ocultar las credenciales que usa para atacar dispositivos vulnerables, algunas de estas son: 1001chin, 1111, 1234, 12345, 123456, 5up, anko, cat1029, dreambox, gm8182, hg2x0, huigu309, ipcam_rt5350, iwkb, entre otros.

Imagen 7. Imagen de referencia de la amenaza

Boletín	2020-221
Asunto	MALWARE GOLDENHELPER ENCONTRADO EN SOFTWARE OFICIAL CHINO
Emisión	16/07/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operative Windows

Descripción

La campaña de distribución del malware GoldenHelper estuvo activa entre enero de 2018 y julio de 2019, sus dominios de comando y control (C2, abreviado en inglés) expiraron en enero de 2020.

De acuerdo con lo observado GoldenHelper utiliza técnicas sofisticadas para ocultar su distribución, presencia y actividad. Algunas de las técnicas que el malware usa incluyen la aleatorización de la ubicación del sistema de archivos, el cronometraje, algoritmo de generación de dominio (DGA, por sus siglas en inglés) basados en IP, la omisión del control de cuentas de usuario (UAC, por sus siglas en inglés) y la escalada de privilegios.

El payload de GoldenHelper es un binario denominado taxver.exe, el cual se descarga y ejecuta con privilegios de nivel SYSTEM desde múltiples ubicaciones en los sistemas infectados.

Relaciones entre las campañas GoldenSpy y GoldenHelper:

• Los malwares se instalan junto con el software fiscal legítimo.
• Los malwares utilizan una infraestructura de control y comando de red separada de la utilizada por el software fiscal.
• Los malwares tienen la capacidad de descargar y ejecutar de forma remota código arbitrario con privilegios de nivel SYSTEM.
• Los malwares utilizan técnicas de ofuscación para ocultar las metodologías de implementación y comunicación.

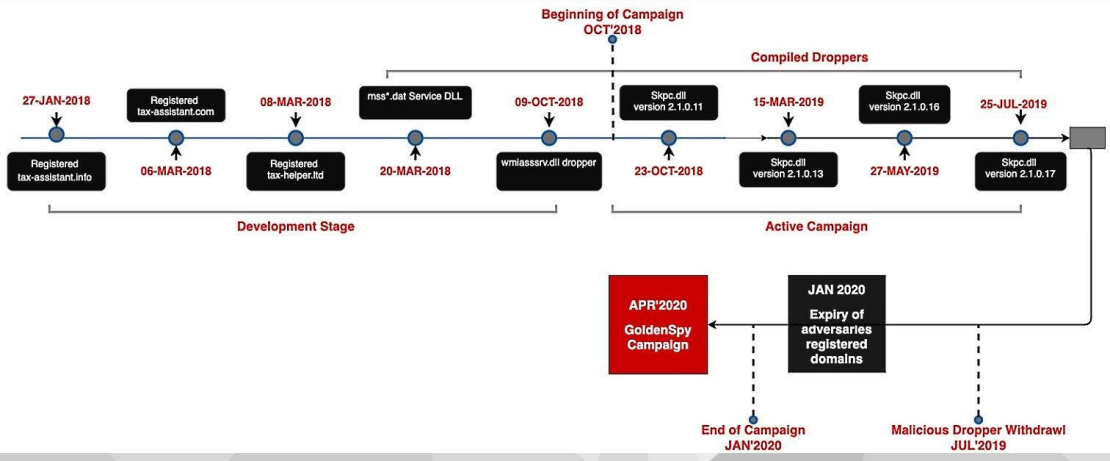


Imagen 8. Línea de tiempo de la campaña de GoldenHelper

Boletín	2020-223
Asunto	NUEVA VÍCTIMA DEL RANSOMWARE NEFILIM
Emisión	17/07/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

Sistema Operativo Windows, servicios RDP y VPN

Descripción

Recientemente los atacantes detrás del ransomware Nefilim agregaron a la empresa Orange a su sitio de exposición de datos y comunicaron que habían comprometido a la empresa a través de su división "Orange Business Solutions".

Por otra parte, la empresa Orange comunicó que fue víctima de un ataque de ransomware dirigido a su división de Orange Business Services entre la noche del sábado 4 de julio y domingo 6 de julio de 2020. De acuerdo con el análisis ejecutado por la empresa, el ataque fue contra la plataforma de TI de Neocles, "Le Forfait informatique", después de este ningún otro servicio se vio afectado.

La plataforma "Le Forfait Informatique" de Orange permite a los clientes empresariales tener computadoras virtuales en la nube.

Como parte de la filtración de datos, los ciberdelincuentes publicaron un archivo de 339MB llamado "Orange_leak_part1.rar", el cual contenía datos robados de la compañía durante el ataque que ejecutaron. Al analizar el archivo "Orange_leak_part1.rar", se encontró que este contenía correos electrónicos, esquemas de aviones y archivos de ATR Aircraft, un fabricante francés de aviones. Lo cual podría indicar que ATR Aircraft fue uno de los clientes de Orange que resultó afectado por el ataque.

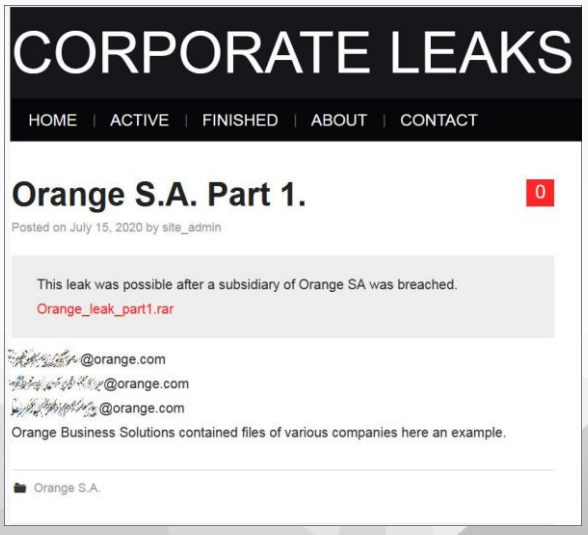


Imagen 9. Imagen de referencia de la filtración de datos

Boletín	2020-224
Asunto	ATAQUES DE APT29 CONTRA ORGANIZACIONES QUE INVESTIGAN VACUNA PARA EL CORONAVIRUS
Emisión	20/07/2020
CVE	CVE-2019-9670, CVE-2019-11510, CVE-2019-13379 y CVE-2019-19781
Categoría	Ataque cibernético
Severidad	Alta

Servicios Afectados

Sistema operativo Windows, Citrix, Pulse Secure, Fortigate y Zimbra's Collaboration Suite

Descripción

Según el Centro Nacional de Seguridad Cibernética (NCSC, por sus siglas en inglés) del Reino Unido (UK, por sus siglas en inglés), se observó que APT29 ha estado ejecutando ataques durante el 2020 contra entidades de Canadá, UK y los Estados Unidos (USA, por sus siglas en inglés).

De acuerdo con lo observado Cozy Bear comienza sus ataques con spear-phishing, pero también explota vulnerabilidades de productos Citrix (CVE-2019-19781), Pulse Secure (CVE-2019-11510), Fortigate (CVE-2019-13379) y Zimbra's Collaboration Suite (CVE-2019-9670).

Después de acceder a la red los atacantes utilizan SoreFang y los malware personalizados WellMess y WellMail, para comprometer aún más a su víctima.

Estas son algunas de las herramientas que usa este grupo de ciberdelincuentes para atacar a sus objetivos gubernamentales, empresas del sector energético, entre otros.

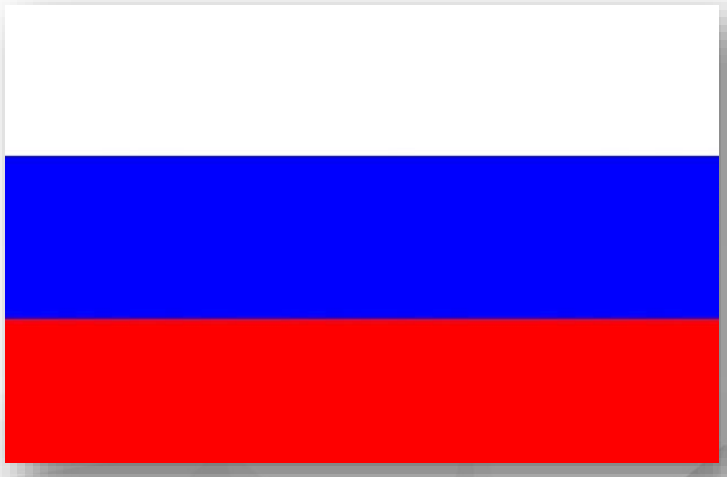


Imagen 10. País de origen de los atacantes

Boletín	2020-225
Asunto	NUEVA CAMPAÑA DE EMOTET
Emisión	20/07/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Se detectó que Emotet se está distribuyendo a través de una campaña de spam de respuesta de envíos, pagos y facturas.

De acuerdo con lo observado, Emotet envía cantidades masivas de spam, estos documentos contienen URL, de sitios maliciosos hechos con WordPress. Uno de los correos maliciosos distribuidos pretende ser de Loomis-express[.]com, esto se hace con la intención de engañar y aumentar las probabilidades de infectar la computadora de la víctima.

Los documentos Word adjuntos usan una nueva plantilla, la cual le comunica al usuario que no se puede abrir correctamente debido a que fue creada en iOS. El documento le solicita a la víctima que habilite la edición del documento, esta nueva plantilla no se ha usado en ninguna campaña anterior. Después de que el usuario haga clic en "Habilitar edición" se habilitan las macros y se ejecuta un comando de PowerShell, este último descarga y ejecuta Emotet desde los sitios maliciosos desarrollados con WordPress.

Hasta el momento se sabe que Emotet con el tiempo instala el troyano TrickBot, este es luego utilizado para obtener contraseñas, cookies, claves SSH, distribuirse a través de una red y finalmente instalar ransomware; en la computadora de la víctima.

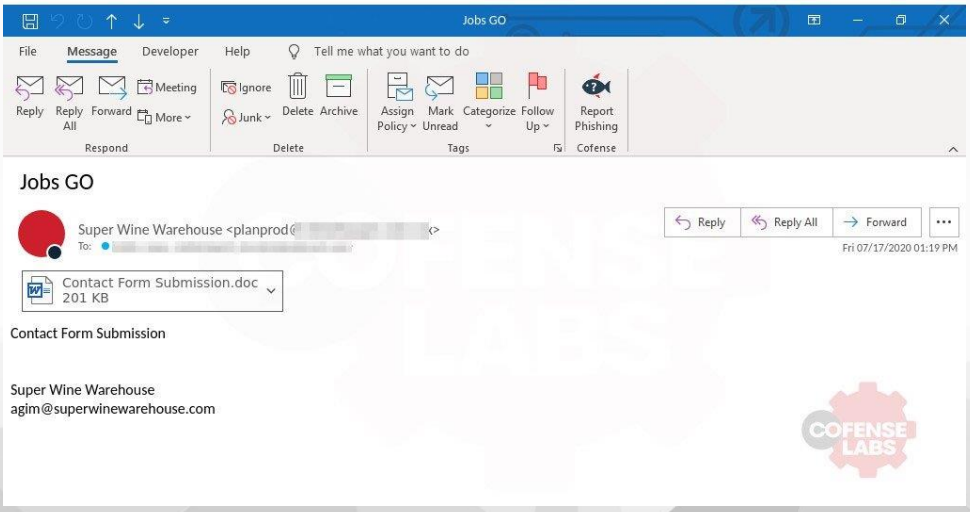


Imagen 11. Imagen de referencia del correo malicioso que es enviado por los atacantes

Boletín	2020-226
Asunto	WSRESET ES APROVECHADO POR LOS ATACANTES
Emisión	21/07/2020
CVE	No tiene
Categoría	Ataque cibernético
Severidad	Alta

Servicios Afectados

Sistema operative Windows

Descripción

Los atacantes están aprovechando wsreset.exe para eliminar archivos de forma arbitraria. Esto se debe a que wsreset.exe se ejecuta con privilegios elevados, ya que se encarga de ver la configuración de Windows, esta vulnerabilidad permite a los atacantes eliminar archivos, aunque no tengas los privilegios.

Después de analizar a wsreset, se detectó que la herramienta elimina los archivos presentes en estas carpetas, restableciendo la cache y las cookies para la aplicación de la Tienda Windows.

La técnica de explotación se basa en el concepto de "unión de carpetas" mediante enlaces simbólicos, estos son usados para indicar un acceso a un directorio o fichero que se encuentra en un lugar distinto. Si un atacante puede crear un enlace que señale desde esta ruta \InetCookies a un directorio destino elegido por el atacante, el directorio destino será el que se elimine cuando se ejecute wsreset. Esto se debe a que se ejecuta con privilegios elevados de forma predeterminada.

Para comenzar, el atacante primero elimina la carpeta \INetCookies. Los usuarios con privilegios limitados pueden eliminar la carpeta, por lo que no representa una dificultad para los atacantes. Después de esto se crea un enlace simbólico haciendo que la ubicación \INetCookies apunte a una carpeta o archivo que el atacante desea eliminar. Para crear el enlace simbólico se puede usar el comando mklink seguido del parámetro /J desde cmd o usar el comando new-item en PoweShell.

Recomendaciones

Limitar el uso de CMD y powershell a usuarios administradores autorizados.

Boletín	2020-227
Asunto	MALWARE DE ORIGEN BRASILEÑO
Emisión	21/07/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Guildma ha estado activo desde al menos 2015, inicialmente sólo se le observaba en ataques dirigidos a usuarios de la banca brasileña. El código de esta amenaza se ha actualizado constantemente, los desarrolladores implementaron nuevas funciones y ampliaron su lista de objetivos a lo largo del tiempo. Se aprovecha de herramientas legítimas, usándolas para evitar ser detectadas por soluciones de seguridad. Esta amenaza se distribuye a través de correos de phishing.

Javali ha estado activo desde noviembre de 2017, se centra en clientes de instituciones financieras ubicadas en Brasil y México. Emplea ataques de múltiples etapas y se distribuye mediante mensajes de phishing utilizando archivos adjuntos de correo electrónico o un archivo HTML que ejecuta Javascript para descargar un archivo malicioso.

Melcoz es una RAT de código abierto desarrollada por un grupo que ha estado activo en Brasil al menos desde 2018, luego se expandió a otros países como Chile y México. Esta amenaza puede obtener contraseñas de los navegadores e información del portapapeles, y de las billeteras de Bitcoin, reemplazando algunos datos de la billetera de la víctima para comprometerla.

Grandoreiro ha estado activo desde 2016, se observó que estuvo involucrada en una campaña en Brasil, México, Portugal y España. El malware está alojado en páginas de Google Sites y se propaga a través de sitios web comprometidos. Los atacantes también lo envían a través de mensajes de phishing, se observó que usa el algoritmo de generación de dominio (DGA, por sus siglas en inglés) para ocultar la dirección C2 utilizada durante el ataque.

Imagen 12. Bandera del país de origen de los malwares

Boletín	2020-228
Asunto	SERVICIOS DE GOOGLE SON APROVECHADOS POR ATACANTES
Emisión	07/07/2020
CVE	No tiene
Categoría	Ataque cibernético
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

En una campaña detectada, los ciberdelincuentes establecieron escenarios que involucra múltiples elementos legítimos para ocultar el robo de credenciales de Office 365.

Se uso el servicio de Google Drive, para alojar un documento PDF malicioso y el storage.googleapis.com para alojar páginas de phishing. El PDF se utiliza para engañar a la víctima haciéndole creer que a través de este puede ingresar a una plataforma de colaboración de SharePoint.

Luego la víctima es redireccionada a una página de phishing, la cual se encuentre publicada en Google Cloud Platform, esta le pide iniciar sesión con las credenciales de Office 365 o la identificación de una organización.

Independientemente de la opción seleccionada para iniciar sesión, se abre una ventana de inicio de sesión de Outlook para completar el presunto proceso. Es poco probable que las víctimas se puedan dar cuenta del engaño ya que las páginas se cargan de fuentes legítimas, cuando se finaliza el proceso de inicio de sesión se entrega a la víctima un PDF genuino de una compañía conocida.

Imagen 13. Imagen de referencia del producto aprovechado por los atacantes

Boletín	2020-229
Asunto	ATAQUES AUTOMATIZADOS A BASE DE DATOS
Emisión	22/07/2020
CVE	No tiene
Categoría	Ataque cibernético
Severidad	Alta

Servicios Afectados

Instancias de Elasticsearch y MongoDB

Descripción

El ataque perpetrado por Meow fue hacia una base de datos Elasticsearch que pertenece a un proveedor de VPN. En un primer momento se notificó a los dueños de la base de datos sobre lo vulnerable que este era por lo que fue asegurada. Sin embargo, poco tiempo después fue víctima de un ataque, la cual tuvo por consecuencia la eliminación de la mayoría de los registros que esta poseía.

No hay mucha información sobre el atacante. El script usado en estos ataques tiene por finalidad sobrescribir o eliminar toda la información de la base de datos de la víctima. También se detectó que este ataque también está afectando a bases de datos expuestas de MongoDB.

Se sospecha que estos ataques tienen por finalidad alertar a los administradores TI que poseen bases de datos vulnerables, esto con la finalidad de mejorar la seguridad de estas. Sin embargo, este tipo de acciones puede ocasionar que información sensible se vea afectada ocasionando daño a las organizaciones que se han visto afectadas.

Recomendación

Evitar exponer instancias de base de datos que tengan información sensible.

Imagen 14. Imagen de referencia de uno de los productos afectados

Boletín	2020-230
Asunto	LAZARUS USA EL FRAMEWORK MATA
Emisión	23/07/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

- Sistema operativo Windows
- Sistema operativo Linux
- Sistema operativo macOS

Descripción

Lazarus también conocido como HIDDEN COBRA, se detectó que este grupo utilizó MATA para comprometer computadoras de compañías de diversas industrias como las de desarrollo de software, un proveedor de servicios de Internet y una empresa de comercio electrónico.

MATA es un framework con varios componentes que incluyen un cargador, un orquestador y múltiples complementos; los cuales son usados para infectar a sistemas Windows, Linux y macOS.

Durante el ataque se puede utilizar MATA para cargar varios complementos en la memoria del sistema infectado, ejecutar comandos, manipular archivos y procesos, inyectar archivos DLL, crear archivos proxy y túneles HTTP en dispositivos Windows. Los complementos también permiten buscar nuevos objetivos que ejecutan los sistemas operativos Linux y macOS, routers, firewalls o dispositivos IoT. En el sistema operativo macOS, MATA puede cargar un módulo plugin_socks que se usa para configurar servidores proxy.

Una vez que vez que el framework MATA está implementado, los atacantes intentan encontrar bases de datos con información confidencial de clientes o negocios.

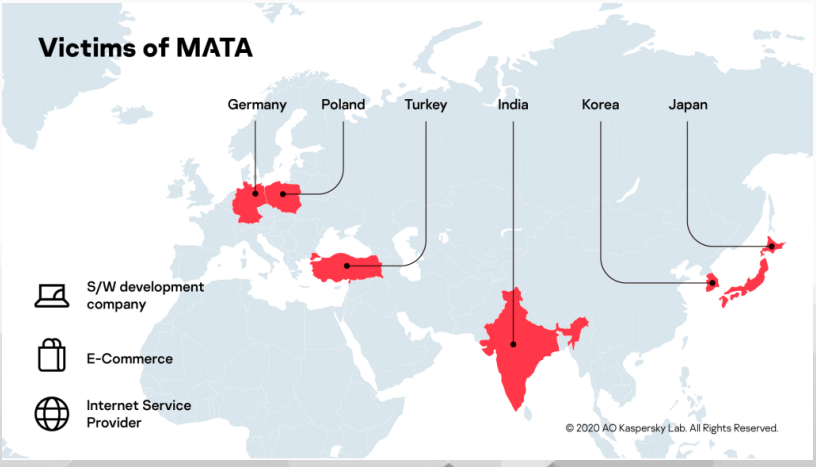


Imagen 15. Imagen de referencia del alguna de las víctimas de MATA

Boletín	2020-231
Asunto	NUEVA BOTNET PROMETEI
Emisión	24/07/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Esta nueva botnet ha sido nombrado como Prometei, se determinó que se encuentra activa desde marzo de 2020. Los ataques se basan en malware multimodular. Para infectar a las computadoras, los cibercriminales combinan distintos binarios como PsExec y WMI, exploits de SMB y credenciales robadas.

En total se detectó más de 15 componentes en los ataques de Prometei, todos gestionados por un módulo principal, el cual cifra los datos antes de enviarlos al servidor de comando y control (C2, abreviado en inglés) a través de HTTP.

Prometei roba contraseñas con una versión modificada de Mimikatz, después se usa el módulo spreader, para analizar y autenticarse en una sesión de SMB. Si al intentar iniciar sesión se falla, spreader utiliza una variante del exploit EternalBlue para distribuir e iniciar el módulo principal. El último payload utilizado en el ataque es el SearchIndexer.exe, el cual es un software de minería de código abierto.

El módulo principal de esta amenaza se propaga en la red bajo los nombres xsvc.exe y zsvc.exe, utiliza un empaquetador diferente que depende de un archivo externo para descomprimirse adecuadamente. Además, Prometei también puede comunicarse con su servidor C2 utilizando proxies TOR o I2P para obtener instrucciones y enviar los datos obtenidos.

Recomendaciones

Segmentar la red de la empresa con la finalidad de evitar que los ciberdelincuentes puedan comprometer redes críticas.

Asunto	FILTRACIÓN DE CÓDIGO FUENTE
Emisión	27/07/2020
CVE	No tiene
Categoría	Filtración de datos
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

Entre las empresas afectadas se encuentran Microsoft, Adobe, Lenovo, AMD, Qualcomm, Motorola, Hisilicon (propiedad de Huawei), Mediatek, GE Appliances, Nintendo, Roblox, Disney, Johnson Controls, entre otros.

Los códigos fueron encontrados en distintas fuentes, parte de la filtración se debe a herramientas de devops mal configuradas las cuales ofrecen acceso al código fuente. Una gran cantidad de estas filtraciones llevan el nombre de "exconfidencial" entre otras etiquetas, estas se encuentran disponibles en GitLab. Se detectó que, en algunos repositorios, además del código de la aplicación se encuentra algunas credenciales.

Se sospecha que algunas de las compañías hasta el momento no se encuentran al tanto de la filtración de su código fuente. En algunos casos, las empresas afectadas no proceden a eliminarlo.

Se informó que algunos de los proyectos fueron publicados por sus propios desarrolladores originales o se actualizaron por última vez hace mucho tiempo. Se cree que parte de la filtración de datos se debe a la mala configuración de SonarQube, la cual es una plataforma para la auditoría de código automatizada y el análisis estático para descubrir errores y vulnerabilidades de seguridad.

Imagen 16. Logo de una de las empresas afectadas

Boletín	2020-234
Asunto	WASTEDLOCKER ATACÓ A GARMIN

Emisión	29/07/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

- Sistema operativo Windows
- Garmin[.]com, Garmin Connect, FlyGarmin, Tecnología satelital inReach y Garmin Explore

Descripción

En un comunicado dado por la compañía dieron a conocer que estaban experimentando una interrupción la afectó a Garmin[.]com y Garmin Connect, lo cual afecto a sus centros de llamadas. Debido a esto la compañía no podía recibir llamadas, correos electrónicos o mensajes de chat en línea.

Si bien Garmin no lo mencionó en su alerta de interrupción, los servicios de flyGarmin utilizado por pilotos de aeronaves también se vieron afectados, incluido el sitio web de flyGarmin y la aplicación web, los servicios de Connext y las aplicaciones de piloto de Garmin.

La tecnología satelital inReach, activación y facturación del servicio, y Garmin Explore, sitio de exploración y letrero de aplicación Explore, utilizados para compartir ubicación, navegación GPS, logística y seguimiento a través de la red satelital Iridium también estuvieron inactivos durante la interrupción.

De acuerdo con lo publicado, se ha confirmado que Garmin se vio afectado por WastedLocker. Se sabe que el ataque inicio el jueves 23 de julio de 2020 en la mañana, los miembros del departamento de TI habían intentado apagar de forma remota las computadoras que se vieron afectadas. Sin embargo, no tuvieron éxito por lo que solicitaron a los empleados de la empresa apagar las computadoras a la que tenían acceso.

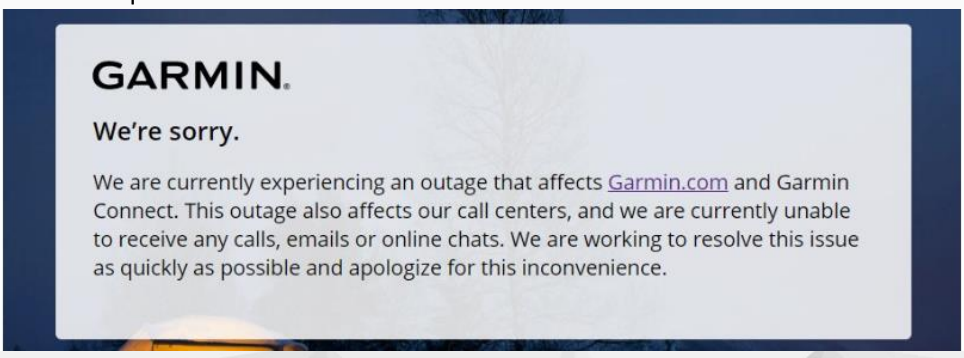


Imagen 17. Imagen de referencia relacionado al ataque

Boletín	2020-235
Asunto	NUEVO RANSOMWARE VHD

Emisión	30/07/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

Sistema operativo Windows

Descripción

VHD es una herramienta de ransomware, la cual infecta la computadora de la víctima, encripta archivos y elimina todas las carpetas de información de volumen de sistema, de esta manera los cibercriminales impiden que se pueda restaurar el sistema de manera exitosa después del ataque.

La infección del ransomware inicia obteniendo acceso a la red de la víctima, después de explotar exitosamente las redes VPN vulnerables. Cuando se implementa el backdoor, puerta trasera en español, los atacantes pueden tomar control del servidor Active Directory de sus víctimas. Lo que les permite distribuir payloads de VHD a todos los sistemas, esto se logra con la ayuda de un cargador basado en Python.

El grupo Lazarus, es identificado como Zinc por Microsoft y como HIDDEN COBRA por la Comunidad de Inteligencia de los Estados Unidos, usa el framework MATA para comprometer y desplegar payloads de VHD en compañías de distintos rubros. Este grupo es conocido por haber distribuido el ransomware WannaCry en el año 2017. Normalmente sus ataques tienen motivaciones financieras.

Imagen 18. Imagen del país de origen de los atacantes

Boletín	2020-237
Asunto	LINUX SE VE AFECTADO POR TRICKBOT
Emisión	31/07/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

Sistema operativo Linux

Descripción

TrickBot es una plataforma de malware de Windows multipropósito que utiliza diferentes módulos para realizar diversas tareas maliciosas, las cuales son: Robo de información, robo de contraseñas, infiltración del dominio de Windows y entrega de malware.

A finales de 2019 se identificó que TrickBot utiliza el framework Anchor_DNS para comunicarse con su servidor de comando y control (C2, abreviado en inglés). Se utiliza este framework cuando se ataca a objetivos que contienen información financiera valiosa.

Además de funcionar como un backdoor que puede dejar un malware en el dispositivo Linux y ejecutarlo, también contiene un ejecutable de TrickBot para Windows incorporado. El binario incrustado es una versión ligera de TrickBot, la cual se utiliza para infectar computadoras con el sistema operativo Windows que se encuentran en la misma red.

Para infectar computadoras Windows, Anchor_Linux copia el malware TrickBot incorporado a los hosts Windows de la red utilizando SMB y $IPC. Cuando se tiene éxito en esta tarea, se configura a la computadora afectada como un servicio utilizando el protocolo remoto Service Control Manager y SMB SVCCTL. Esta nueva versión, permite a los atacantes infectar primero dispositivos que utilizan Linux para luego infectar computadoras que ejecutan Windows.

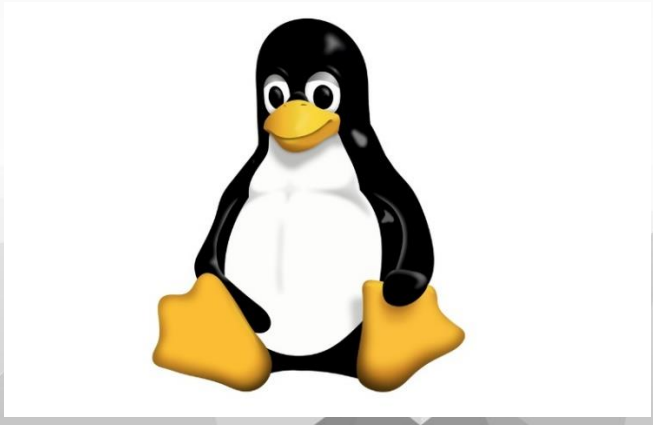


Imagen 19. Imagen de referencia del sistema operativo afectado

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 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.