SECURESOFT CORPORATION
e-Secure Consulting Group

# Reporte Semanal de Ciberinteligencia Securesoft

**Fecha:**

**14 Julio 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

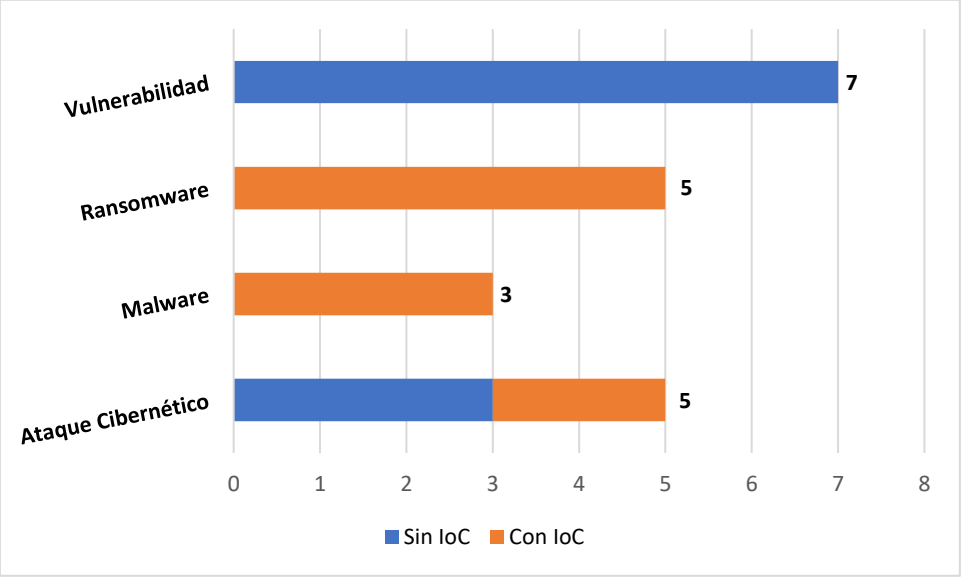
Este documento muestra el resumen, la fecha de publicación, CVE asociado y servicios afectados de vulnerabilidades y amenazas que se han hecho públicas en el transcurso del 25 de junio hasta el 13 de julio del 2020.

# 3. Resumen

En el presente informe se exponen 20 análisis de vulnerabilidad y amenazas, de las cuales 4 han sido consideradas como críticas mientras que 16 como altas.

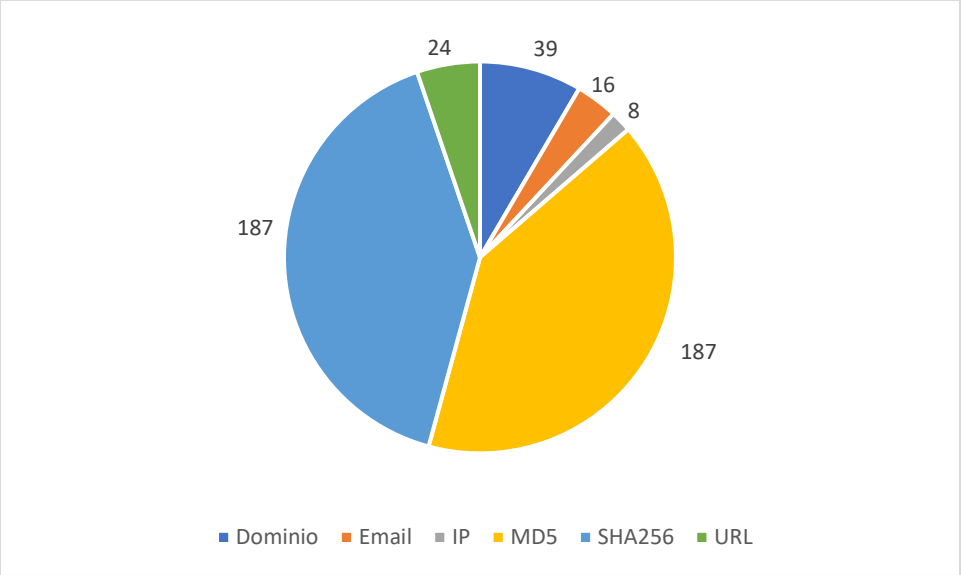
## Análisis por tipología

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 461 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-2020-5902 está siendo explotada de manera constante. Por lo que sugiere que lea el Boletín 2020-209, en este informe se cuenta con una breve descripción sin embargo recomendamos ver todo el contenido del boletín. Durante los últimos días se ha registrado mucha actividad que se relacionan con la vulnerabilidad.

- Otra vulnerabilidad que es tendencias es la CVE-2020-2021, para más información se sugiere leer el resumen que se encuentra en este informe y el Boletín 2020-204. Esta es una vulnerabilidad crítica. Durante los últimos días se ha registrado muchas actividades que se relacionan con la vulnerabilidad.

## Actividades maliciosas asociadas a ransomware

- Durante las últimas se ha detectado que el nuevo ransomware Wastedlocker, asociado al grupo de cibercriminales Evil Corp, ha estado muy activo. Sus principales víctimas son usuarios de Windows. Para más información leer el resumen de esta amenaza que se encuentra en este informe o ver el Boletín 2020-199. Durante los últimos días se ha registrado muchas actividades maliciosas relacionados a este ransomware.

# 4. Detalles

## Vulnerabilidades

| | |
|---|---|
| Boletín | 2020-205 |
| Asunto | ACTUALIZACIÓN DE WINDOWS 10 Y WINDOWS SERVER |
| Emisión | 01/07/2020 |
| CVE | CVE-2020-1425 y CVE-2020-1457, |
| Categoría | Vulnerabilidad |
| Severidad | Crítica |

## Servicios Afectados

• Windows 10 versiones 1709, 1803, 1809, 1903, 1909 y 2004

• Windows Server versiones 1709, 1803, 1903, 1909, 2004 y 2019

**Descripción**

Las dos vulnerabilidades han sido asignados a los CVE-2020-1425 y CVE-2020-1457, donde la primera tiene una severidad crítica. En ambas la vulnerabilidad es de ejecución remota de código, esto se debe a la forma en la que la Biblioteca códecs de Microsoft Windows maneja los objetos en memoria.

La explotación exitosa de la vulnerabilidad CVE-2020-1425, permite a un atacante obtener información para comprometer aún más el sistema del usuario. Mientras que la vulnerabilidad CVE-2020-1457, permite la ejecución de código de manera arbitraria.

La explotación de estas vulnerabilidades requiere de un programa para procesar un archivo de imagen especialmente diseñado.

De acuerdo con lo publicado por Microsoft los clientes afectados recibirán la actualización de estas vulnerabilidades de manera automática a través de Microsoft Store.

**Actualización o Mitigación**

Aplicar las actualizaciones para estas vulnerabilidades a través de Microsoft Store. Para ello haga clic aquí.

| | |
|---|---|
| Boletín | 2020-206 |
| Asunto | CISCO PUBLICA ACTUALIZACIÓN DE SEGURIDAD |
| Emisión | 02/07/2020 |
| CVE | CVE-2020-3297 |
| Categoría | Vulnerabilidad |
| Severidad | Alta |

## Servicios Afectados

- 250 Series Smart Switches
- 350 Series Managed Switches
- 350X y 550X Series Stackable Managed Switches
- Small Business 200 Series Smart Switches
- Small Business 300 Series Managed Switches
- Small Business 500 Series Stackable Managed Switches

**Descripción**

Cisco System publicó una advertencia de una vulnerabilidad de alta gravedad, que afecta a más de media docena de switches. Esta permite a los atacantes remotos no autenticados acceder a las interfaces de administración de los dispositivos vulnerable con privilegios administrativos.

Hasta el momento Cisco ha comunicado que no se tiene conocimiento de la explotación activa de esta vulnerabilidad.

La vulnerabilidad ha sido asignada al CVE-2020-3297, posee una severidad alta, tiene un puntaje de 8.1 de 10.0 en la escala de CVSS. Esta se debe al uso de una generación de entropía débil para los valores de los identificadores de sesión. Aprovechándose de esto un atacante puede eludir la autenticación y obtener los privilegios de la cuenta de sesión en el dispositivo vulnerable. Si la víctima es un usuario administrador, el atacante puede obtener privilegios administrativos en el dispositivo.

**Actualización o Mitigación**

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


**Imagen 1. Imagen de referencia de la marca de los productos afectados**

| | |
|---|---|
| Boletín | 2020-207 |
| Asunto | VULNERABILIDADES EN APACHE GUACAMOLE |
| Emisión | 02/07/2020 |
| CVE | CVE-2020-9497 y CVE-2020-9498 |
| Categoría | Vulnerabilidad |
| Severidad | Alta |

## Servicios Afectados

Apache Guacamole

**Descripción**

Las vulnerabilidades CVE-2020-9497 y CVE-2020-9498 permiten a un atacante u otra amenaza comprometer con éxito una computadora dentro de una organización, esto permite interceptar y controlar las sesiones conectadas al servidor Guacamole, incluso tomar el control total del servidor.

A continuación, la relación de vulnerabilidades:

• CVE-2020-9497: Permite la divulgación de información que se encuentra dentro de la memoria del proceso guacd.

• CVE-2020-9498: Permite posiblemente ejecución de código arbitrario con los privilegios del proceso guacd.

• Lecturas fuera de límites en FreeRDP: Permite aprovecharse de una falla de diseño en FreeRDP.

Mediante el uso de las vulnerabilidades CVE-2020-9497 y CVE-2020-9498, una computadora corporativa maliciosa puede tomar el control del proceso guacd cuando un usuario remoto solicita conectarse a su computadora.

**Actualización o Mitigación**

Aplicar las actualizaciones proporcionadas por Apache Guacamole. Para ello haga clic aquí.

| | |
|---|---|
| Boletín | 2020-209 |
| Asunto | ACTUALIZACIÓN DE SEGURIDAD EN DISPOSITIVOS BIG-IP |
| Emisión | 06/07/2020 |
| CVE | CVE-2020-5902 |
| Categoría | Vulnerabilidad |
| Severidad | Crítica |

## Servicios Afectados

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM), versiones:

- 15.1.0 y 15.0.0
- desde 14.1.0 hasta 14.1.2
- desde 13.1.0 hasta 13.1.3
- desde 12.1.0 hasta 12.1.5
- desde 11.6.1 hasta 11.6.5

**Descripción**

BIG-IP es un dispositivo de red multipropósito fabricado por F5 Networks. Estos pueden configurarse para funcionar como sistemas de modelado de tráfico, balanceadores de carga, firewalls, puertas de acceso, limitadores de velocidad o middleware SSL. Además, son utilizados en redes gubernamentales, redes de servicios de internet, centros de datos de computación en la nube y en redes corporativas.

Debido a ello, es crítico que se haya descubierto la vulnerabilidad asignada al CVE-2020-5902, la cual permite a los atacantes tomar el control total sobre los dispositivos vulnerables conectados a Internet.

De acuerdo con nuestras fuentes de información, se han publicado diversos exploits de Pruebas de Concepto (PoC, por sus siglas en inglés), las cuales demuestran lo fácil que es explotar está vulnerabilidad. Uno de los exploits publicado permite acceder a las credenciales almacenadas o ver los archivos de configuración de los dispositivos vulnerables.

**Actualización o Mitigación**

Aplicar las actualizaciones proporcionadas por Apache Guacamole. Para ello haga clic aquí.

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

| | |
|---|---|
| Boletín | 2020-212 |
| Asunto | CITRIX PUBLICA ACTUALIZACIONES DE SEGURIDAD |
| Emisión | 08/07/2020 |
| CVE | Varios |
| Categoría | Vulnerabilidad |
| Severidad | Alta |

## Servicios Afectados

- Citrix ADC
- Citrix Gateway
- Citrix SDWAN WANOP
- Citrix Gateway Plug-in para Linux

**Descripción**

Citrix ha publicó actualizaciones para 11 vulnerabilidades de alta gravedad para sus productos. La explotación exitosa de estas vulnerabilidades permite denegación de servicio (DoS, por sus siglas en inglés), robo de información, escalamiento de privilegios, entre otras.

De acuerdo con lo publicado por Citrix, no se tiene conocimiento de ninguna explotación activa de estas vulnerabilidades por parte de los atacantes. También publicó que 5 de las 11 vulnerabilidades tienen barreras de seguridad que impiden su explotación, entre estas una reduce el riesgo de un DoS.

**Actualización o Mitigación**

Se recomienda ver el contenido completo de esta noticia, para ello haga clic en el boletín que está en la tabla superior de esta página. En ese enlace encontrará mayor detalle de todas las vulnerabilidades junto con la actualización de cada vulnerabilidad.

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

| | |
|---|---|
| Boletín | 2020-213 |
| Asunto | ACTUALIZACIONES DE PAN-OS |
| Emisión | 09/07/2020 |
| CVE | CVE-2020-2030 y CVE-2020-2034 |
| Categoría | Vulnerabilidad |
| Severidad | Alta |

## Servicios Afectados

Pan-OS versiones anteriores a 9.1.3, 9.0.9 y 8.1.15, y todas las versiones 8.0.* y 7.1.*

**Descripción**

De acuerdo con la escala de puntaje CVSS, la vulnerabilidad más grave es la CVE-2020-2034, que afecta a GlobalProtect y permite que un atacante no autenticado con acceso al sistema objetivo ejecute comandos arbitrarios del sistema operativo con permisos de root. Esta es explotable solo si la función GlobalProtect está habilitada, por ello un atacante debe poseer cierto nivel de información específica sobre la configuración del firewall o realizar ataques de fuerza de bruta para explotar la vulnerabilidad.

Por otro lado, la vulnerabilidad de severidad alta asignada al CVE-2020-2030, permite que un atacante con acceso a la interfaz de administración PAN-OS pueda ejecutar comandos de manera arbitraria en el sistema operativo con privilegios de root.

Palo Alto Networks anunció que ambas vulnerabilidades fueron descubiertas dentro de la empresa, y no existe evidencia de explotación por parte de los atacantes. De acuerdo con el fabricante las vulnerabilidades anteriormente mencionadas no son tan graves como la CVE-2020-2021, la cual tiene una severidad crítica, esta permite la omisión de autenticación, para más información ver Boletín 2020-204.

**Actualización o Mitigación**

Aplicar las actualizaciones proporcionadas por Palo Alto Networks de acuerdo con la vulnerabilidad. Para la vulnerabilidad CVE-2020-2030 haga clic aquí y para la CVE-2020-2030 haga clic aquí.

| | |
|---|---|
| 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.

Sin embargo, 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 proporcionadas por Zoom. Para ello haga clic aquí.

**Imagen 4. Imagen de referencia del producto afectado**

## Amenazas

| | |
|---|---|
| Boletín | 2020-198 |
| Asunto | NUEVO ATAQUE DE REVIL RANSOMWARE |
| Emisión | 24/06/2020 |
| CVE | No tiene |
| Categoría | Ransomware |
| Severidad | Alta |

## Servicios Afectados

Sistema operativo Windows

**Descripción**

En la presente campaña se observó, que los atacantes detrás de REvil han utilizado herramientas de prueba de penetración Cobalt Strike para implementar payloads del ransomware en las redes de sus víctimas.

Los atacantes detrás de REvil hicieron todo lo posible para evitar ser detectados después de comprometer la red de la víctima, usando una infraestructura alojada en servicios legítimos como Pastebin (almacenamiento de payload), y Amazon CloudFront (servidor de comando y control). Por otro lado, también deshabilitaron el software de seguridad y obtuvieron credenciales que luego usaron para agregar cuentas falsas.

Para los atacantes las empresas de servicios y alimentos eran sus principales objetivos, ya que al ser grandes creen que estas organizaciones pagaran el rescate para tener acceso a la información que se vio afectada.

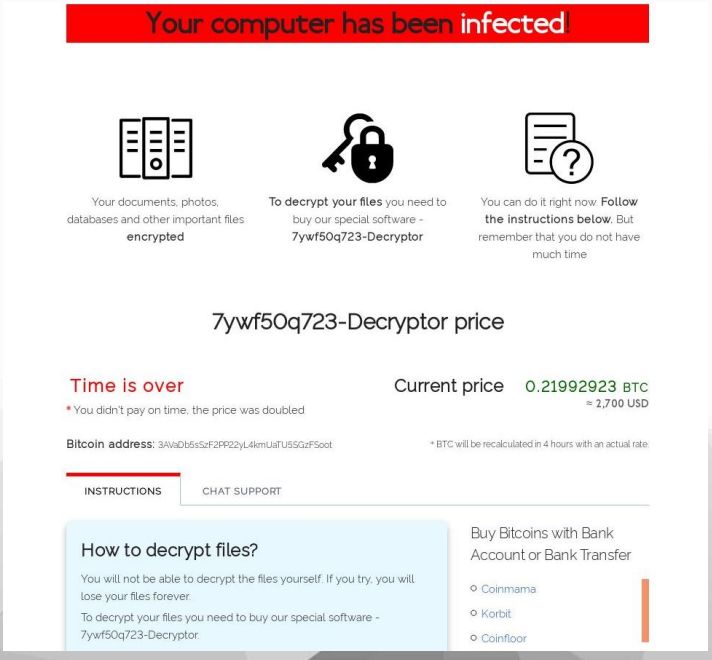


**Imagen 5. Imagen de referencia de una de una página relacionada a REvil**

| | |
|---|---|
| Boletín | 2020-199 |
| Asunto | WASTEDLOCKER RANSOMWARE |
| Emisión | 24/06/2020 |
| CVE | No tiene |
| Categoría | Ransomware |
| Severidad | Alta |

## Servicios Afectados

Sistema operativo Windows

**Descripción**

Evil Corp ha empezado a distribuir una nueva variante de ransomware llamada WastedLocker, la cual es usada en ataques contra empresas. En esta campaña para distribuir el ransomware, los atacantes están que insertan código malicioso que muestran alertas de actualización de software falsas.

Cuando se inicia, el ransomware WastedLocker elegirá un archivo EXE o DLL aleatorio en C:\Windows\System32 y usará el nombre de ese archivo para crear uno nuevo sin una extensión en la carpeta %AppData%. Adjunto a ese archivo hay una secuencia de datos alternativa llamada 'bin', que luego se ejecutará.

Una vez que se ejecuta el ransomware, este intentará cifrar todas las unidades de la computadora, omitiendo archivos en carpetas específicas o que contengan ciertas extensiones. Esto evidencia un ataque dirigido, debido a ello se deduce que el ransomware está diseñado para atacar a una empresa.

Al momento de encriptar los archivos el ransomware agregará una extensión, la cual está formada por las iniciales de la empresa afectada, seguida de la palabra "wasted". La nota de rescate tendrá casi el mismo formato, ha esta se le agrega "_info" en el nombre del archivo cifrado.

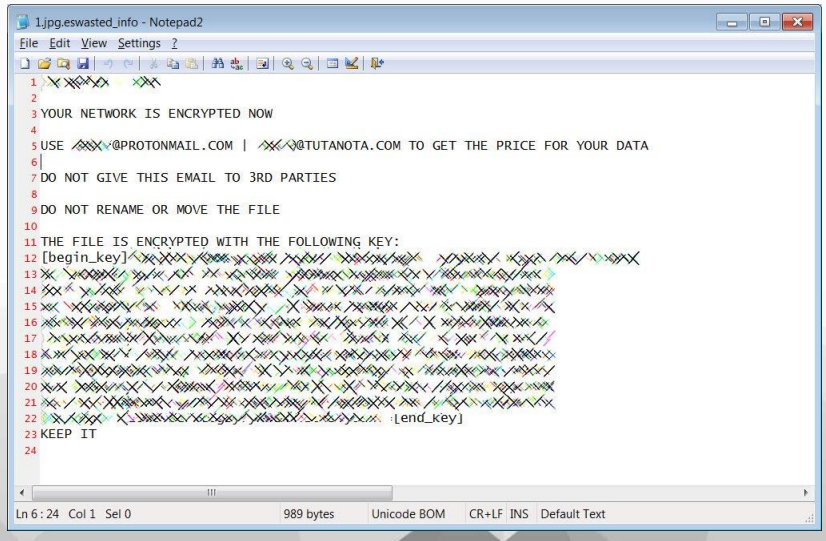


**Imagen 6. Imagen de referencia de una de una página relacionada a WastedLocker**

| | |
|---|---|
| Boletín | 2020-200 |
| Asunto | NUEVO MALWARE LUCIFER |
| Emisión | 25/06/2020 |
| CVE | Varios |
| Categoría | Malware |
| Severidad | Crítica |

## Servicios Afectados

Sistema operativo Windows

**Descripción**

De acuerdo con lo informado al inicio se creía que el malware era utilizado solo para minar criptomonedas, pero luego se descubrió que posee un componente de DDoS, así como un mecanismo de propagación automática al aprovecharse de múltiples vulnerabilidades y de ataques de fuerza bruta.

La propagación de esta amenaza se debe a que posee exploits para las siguientes vulnerabilidades: CVE-2014-6287, CVE-2017-0144, CVE-2017-0145, CVE-2017-8464, CVE-2017-9791, CVE-2017-10271, CVE-2018-7600, CVE-2018-20062, CVE-2018-1000861 y CVE-2019-9081. Una vez que los atacantes consiguen explotar alguna de estas vulnerabilidades pueden ejecutar comandos de manera arbitraria en sus objetivos.

Para el ataque de fuerza bruta, el malware usa un diccionario de 300 contraseñas y solo siete nombres de usuario, los cuales son: sa, SA, su, kisadmin, SQLDebugger, mssql, y Chred1433.

Además de todo lo anterior mencionado, Lucifer busca computadoras con los puertos TCP 135 (RPC) y 1433 (MSSQL) abiertos. Una vez consigue afectar la computadora, realiza una copia de este.

La última versión de este malware viene con protección anti-análisis y verifica el nombre del usuario y la computadora de la máquina infectada antes de continuar.

**Imagen 7. Imagen de referencia de la amenaza**

| | |
|---|---|
| Boletín | 2020-201 |
| Asunto | SERVIDORES EXCHANGE BAJO ATAQUE |
| Emisión | 26/06/2020 |
| CVE | CVE-2020-0688 |
| Categoría | Vulnerabilidad |
| Severidad | Alta |

## Servicios Afectados

Microsoft Exchange Server 2010 Service Pack 3, 2013, 2016 y 2019

**Descripción**

Exchange ha sido atacado por varios cibercriminales, los cuales son respaldados por distintos gobiernos del mundo. Estos se han estado aprovechando de la vulnerabilidad asignada al CVE-2020-0688, la cual fue corregida en febrero de 2020. Esta vulnerabilidad fue abordada en nuestro Boletín 2020-077.

La vulnerabilidad mencionada anteriormente implica que los servidores de correo electrónico de Exchange han estado utilizando claves criptográficas idénticas para el backend del panel de control, lo que permite a los atacantes remotos ejecutar malware y tomar el control del servidor, para luego tener acceso a los correos electrónicos de su víctima.

Normalmente los servidores de Exchange se ven comprometidos a través de ataques de phishing o vulnerabilidades de escritorio, desde allí los atacantes empiezan a moverse por la red de la organización hasta llegar al servidor Exchange.

En la mayoría de los ataques detectados contra los servidores de Exchange, se detectó que los atacantes pretenden implementar una web shell. Después de implementar esto, los atacantes exploraron el dominio de destino, en la cual se encontró un servidor mal configurado. En estos se agregan nuevas cuentas a grupos con altos privilegios como administradores, usuarios de escritorio remoto y administradores empresariales.

Esto le da a los atacantes acceso sin restricciones a cualquier usuario o grupo de la organización. Posteriormente, las credenciales de estas cuentas son utilizadas en herramientas nativas de Windows para volcar la memoria del Servicio de subsistema de autoridad de seguridad local (LSASS, por sus siglas en inglés), servicio que permite manejar la autenticación en dominios de Active Directory.

**Actualización o Mitigación**

Aplicar las actualizaciones recomendadas por Microsoft. Para ello haga clic aquí.

| | |
|---|---|
| Boletín | 2020-202 |
| Asunto | NUEVO RANSOMWARE RANSOM X |
| Emisión | 30/06/2020 |
| CVE | No tiene |
| Categoría | Ransomware |
| Severidad | Alta |

## Servicios Afectados

Sistema operativo Windows

**Descripción**

Según lo observado Ransom X termina con 289 procesos relacionados a software de seguridad, servidores de bases de datos, software MSP, herramientas de acceso remoto y servidores de correo. El ransomware también omitirá varias carpetas del sistema de Windows y cualquier archivo que coincida con las siguientes extensiones: .ani, .cab, .cpl, .cur, .diagcab, .diagpkg, .dll, .drv, .hlp, .icl, .icns, .ico, .iso, .ics, .lnk, .idx, .mod, .mpa, .msc, .msp, .msstyles, .msu, .nomedia, .ocx, .prf, .rtp, .scr, .shs, .spl, .sys, .theme, .themepack, .exe, .bat, .cmd, .url y .mui.

Se sospecha que las siguientes carpetas crypt_detect, cryptolocker y ransomware, son utilizadas para almacenar el ejecutable del ransomware y otras herramientas utilizadas por los atacantes, ya que estas carpetas son omitidas al momento de realizar la encriptación de los archivos en la computadora de la víctima. De esta manera los atacantes encriptan una computadora mientras también atacan a otras computadoras en la red sin temor a que sus herramientas se encripten.

Ransom X ejecuta una serie de comandos a lo largo del proceso de cifrado que permiten lo siguiente:

- Borrar registros de eventos de Windows
- Eliminar diarios NTFS
- Deshabilitar Restaurar sistema
- Deshabilitar el entorno de recuperación de Windows
- Eliminar catálogos de copia de seguridad de Windows

Una vez que el ransomware se ejecuta comienza a encriptar todos los datos en la computadora de la víctima y agrega una extensión personalizada asociada a la víctima a cada archivo encriptado.

| | |
|---|---|
| Boletín | 2020-203 |
| Asunto | INCREMENTO DE ATAQUES CONTRA SERVICIOS RDP |
| Emisión | 30/06/2020 |
| CVE | No tiene |
| Categoría | Ataque cibernético |
| Severidad | Alta |

## Servicios Afectados

Servicios RDP de Windows

**Descripción**

Las computadoras personales se han convertido en el principal instrumento para conectarse al entorno de trabajo a través de los RDP, siendo el protocolo de Windows la más usada.

Esto está siendo aprovechado por los atacantes para obtener acceso a la red de las compañías, escalando en privilegios e instalando malware dentro de ellas.

Entre diciembre de 2019 y hasta febrero de 2020, el número de ataques contra los servicios RDP fueron entre 40,000 y 70,000 diarios. Sin embargo, desde febrero aumentó hasta 80,000 ataques diarios. Desde entonces, esta cantidad ha ido aumentando hasta llegar a los 100,000 en abril y mayo de 2020, lo cual coincide cuando la mayoría de los países habían declarado la emergencia nacional debido al Covid-19.

La mayoría de los ataques registrados entre enero y mayo de 2020 se originaron desde los países de Estados Unidos, China, Rusia, Alemania y Francia. Estos tenían en su mayoría como objetivo IP's específicas que se encontraban en Rusia, Alemania, Brasil y Hungría.

De acuerdo con lo publicado después del compromiso del RDP, los atacantes infectan las computadoras de las víctimas con ransomware. Esto tiene por objetivo exigir un rescate por la información cifrada. También se ha observado que los cryptojacking y los backdoors son otras amenazas que los atacantes tratan de implementar en las computadoras infectadas.

**Actualización o Mitigación**

• Evaluar aplicar un factor de doble autenticación para el uso del servicio RDP.

• Evitar exponer servicios RDP a Internet y verificar que se encuentren bloqueados a nivel de perímetro.

| | |
|---|---|
| Boletín | 2020-204 |
| Asunto | ATAQUES DE CIBERESPIONAJE EN EUROPA Y ORIENTE MEDIO |
| Emisión | 01/07/2020 |
| CVE | CVE-2020-2021 |
| Categoría | Ataque cibernético |
| Severidad | Crítica |

## Servicios Afectados

• Todas las versiones de PAN-OS 8.0 (EOL)

• PAN-OS versiones de 8.1 hasta 8.1.15, de 9.0 hasta 9.0.9 y de 9.1 hasta 9.1.3

**Descripción**

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés) de los Estados Unidos (EE.UU., por sus siglas en inglés) ha publicado que los atacantes están que explotan una vulnerabilidad crítica de una serie de firewalls de Palo Alto Networks, y dispositivos VPN empresariales, lo que les permite acceder a dispositivos sin autenticación.

La vulnerabilidad CVE-2020-2021, permite la omisión de autenticación, debido a esto los atacantes pueden acceder al dispositivo sin tener que proporcionar ninguna credencial. Sin embargo, la vulnerabilidad solo puede ser explotada cuando la autenticación SAML está habilitada y la opción "Validar certificado de proveedor de identidad" está deshabilitada.

Esta combinación permite que un atacante no autenticado acceda a recursos protegidos a través de una verificación incorrecta de firmas en la autenticación SAML PAN-OS. Para poder explotar la vulnerabilidad es necesario que el atacante tenga acceso a la red en la que se encuentra el servidor vulnerable.

**Actualización o Mitigación**

Aplicar las actualizaciones recomendadas por Palo Alto Networks. Para ello haga clic aquí.

**Imagen 8. Imagen de referencia del producto afectado**

| | |
|---|---|
| Boletín | 2020-208 |
| Asunto | EKANS ATACA SISTEMAS DE CONTROL INDUSTRIAL |
| Emisión | 03/07/2020 |
| CVE | No tiene |
| Categoría | Ransomware |
| Severidad | Alta |

## Servicios Afectados

Sistema operative Windows

**Descripción**

De acuerdo con lo observado durante el presente año, 2020. Cuando este ataca sistemas críticos, como servicios públicos y de fabricación, puede interrumpir el correcto funcionamiento de estos, por lo que las víctimas se pueden sentir muy presionados a pagar el rescate. Normalmente este ransomware se utiliza en campañas contra Sistemas de Control Industrial (ICS, por sus siglas en inglés).

Se analizaron dos muestras, una corresponde al mes de mayo y la otra a junio, ambas son del año 2020. Las muestras analizadas, evidencian que Ekans está escrito en GO, lenguaje de programación utilizado por los atacantes para el desarrollo de malware, ya que es fácil de compilar para trabajar en diferentes sistemas operativos.

El malware intentará confirmar su objetivo resolviendo el dominio y comparando esta información con las listas de IP. Una vez que se adquiere un objetivo, buscará controladores de dominio.

Una vez que infecta a una computadora vulnerable, este empieza a cifrar archivos y dejar una nota de rescate, la cual exige un pago a cambio de obtener una clave que permite el descifrado de los archivos afectados. Sin embargo, la muestra de junio es capaz de causar estragos en un entorno industrial, incluida la característica de desactivar los firewalls de las computadoras afectadas.

**Imagen 9. Imagen de referencia de la amenaza**

| | |
|---|---|
| Boletín | 2020-210 |
| Asunto | SE REGISTRAN ATAQUES DE TA505 EN LATINOAMÉRICA |
| Emisión | 06/07/2020 |
| CVE | No tiene |
| Categoría | Ataque cibernético |
| Severidad | Alta |

## Servicios Afectados

Sistema operativo Windows

**Descripción**

Recientemente se ha detectado que el grupo TA505 está que distribuye malware vía spear-phishing, desde cuentas comprometidas, las cuales pretenden hacerse pasar por remitentes conocidos. El correo enviado contiene un html adjunto, este redirecciona a la víctima a un dominio controlado por TA505, desde el cual se descarga un excel.

Detalles para considerar de la campaña:

• El correo y plantilla de excel está escrito en español.

• El archivo adjunto en los correos contiene tags HTML aleatorios y a través de los tags data u object, incrusta un sitio, desde el cual se descarga el excel malicioso.

• Al abrir el excel se instala GET2, el cual envía información al Servidos de Comando y Control (C2, abreviado en inglés) e inicia con las descarga e instalación de SDBBot.

• Luego de recopilar información y verificar el entorno, se despliega CLOP ransomware en la red corporativa.

• Los correos tienen como asunto: Factura Electronica, Orden de Compra y Cheques.

• Las urls que se encuentran en los archivos html, se encuentran alojadas en servidores comprometidos, un servidor puede tener muchas URL's de redirección.

Se sospecha que TA505 recopiló más de dos millones de correos y cientos de cuentas SMTP vulnerables, las cuales están usando para atacar.

| | |
|---|---|
| Boletín | 2020-211 |
| Asunto | SKIMMING EN TIENDAS EN LÍNEA ESTADOUNIDENSES ASOCIADO A NORCOREANOS |
| Emisión | 07/07/2020 |
| CVE | No tiene |
| Categoría | Ataque cibernético |
| Severidad | Alta |

## Servicios Afectados

Tiendas en línea

**Descripción**

Se sospecha que Lazarus utilizó sitios web legítimos para obtener los datos de las tarjetas de crédito de sus víctimas. El robo de la información de tarjetas de crédito de clientes de tiendas en línea se ha incrementado durante los últimos años. Este tipo de ataques se conocen como MageCart, en este ataque los cibercriminales crean scripts maliciosos (skimmers web) que se encargan de obtener la información confidencial de la página de pago.

Se detectó que los skimmers de esta campaña se cargaban desde dominios que eran utilizados en ataques de spear-phishing por parte del grupo Lazarus. Alguna de las víctimas son Claire's, Wongs Jewelers, Focus Camera, Paper Source, Jit Truck Parts, CBD Armor, Microbattery, Realchem, entre otras tiendas.

Se identificó que los atacantes han utilizado múltiples dominios en distintas fechas, para realizar sus ataques. En la campaña del 2019, el nodo de filtración era el sitio web de Lux Model Agency. Sin embargo, el script malicioso que fue usado para infectar la página desapareció en 24 horas y volvió a aparecer en la misma tienda después de una semana.

En otra campaña entre febrero y marzo de 2020, los cibercriminales registraron dominios que podían confundirse fácilmente con el nombre de las marcas Claire, Focus Camera y PaperSource. Luego se descubrió que los sitios de las tres marcas, anteriormente mencionadas, habían sido comprometidos con skimmers, mientras que los dominios falsos fueron usados para cargar script y recopilar los datos obtenidos.

**Imagen 10. Imagen de referencia del país de origen del grupo de atacante**

| | |
|---|---|
| Boletín | 2020-214 |
| Asunto | EVILNUM UTILIZA PROVEEDOR DE MALWARE COMO SERVICIO |
| 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 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). La mayoría de los servidores solo se identifican por una dirección IP.

Se detectó que Evilnum utiliza ampliamente las herramientas de Golden Chickens. Entre los payloads usados por estos se encuentran TerraStealer, TerraTV y TerraPreter. 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.

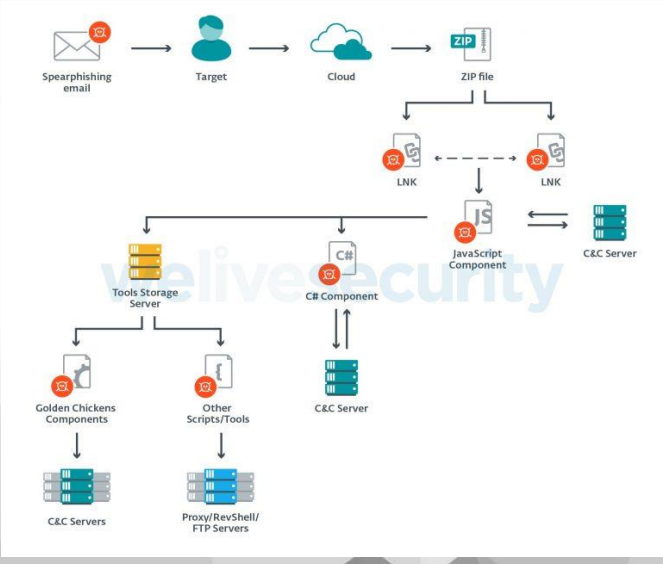



**Imagen 11. Componentes de Evilnum**

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

## Servicios Afectados

Sistema operativo Windows

**Descripción**

Al igual que otros ransomware los atacantes detrás de este, primero comprometen las redes de su víctima para luego propagarse lateralmente hasta obtener credenciales de administrador de dominio. Una vez que se logra esto, se procede a implementar el ransomware.

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. 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. El ransomware borra las copias de seguridad de Shadow Volumen y comenzará a cifrar la computadora.

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.

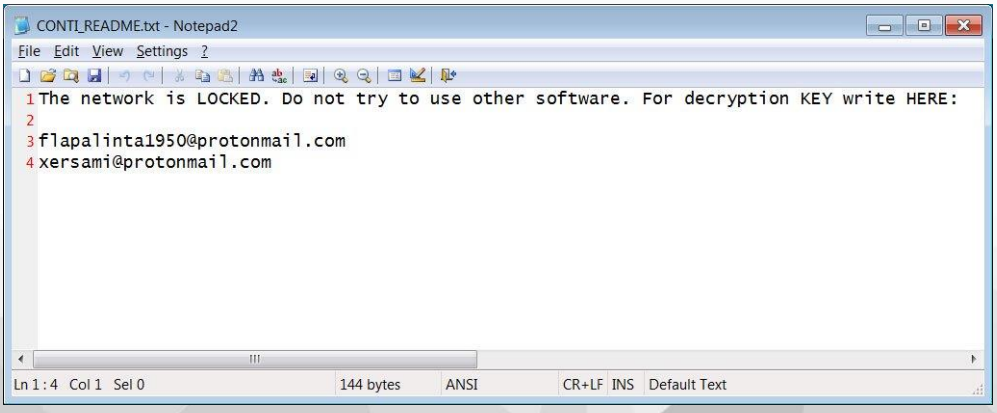



**Imagen 12. Imagen de referencia de la nota que muestra el ransomware**

| | |
|---|---|
| Boletín | 2020-217 |
| Asunto | TRICKBOT ADVIERTE POR ERROR A SUS VÍCTIMAS |
| Emisión | 13/07/2020 |
| CVE | No tiene |
| Categoría | Malware |
| 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.

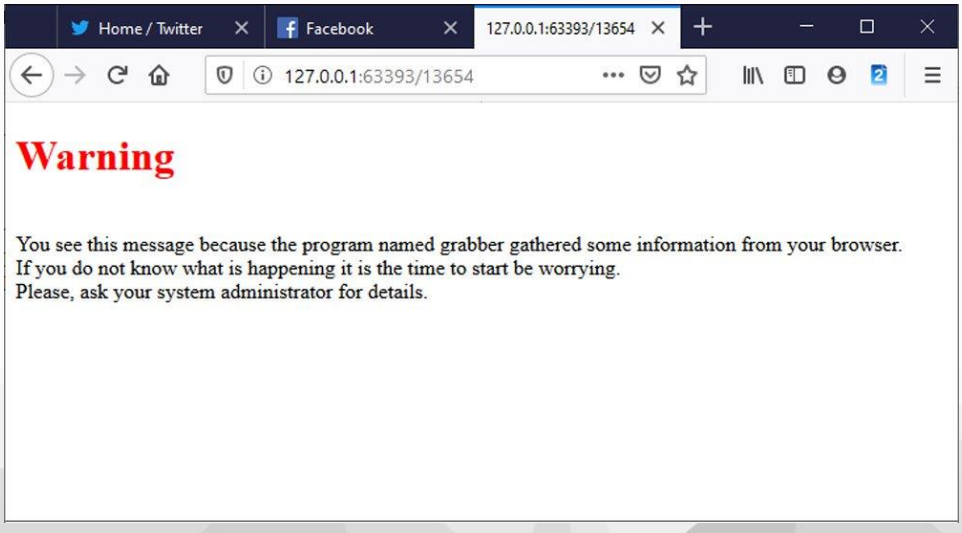



**Imagen 13. Imagen de referencia de la advertencia que muestra el malware**

# 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 IOCs 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.