SECURESOFT CORPORATION
e-Secure Consulting Group

Reporte Quincenal de Ciberinteligencia Securesoft

Fecha:

12 mayo de 2021

El presente documento contiene información para la comunidad de ciberseguridad.

Equipo de Ciberinteligencia

CIB-FOR-2021-009

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

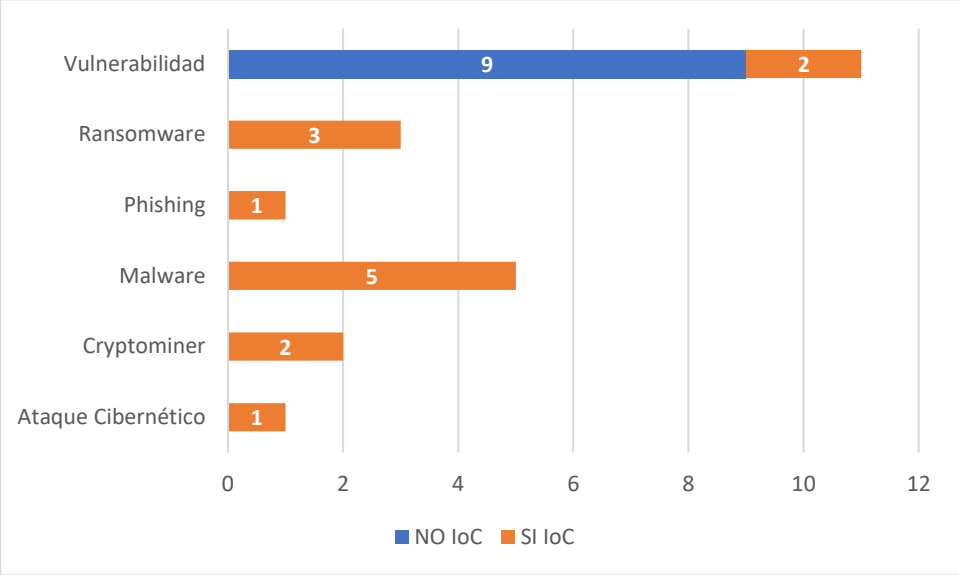
Este documento muestra el resumen, la fecha de publicación, CVE asociado y servicios afectados de vulnerabilidades y amenazas que se han hecho públicas en el transcurso del 16 de abril hasta el 30 de abril del 2021.

3. Resumen

En el presente informe se exponen 23 análisis de vulnerabilidad y amenazas, de las cuales 8 tiene severidad crítica, 9 tienen severidad alta y 6 severidad media.

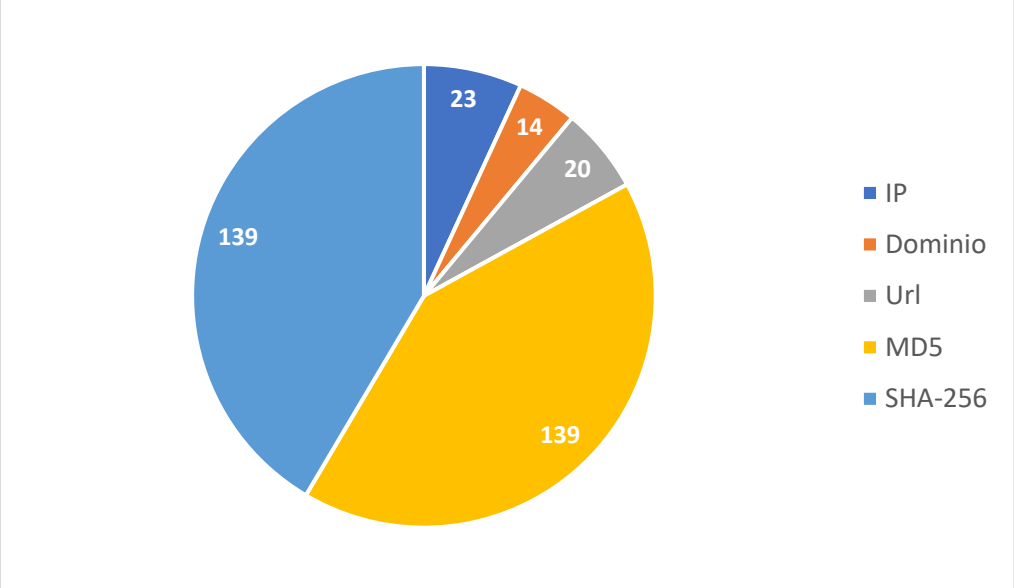
Amenazas analizadas por tipología

En las investigaciones elaboradas para el presente informe se trataron vulnerabilidad, ransomware, phishing, malware, cryptominer y ataque cibernético. 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 335 IoCs entre direcciones IP, Dominios, Subdominios, URL, MD5 y SHA256.



Tendencias en nuevas vulnerabilidades

- Múltiples agencias de seguridad han publicado de manera conjunta un aviso de seguridad cibernética llamado Russian SVR Targets US and Allied Networks, para exponer el actual Servicio de Inteligencia Exterior de Rusia (SVR) que se encuentran explotando cinco vulnerabilidades conocidas públicamente. Para más información leer el Boletín 2021-163.

- Se ha detectado una nueva vulnerabilidad que afecta a la VPN SSL Pulse Connect Secure, la cual se encuentra registrado como CVE-2021-22893 y tiene una puntuación 10 de 10 de gravedad máxima. Para más información leer el Boletín 2021-167.

- SonicWall ha abordado tres vulnerabilidades de seguridad críticas en su producto de seguridad de correo electrónico (ES) alojado y local que se están explotando. Para más información leer el Boletín 2021-169.

- SAP para este mes abordó múltiples vulnerabilidades críticas. El más grave de ellos afecta el producto Business Client. Además, otros dos productos de la compañía recibieron parches para fallas de gravedad crítica que brindan a los usuarios no autorizados acceso a los objetos de configuración y permiten la ejecución remota de código. Para más información leer el Boletín 2021-171.

Tendencias en actividades maliciosas

- Ciberdelincuentes relacionados al grupo APT Iron Tiger han actualizado una variante de malware SysUpdate, el cual ahora ejecuta cinco archivos en su método de propagación en lugar de los tres habituales, para más información leer Boletín 2021-170.

- Ciberdelincuentes están explotando las fallas de ProxyLogon Microsoft Exchange Server para captart máquinas vulnerables a una botnet de criptomonedas llamada Prometei, la cual abarca sectores de finanzas, seguros, comercio minorista, fabricación, servicios públicos, viajes y construcción, comprometiendo redes de entidades ubicadas en los EE. UU., Reino Unido y varios países de Europa, América del Sur y Asia Oriental, para más información leer Boletín 2021-174.

- Desde el mes de marzo de 2020 hasta febrero de 2021, un ciberdelincuente se conectó a una entidad comprometida a través del dispositivo Pulse Secure VPN utilizando direcciones IP remotas con sede en EE.UU., para más información leer Boletín 2021-175.

- Los servidores de Microsoft SharePoint ahora se han unido a la lista de dispositivos de red que están siendo abusados como vector de entrada a las redes corporativas por bandas de ransomware, para más información leer Boletín 2021-179.

4. Detalles

Vulnerabilidades

Boletín	2021-158
Asunto	MICROSOFT CORRIGE 114 VULNERABILIDADES EN EL PARCHE DE SEGURIDAD DE ABRIL
Emisión	16/04/2021
CVE	Según Tabla Boletín
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Múltiples servicios de Microsoft

Descripción

Microsoft publicó actualizaciones de seguridad que abordan 114 vulnerabilidades, de las cuales 19 fueron clasificadas como críticas. Este lanzamiento incluye parches para cuatro vulnerabilidades de ejecución remota de código (RCE) en Microsoft Exchange.

Las cuatro vulnerabilidades en Exchange afectan a las versiones 2013, 2016 y 2019 y son las siguientes: CVE-2021-28480, CVE-2021-28481, CVE-2021-28482 y CVE-2021-28483.

Además de las vulnerabilidades en Exchange, se repararon cinco zero-days. Las mismas son la CVE-2021-27091, CVE-2021-28310, CVE-2021-28312, CVE-2021-28437 y la CVE-2021-28458. En el caso de la CVE-2021-28310, se trata de una vulnerabilidad de escalación de privilegios que ha estado siendo explotada da manera activa por atacantes.

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 de los hipervínculos compartidos en el boletín de acuerdo a cada vulnerabilidad mencionada.

Boletín	2021-163
Asunto	SVR EXPLOTA VULNERABILIDADES PUBLICAS
Emisión	20/04/2021
CVE	CVE-2018-13379, CVE-2019-9670, CVE-2019-11510, CVE-2019-19781 y CVE-2020-4006
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

- FortiOS 6.0.0 a 6.0.4, 5.6.3 a 5.6.7 y 5.4.6 a 5.4.12
- Synacor Zimbra Collaboration Suite 8.7.x antes de 8.7.11p10
- Pulse Connect Secure 9.0R1 - 9.0R3.3, 8.3R1 - 8.3R7, 8.2R1 - 8.2R12 y 8.1R1 - 8.1R15
- Pulse Policy Secure 9.0R1 - 9.0R3.1, 5.4R1 - 5.4R7, 5.3R1 - 5.3R12, 5.2R1 - 5.2R12 y 5.1R1 - 5.1R15
- Citrix Application Delivery Controller, Citrix Gateway y dispositivo Citrix SD-WAN WANOP
- VMware Workspace ONE Access

Descripción

Múltiples agencias de seguridad han publicado de manera conjunta un aviso de seguridad cibernética llamado Russian SVR Targets US and Allied Networks, para exponer el actual Servicio de Inteligencia Exterior de Rusia (SVR) que se encuentran explotando cinco vulnerabilidades conocidas públicamente.

El SVR también se encuentra conocido como APT29, Cozy Bear y The Dukes, quienes utilizan con frecuencia vulnerabilidades conocidas públicamente para realizar escaneos y actividades de explotación contra sistemas vulnerables en un esfuerzo menor por obtener credenciales de autenticación y usarlas para obtener acceso con mayores privilegios. Actualmente abarcan las redes estadounidenses y aliadas, incluida la seguridad nacional y los sistemas relacionados con el gobierno.

El aviso de seguridad cibernética contiene los siguientes CVE:

- CVE-2018-13379 se analiza en: Fortinet FortiGate VPN
- CVE-2019-9670 se describe en: Synacor Zimbra Collaboration Suite
- CVE-2019-11510 se describe en: Pulse Secure Pulse Connect Secure VPN
- CVE-2019-19781 se describe en: Citrix Application Delivery Controller y Gateway
- CVE-2020-4006 se describe en: VMware Workspace ONE Access.

Actualización o Mitigación

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

Boletín	2021- 165
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE APACHE HTTP SERVER
Emisión	20/04/2021
CVE	CVE-2012-0883
Categoría	Vulnerabilidad
Severidad	Media

Servicios Afectados

• Versiones anteriores a Apache HTTP Server 2.4.2

Descripción

Una vulnerabilidad, que fue clasificada como crítica, fue encontrada en Apache HTTP Server 2.4.2 en Oracle Solaris (Web Server). Este problema se ve afectado por un procesamiento desconocido en la biblioteca ld_library_path.

Esta vulnerabilidad se reveló en diciembre del 2012 como aviso confirmado clasificada como CVE-2012-0883. El ataque puede iniciarse de forma remota. No se requiere ninguna forma de autenticación para la explotación. A través de la manipulación de un input desconocido se causa una vulnerabilidad de clase escalada de privilegios.
La explotación exitosa requiere la interacción del usuario por parte de la víctima. Se conocen los detalles técnicos, pero no hay ningún exploit disponible. Esta vulnerabilidad está asignada a T1068 por el proyecto MITRE ATT & CK.
Los paquetes httpd de Red Hat Enterprise Linux y Fedora no se ven afectados debido a la aplicación de httpd - * - apctl.patch, que elimina el soporte para la lectura en el archivo envvars, donde se origina esta falla.

Actualización o Mitigación

• Realizar la actualización a la versión 2.4.2 de Apache HTTP Server

Boletín	2021- 166
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE WORDPRESS
Emisión	20/04/2021
CVE	CVE-2021-29447 y CVE-2021-29450
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Versiones anteriores a 5.7.1 de WordPress

Descripción

WordPress ha publicado la versión 5.7.1 de su sistema de administración de contenido (CMS), la cual contiene más de 25 correcciones de errores, incluidos parches para dos vulnerabilidades de seguridad.

Una de las fallas de seguridad parchadas es una vulnerabilidad de entidad externa XML (XXE) en la biblioteca ID3 en PHP 8, que es utilizada por WordPress. Rastreada como CVE-2021-29447, la vulnerabilidad se considera de alta gravedad.

La segunda vulnerabilidad que afectando a la API REST podría explotarse para acceder a datos confidenciales. Registrado como CVE-2021-29450, el error de seguridad se considera de gravedad media. El problema existe en un bloque en el editor de WordPress, que los atacantes podrían aprovechar para exponer publicaciones y páginas protegidas con contraseña. La explotación exitosa de la falla requiere que el atacante tenga al menos privilegios de colaborador.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) indicó que las vulnerabilidades abordadas en WordPress 5.7.1 afectan las versiones 4.7 a 5.7 y que los ciberdelincuentes capaces de explotar con éxito una de estas podría tomar el control de un sitio web afectado.

Actualización o Mitigación

• Realizar la actualización a la versión 5.7.1 de WordPress.

Boletín	2021- 167
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE VPN PULSE SECURE
Emisión	21/04/2021
CVE	CVE-2021-22893
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• VPN SSL Pulse Connect Secure versión 9.0R3, 9.0R3.1, 9.0R3.2, 9.0R3.4, 9.0R3.5, 9.0R4, 9.0R4.1, 9.0R5.0, 9.0R6.0, 9.1R1, 9.1R2, 9.1R3, 9.1R4, 9.1R4.1, 9.1R4.2, 9.1R4.3, 9.1R5, 9.1R6, 9.1R7, 9.1R8, 9.1R8.1, 9.1R8.2, 9.1R8.4, 9.1 R9, 9.1R9.1, 9.1R9.2, 9.1R10, 9.1R10.0, 9.1R10.2, 9.1R11, 9.1R11.0, 9.1R11.1 y 9.1R11.3.

Descripción

La vulnerabilidad CVE-2021-22893 está siendo explotada y permite a un usuario no autenticado realizar la ejecución remota de archivos arbitrarios en la VPN, además de otros fallos que afectan a la VPN Pulse Secure. El abuso de la vulnerabilidad está orientado a empresas muy diversas, además de instituciones gubernamentales. Esta vulnerabilidad tiene una puntuación CVSS crítica y representa un riesgo significativo para las redes VPN Pulse Secure.

Los usuarios pueden actualizar a la versión 9.1R.11.4 y poder así corregir este problema. Además, Pulse Secure ha lanzado la herramienta Pulse Connect Secure Integrity Tool para que los usuarios sepan si su sistema se ha visto afectado o no por esta vulnerabilidad.

Actualización o Mitigación

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

Boletín	2021- 168
Asunto	APT'S APROVECHAN TÉCNICAS DE DERIVACIÓN DE AUTENTICACIÓN Y PULSE SECURE
Emisión	21/04/2021
CVE	CVE-2021-22893
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Pulse Secure VPN

Descripción

Durante la investigación sobre las actividades de UNC2630, se ha descubierto una nueva familia de malware llamada SLOWPULSE. Este malware y sus variantes se aplican como modificaciones a los archivos legítimos de Pulse Secure para omitir o registrar credenciales en los flujos de autenticación que existen dentro del objeto legítimo compartido de Pulse Secure libdsplibs[.]so. Tres de las cuatro variantes descubiertas permiten al atacante eludir la autenticación de dos factores. A continuación, se detalla una breve descripción general de estas variantes.

Variante 1 de SLOWPULSE

Esta variante es responsable de eludir las rutinas de autenticación LDAP y RADIUS-2FA si el atacante proporciona una contraseña secreta de puerta trasera. La muestra inspecciona las credenciales de inicio de sesión utilizadas al comienzo de la rutina asociada de cada protocolo y fuerza estratégicamente la ejecución del parche de autenticación exitoso si la contraseña proporcionada coincide con la contraseña de puerta trasera elegida por el atacante.

Actualización o Mitigación

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

Boletín	2021- 169
Asunto	ACTUALZIACIÓN DE SEGURIDAD DE SONICWALL
Emisión	22/04/2021
CVE	CVE-2021-20021 y CVE-2021-20022 y CVE-2021-20023
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Versiones 10.0.1, 10.0.2, 10.0.3 y 10.0.4 de Email Security para sistemas operativos Windows, hardware, dispositivos virtuales ESXi y Hosted Email Security

Descripción

Rastreadas como CVE-2021-20021 y CVE-2021-20022 y CVE-2021-20023, permiten la ejecución de código de manera remota en los dispositivos. Estas vulnerabilidades fueron ejecutadas en conjunción para obtener acceso administrativo y la ejecución de código en un dispositivo de SonicWall. Los fallos descubiertos afectan a SonicWall Email Security, en sus versiones hardware, dispositivo virtual o instalación software sobre sistema operativo Windows. SonicWall Hosted Email Security también se vio afectado.

El adversario aprovechó estas vulnerabilidades, con un conocimiento profundo de la aplicación SonicWall, para instalar una puerta trasera, acceder a archivos y correos electrónicos, y moverse lateralmente a la red de la organización afectada.

A continuación, se muestra un breve resumen de los tres defectos:

• CVE-2021-20021: Permite a un atacante crear una cuenta administrativa enviando una solicitud HTTP diseñada al host remoto.

• CVE-2021-20022: Permite a un atacante autenticado posteriormente cargar un archivo arbitrario en el host remoto.

• CVE-2021-20023: Un error de recorrido de directorio que permite a un atacante autenticado posteriormente leer un archivo arbitrario en el host remoto.

Además, el acceso administrativo no solo permitió al atacante explotar CVE-2021-20023 para leer archivos de configuración, contando aquellos que contienen información sobre cuentas existentes, así como credenciales de Active Directory, sino también vulnerar el CVE-2021-20022 para cargar un archivo ZIP que contiene un JSP - shell web basado en BEHINDER que es capaz de aceptar comunicaciones cifradas de comando y control (C2).

Actualización o Mitigación

• Realizar la actualización a la versión 10.0.9.6173 Hotfix para Windows y 10.0.9.6177 Hotfix para hardware y dispositivos virtuales ESXi.

Boletín	2021- 171
Asunto	ACTUALIZACIÓN DE SEGURIDAD EN SAP EN BUSINESS CLIENT, COMMERCE Y NETWEAVER
Emisión	22/04/2021
CVE	CVE-2021-27602, CVE-2021-21481, CVE-2021-21482, CVE-2021-21483, CVE-2020-26832, CVE-2021-27608 y CVE-2021-21485
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

- Versiones anteriores a 7.10, 7.11, 7.30, 7.31, 7.40, 7.50 de NetWeaver
- SAP Commerce 1808, 1811, 1905, 2005 y 2011
- SAP Business Client

Descripción

El equipo de seguridad de productos de SAP compartió en total 19 notas de seguridad, de los cuales, cinco son actualizaciones de errores anteriores. Y una de estas actualizaciones se refiere a una vulnerabilidad que afecta a SAP Business Client, una interfaz de usuario que actúa como un punto de entrada a varias aplicaciones comerciales de SAP. Este riesgo de seguridad no reside en el producto en sí, sino en el control del navegador que lo acompaña.

Además, SAP entregó una actualización que corrige un error de ejecución de código remoto en SAP Commerce que se utiliza para organizar la información del producto para su distribución a través de múltiples canales de comunicación. El problema se identifica como CVE-2021-27602 y afecta a SAP Commerce 1808, 1811, 1905, 2005 y 2011. Un atacante autorizado en la aplicación Backoffice Product Content Management de SAP Commerce puede explotarla para lograr la ejecución remota de código en el sistema inyectando código malicioso en las reglas de origen.

Otra actualización que SAP considera crítica es para el componente Servicio de migración en la pila de software NetWeaver (versiones 7.10, 7.11, 7.30, 7.31, 7.40, 7.50) que permite a las organizaciones integrar datos y procesos comerciales de múltiples fuentes. La vulnerabilidad identifica como CVE-2021-21481. Los atacantes no autorizados podrían acceder a los objetos de configuración para obtener derechos administrativos en el sistema.

Actualización o Mitigación

- Realizar actualización de seguridad en base a las notas de seguridad indicadas.

Boletín	2021- 172
Asunto	ACTUALIZACIONES DE SEGURIDAD DE ORACLE
Emisión	23/04/2021
CVE	CVE-2021-2177, CVE-2020-1472, CVE-2021-2317, CVE-2021-2256 y CVE-2021-2248
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• E-Business Suite de Oracle
• Fusion Middleware y Retail Applications
• Oracle Virtualization
• Cloud Infrastructure Storage Gateway, Storage Cloud Software Appliance y ZFS Storage Appliance Kit

Descripción

La más grave de estas vulnerabilidades podrían aprovecharse para ejecutar código de forma remota dentro del contexto de las aplicaciones vulnerables, lo que podría resultar en un compromiso total del sistema.

E-Business Suite de Oracle recibió parches para la mayor cantidad de agujeros de seguridad. De estos, 22 podrían ser explotados de forma remota por atacantes no autenticados. También, MySQL también se vio muy afectado, con parches para 49 vulnerabilidades, 10 de las cuales podrían explotarse de forma remota sin autenticación.

Fusion Middleware y Retail Applications también recibieron correcciones para una gran cantidad de problemas de seguridad, de los cuales 36 son explotables de forma remota sin autenticación y 31 explotables por atacantes remotos no autenticados.

De las 24 fallas parcheadas en Oracle Virtualization, 5 de estas podrían ser explotadas por atacantes remotos sin autenticación y 2 de ellas tienen una puntuación CVSS de 10 (CVE-2021-2177 y CVE-2021-2248).

Además, se abordaron otros tres errores con la puntuación CVSS más alta en ZFS Storage Appliance Kit (CVE-2020-1472), Cloud Infrastructure Storage Gateway (CVE-2021-2317) y Storage Cloud Software Appliance (CVE-2021-2256).

Se recomienda a las organizaciones que revisen los parches trimestrales de Oracle y apliquen las actualizaciones de software necesarias lo antes posible, para asegurarse de que permanezcan protegidas de posibles ataques. Oracle dice que recibe periódicamente informes de ataques dirigidos a vulnerabilidades antiguas para las que ya hay parches disponibles.

Actualización o Mitigación

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

Boletín	2021- 176
Asunto	CIBERDELINCUENTES APROVECHAN VULNERABILIDADES DE SOLITON FILEZEN PARA OBTENER DATOS CONFIDENCIALES
Emisión	26/04/2021
CVE	CVE-2020-5639 y CVE-2021-20655
Categoría	Vulnerabilidad
Severidad	Media

Servicios Afectados

• Soliton FileZen V3.0.0 a V4.2.7

• Soliton FileZen V5.0.0 a V5.0.2

Descripción

Los servidores FileZen permiten a los usuarios compartir datos de acuerdo con sus necesidades, superando problemas con límites de tamaño de archivo, filtros de contenido y pérdida de potencia en la red.

La vulnerabilidad CVE-2020-5639 es un problema de recorrido de ruta de acceso que podría ser aprovechado por atacantes remotos para cargar un archivo arbitrario a través de una solicitud HTTP especialmente diseñada, lo que podría conducir a la ejecución arbitraria de comandos del sistema operativo. La vulnerabilidad CVE-2021-20655 podría ser aprovechada por un atacante remoto con derechos de administrador para ejecutar comandos shell arbitrarios en el sistema destino.

Las dos vulnerabilidades fueron explotadas y evidencias en una campaña de ataque cibernético a gran escala que también resultó con el acceso no autorizado a un almacenamiento compartido de archivos Soliton FileZen utilizado por el personal de la Oficina del Gabinete del Primer Ministro japonés.

Actualización o Mitigación

• Realizar la actualización a la versión V4.2.8 y V5.0.3.

Boletín	2021- 180
Asunto	VULNERABILIDAD EN KDC PERMITE OBTENER ACCESO SIN RESTRICCIONES EN F5 BIG-IP
Emisión	30/04/2021
CVE	CVE-2021-23008 y CVE-2021-23016
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• APM BIG-IP versión 11.5.2 - 11.6.5, 12.1.0 - 12.1.5, 13.1.0 - 13.1.3, 14.1.0 - 14.1.3, 15.0.0 - 15.1.2 y 16.0.0 - 16.0.1

Descripción

La vulnerabilidad existe específicamente en uno de los componentes de software centrales del dispositivo: Access Policy Manager (APM). Administra y aplica las políticas de acceso, es decir, se asegura de que todos los usuarios estén autenticados y autorizados para usar una aplicación determinada. APM a veces también se usa para proteger el acceso a la consola de administración de Big-IP. Por ello, APM implementa Kerberos como un protocolo de autenticación requerido por una política de APM.

Según el aviso de F5, para que el ataque funcione, se requiere que el atacante ya esté dentro del entorno del objetivo. Sin embargo, el acceso inicial puede no ser tan difícil: En marzo, salieron a la luz cuatro fallas críticas de ejecución remota de código (RCE) en la infraestructura de redes empresariales BIG-IP y BIG-IQ de F5 que podrían permitir a los atacantes tomar el control total sobre un sistema vulnerable.

La compañía también publicó parches para una vulnerabilidad de gravedad media en BIG-IP APM (CVE-2021-23016) que podría abusarse para eludir restricciones internas y recuperar contenido estático almacenado dentro de APM.

Actualización o Mitigación

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

Amenazas

Boletín	2021- 159
Asunto	NUEVA INFORMACIÓN DEL RANSOMWARE RAGNAR LOCKER
Emisión	16/04/2021
CVE	No
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

Recientemente se brindó más detalle del ataque de ransomware y como los ciberdelincuentes obtuvieron acceso a la red, comprometiendo computadoras y robando información personal a miles de personas. Las actividades de ransomware fueron atribuidas a Ragnar Locker, quienes declararon que secuestraron 1 TB de datos confidenciales de Capcom y exigieron un rescate de $ 11 millones a cambio de no publicar la información y ofrecer una herramienta de descifrado.

Los operadores de Ragnar Locker obtuvieron acceso a la red interna de Capcom apuntando a un antiguo dispositivo de respaldo VPN ubicado en el norte de la compañía. Parece que en el momento del ataque, Capcom estaba en el proceso de aumentar sus defensas de red, por lo tanto, el dispositivo VPN comprometido estaba dándose de baja, pero en el fondo de la pandemia presionando por el trabajo remoto, el antiguo servidor VPN continuó funcionando. Funciona como respaldo de emergencia en caso de problemas de comunicación.

La evaluación final de la compañía con respecto a la violación de datos es que 15,649 personas se han visto afectadas. La información filtrada no incluía detalles de tarjetas de pago, solo datos corporativos y personales que incluyen nombres, direcciones, números de teléfono y direcciones de correo electrónico.

Recientemente se han identificado publicaciones en Twitter donde se evidencia que el ransomware Ragnar Locker ha realizado posibles ataques satisfactorios a la entidad bancaria First National Bank Northwest Florida.

Actualización o Mitigación

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

Boletín	2021-160
Asunto	NUEVA VARIANTE BOTNET GAFGYT UTILIZA MÓDULOS BASADOS EN MIRAI
Emisión	19/04/2021
CVE	CVE-2017-17215, CVE-2018-10561 y CVE-2014-8361
Categoría	Malware
Severidad	Media

Servicios Afectados

• Sistemas operativos Linux

Descripción

Gafgyt es una botnet que se descubrió por primera vez en 2014. Se dirige a dispositivos vulnerables de Internet de las cosas (IoT) como routers Huawei, routers Realtek y dispositivos ASUS, que luego utiliza para lanzar ataques distribuidos de denegación de servicio (DDoS) a gran escala. También suele utilizar vulnerabilidades conocidas como CVE-2017-17215 y CVE-2018-10561 para descargar payloads en dispositivos infectados.

La última variante ahora ha incorporado varios módulos basados en Mirai junto con nuevos exploits. Las capacidades extraídas de Mirai incluyen varios métodos para llevar a cabo ataques DDoS:

• Inundación HTTP, en la que la botnet envía una gran cantidad de solicitudes HTTP a un servidor de destino para abrumarlo.

• Inundación UDP, donde la botnet envía varios paquetes UDP a un servidor víctima como un medio para agotarlo.

• Varios ataques de inundación de TCP, que aprovechan un protocolo de enlace TCP de tres vías normal, el servidor víctima recibe una gran cantidad de solicitudes, lo que hace que el servidor deje de responder.

• Y un módulo STD, que envía una cadena aleatoria (desde una matriz de cadenas codificada) a una dirección IP en particular.

Mientras tanto, las últimas versiones de Gafgyt contienen nuevos enfoques para lograr el compromiso inicial de los dispositivos de IoT, descubrió Uptycs; Este es el primer paso para convertir los dispositivos infectados en bots para luego realizar ataques DDoS en direcciones IP específicas. Estos incluyen un módulo copiado de Mirai para la fuerza bruta de Telnet y exploits adicionales para vulnerabilidades existentes en dispositivos Huawei, Realtek y GPON.

Actualización o Mitigación

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

Boletín	2021-161
Asunto	MALWARE XMRIG MINER ATACA SERVIDORES NAGIOS
Emisión	19/04/2021
CVE	CVE-2021-25296
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Nagios XI versión 5.7.5

Descripción

Nagios XI es un software ampliamente utilizado que proporciona soluciones de monitoreo de redes y servidores empresariales. La característica en Nagios XI que está bajo explotación es el WMI (Windows Management Instrumentation), el cual permite que los scripts administren las computadoras personales y los servidores de Microsoft Windows, tanto en forma local como remota.

El troyano XMRig miner es una versión modificada de XMRig, que es un minero de criptomonedas multiplataforma de código abierto. Los ciberdelincuentes intentan ejecutar un script bash obtenido del servidor comprometido con IP 118[.]107[.]43[.]174. El script bash ejecutado por el atacante, descarga el minero XMRig desde el mismo servidor donde está alojado el script y libera una serie de scripts para ejecutar el minero XMRig en segundo plano. Una vez que el ataque tenga éxito, los dispositivos se verán comprometidos por criptojacking.

La actualización de Nagios XI a la última versión mitiga la vulnerabilidad. Los usuarios que no puedan utilizar la versión actualizada de Nagios XI pueden actualizar el archivo /usr/local/nagiosxi/html/includes/configwizards/windowswmi/windowswmi.inc.php.

Actualización o Mitigación

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

Boletín	2021-162
Asunto	MALWARE SE PROPAGA A TRAVÉS DE PROYECTOS DE XCODE PARA MAC M1 DE APPLE
Emisión	19/04/2021
CVE	No
Categoría	Malware
Severidad	Media

Servicios Afectados

• Chips M1 de Apple

Descripción

En marzo de 2021, Kaspersky descubrió muestras XCSSET compiladas para los nuevos chips Apple M1, en una campaña de malware en curso, donde los ciberdelincuentes están adaptando activamente sus ejecutables y transfiriéndolos para que se ejecuten en los nuevos Apple Silicon Macs de forma nativa. Este, aloja los paquetes de actualización de Safari en el servidor, luego descarga e instala los paquetes para la versión del sistema operativo del usuario. Además de troyanizar Safari para extraer datos, el malware también es conocido por explotar el modo de depuración remota en otros navegadores como Google Chrome, Brave, Microsoft Edge, Mozilla Firefox, Opera, Qihoo 360 Browser y Yandex Browser para llevar a cabo ataques UXSS.

Este malware vuelve a empaquetar los módulos de payloads para imitar las aplicaciones legítimas de Mac, que son en última instancia responsables de infectar los proyectos locales de Xcode e inyectar el payload principal para que se ejecute cuando se compile el proyecto comprometido.

Los módulos XCSSET vienen con la capacidad de robar credenciales, capturar capturas de pantalla, inyectar JavaScript malicioso en sitios web, extraer datos de usuarios de diferentes aplicaciones e incluso cifrar archivos para obtener un rescate.

El modo de distribución de XCSSET a través de proyectos Xcode manipulados representa una seria amenaza, ya que los desarrolladores afectados que comparten sin saberlo su trabajo en GitHub podrían transmitir el malware a sus usuarios en forma de proyectos Xcode comprometidos, lo que lleva a un ataque similar a una cadena de suministro para los usuarios que confían en estos repositorios como dependencias en sus propios proyectos.

Además, el malware intenta robar información de la cuenta de varios sitios web, incluidas las plataformas de comercio de criptomonedas Huobi, Binance, NNCall.net, Envato y 163.com, con capacidades para reemplazar la dirección en la billetera de criptomonedas de un usuario con las que están bajo el control del atacante.

Actualización o Mitigación

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

Boletín	2021-164
Asunto	CAMPAÑAS DE CIBERATAQUES DE INGENIERÍA SOCIAL ASOCIADAS A SLACK Y BASECAMP
Emisión	20/04/2021
CVE	No
Categoría	Ataque Cibernético
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows
• Slack y BaseCamp

Descripción

BazarLoader se observó por primera vez en abril del año pasado y desde entonces se han observado al menos seis variantes. Este malware está escrito en C ++ tiene la función principal de descargar y ejecutar módulos adicionales.

En la primera campaña detectada recientemente, los ciberdelincuentes se dirigen a empleados de grandes organizaciones con correos electrónicos que pretenden ofrecer información importante relacionada con contratos, servicio al cliente, facturas o nóminas. Los enlaces dentro de los correos electrónicos están alojados en el almacenamiento en la nube de Slack o BaseCamp, lo que podría hacer parecer legítimos si el objetivo trabaja en una organización que utiliza una de esas plataformas.

Los atacantes exhibieron de manera prominente la URL que apuntaba a uno de estos sitios web legítimos bien conocidos en el cuerpo del documento, dándole una apariencia de credibilidad. La URL podría ofuscarse aún más mediante el uso de un servicio de acortamiento de URL, para que sea menos obvio que el enlace apunta a un archivo con una extensión .EXE.

Para este caso, si se hace clic en el enlace, BazarLoader se descarga y se ejecuta en la máquina de la víctima. Los enlaces normalmente apuntan directamente a un ejecutable firmado digitalmente con un gráfico de Adobe PDF como icono. Los archivos suelen perpetuar la artimaña, con nombres como presentation-document.exe, preview-document- [número] .exe o annualreport.exe. Estos archivos ejecutables, cuando se ejecutan, inyectan un payload DLL en un proceso legítimo, como el shell de comandos de Windows, cmd.exe.

Actualización o Mitigación

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

Boletín	2021- 170
Asunto	GRUPO APT IRON TIGER ACTUALIZA MALWARE SYSUPDATE
Emisión	22/04/2021
CVE	CVE-2018-0798, CVE-2017-11882, CVE-2018-0802 y CVE-2021-26855
Categoría	Malware
Severidad	Crítica

Servicios Afectados

- Sistemas operativos Windows
- Microsoft Equation Editor
- Microsoft Exchange

Descripción

Se encontró nueva variante de malware SysUpdate actualizado que ahora usa cinco archivos en su rutina de infección. Se identificó una muestra perteneciente a la familia de malware SysUpdate, también llamada Soldier, FOCUSFJORD e HyperSSL. SysUpdate fue descrito por primera vez por NCC Group en 2018. En el pasado, SysUpdate se cargaba en la memoria mediante un método que involucraba tres archivos como un ejecutable legítimo, a veces firmado y vulnerable a la descarga lateral de la biblioteca de vínculos dinámicos (DLL), un DLL comprometido que era cargado por el archivo legítimo y un archivo binario que generalmente contiene código ofuscado, descomprimido en la memoria por el DLL comprometido.

Actualmente, Iron Tiger se encuentra utilizando cinco archivos bajo la siguiente distribución:

- dlpumgr32.exe, un archivo legítimo firmado que pertenece DESlock.

- DLPPREM32.DLL, una DLL maliciosa cargada por dlpumgr32.exe que carga y decodifica DLPPREM32.bin

- DLPPREM32.bin, un shellcode que descomprime y carga un launcher en la memoria.

- data.res, un archivo cifrado decodificado por el launcher y que contiene dos versiones de SysUpdate: una para una arquitectura de 32 bits y otra para una arquitectura de 64 bits

- config.res, un archivo cifrado decodificado por el launcher y que contiene la configuración de SysUpdate, como la dirección de comando y control.

En resumen, el launcher actúa como un instalador: copiará el malware en un lugar fijo y se asegurará de que se ejecute durante el próximo arranque del host infectado permitiendo a los ciberdelincuentes realizar capturas de pantalla, administrar archivos (como buscar, eliminar, mover, cargar y descargar), administrar procesos y servicios y ejecutar comandos.

Actualización o Mitigación

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

Boletín	2021- 173
Asunto	LAZARUS APT REALIZA CAMPAÑA DE SPEAR PHISHING
Emisión	23/04/2021
CVE	No
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

El ataque probablemente comenzó distribuyendo correos electrónicos de phishing que estaban armados con un archivo comprometido. La siguiente figura muestra el proceso general de este ataque.

Al abrir el documento, le pide al usuario que habilite la macro para ver el documento y con una ventana emergente que solicita una confirmación, se procederá a descargar el malware.

La macro agregó la extensión zip al archivo BMP durante el proceso de conversión de la imagen para simular que es un archivo zip. Este archivo BMP tiene un archivo HTA incrustado. Esta HTA contiene un JavaScript que crea "AppStore.exe" en el directorio "C: \ Users \ Public \ Libraries \ AppStore.exe" y luego completa su contenido.

Se observa que han utilizado un método complejo para eludir los mecanismos de seguridad en los que ha incrustado su archivo HTA malicioso como un archivo zlib comprimido dentro de un archivo PNG que luego se descomprime, convirtiéndose al formato BMP. El primer payload tiene la capacidad de autoeliminarse y fue un launcher que decodificó y descifró el payload de la segunda etapa en la memoria. El payload de la segunda etapa tiene la capacidad de recibir y ejecutar comandos, así como realizar exfiltración y comunicarse a un servidor de comando y control.

En resumen, una vez finalizado el proceso de inicialización, comprueba si las comunicaciones con los servidores de comando y control fueron exitosas o no, y si fueron exitosas pasa al siguiente paso en el que recibe los comandos del servidor y realiza diferentes acciones en base a lo programado.

Actualización o Mitigación

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

Boletín	2021-174
Asunto	PROMETEI BOTNET EXPLOTA SERVIDORES DE MICROSOFT EXCHANGE SIN PARCHES
Emisión	24/04/2021
CVE	CVE-2021-27065 y CVE-2021-26858
Categoría	Cryptominer
Severidad	Alta

Servicios Afectados

• Sistemas operativos Linux y Windows

Descripción

Prometei explota las vulnerabilidades de Microsoft Exchange recientemente divulgados asociados a los ataques de hafnio para vulnerar la red para la implementación de software malicioso, la recolección de credenciales y más.

Descubierto por primera vez en julio de 2020, Prometei es una botnet multimodular, con el actor detrás de la operación que emplea una amplia gama de herramientas especialmente diseñadas y exploits conocidos como EternalBlue y BlueKeep para recolectar credenciales, propagarse lateralmente a través de la red y aumentar la cantidad de sistemas que participan en el grupo de criptominería.

Prometei tiene versiones basadas en Windows y Linux-Unix, y ajusta su payload según el sistema operativo detectado en las máquinas infectadas objetivo cuando se propaga a través de la red y está construido para interactuar con cuatro servidores de comando y control (C2) diferentes, lo que fortalece la infraestructura de la botnet y mantiene las comunicaciones continuas, haciéndola más resistente a las caídas.

Las intrusiones aprovechan las vulnerabilidades recientemente parcheadas en los servidores Microsoft Exchange con el objetivo de vulnerar el poder de procesamiento de los sistemas Windows para minar Monero.

En la secuencia de ataque observada por la empresa, se descubrió que el adversario explotaba las fallas del servidor Exchange CVE-2021-27065 y CVE-2021-26858 como un vector de compromiso inicial para instalar el shell web de China Chopper y obtener acceso por la puerta trasera a la red. Con este acceso en su lugar, el actor de amenazas lanzó PowerShell para descargar el payload inicial de Prometei desde un servidor remoto.

Las versiones recientes del módulo bot vienen con capacidades de puerta trasera que admiten un amplio conjunto de comandos, incluido un módulo adicional llamado "Microsoft Exchange Defender" que se hace pasar por un producto legítimo de Microsoft, que probablemente se encarga de eliminar otros shells web competidores que puedan estar instalados. en la máquina para que Prometei tenga acceso a los recursos necesarios para extraer criptomonedas de manera eficiente

Actualización o Mitigación

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

Boletín	2021-175
Asunto	CIBERDELINCUENTE PROPAGA MALWARE SUPERNOVA A TRAVÉS DE RED VPN
Emisión	26/04/2021
CVE	CVE-2020-10148
Categoría	Malware
Severidad	Crítica

Servicios Afectados

• Pulse Secure VPN

Descripción

Atacante se conectó en la red Pulse Secure VPN de una entidad de Estados Unidos con múltiples cuentas de usuarios las cuales no tenían habilitada la autenticación multifactor. Una vez autenticado en la red VPN, se observa en los registros que el ciberdelincuente utilizo una máquina virtual, luego realizo un movimiento lateral en el dispositivo SolarWinds Orion de la entidad y estableció persistencia mediante el uso de un script de powershell para poder decodificar e instalar el malware SUPERNOVA.

Se cree que el atacante aprovechó el CVE-2020-10148 para omitir la autenticación en el dispositivo SolarWinds y luego usó la API de SolarWinds Orion ExecuteExternalProgram para ejecutar comandos con los mismos privilegios que estaba ejecutando el dispositivo SolarWinds.

El webshell SUPERNOVA permite que un operador remoto inyecte dinámicamente el código fuente de C # en un portal web proporcionado, a través del paquete de software SolarWinds. El código inyectado se compila y ejecuta directamente en la memoria. Permitiendo a un operador remoto realizar reconocimientos, mapeo de dominios y robar información confidencial y/o sensible.

Actualización o Mitigación

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

Boletín	2021- 177
Asunto	NUEVA BOTNET DE CRIPTOMINERÍA SYSRV-HELLO
Emisión	28/04/2021
CVE	CVE-2019-10758, CVE-2017-11610, CVE-2020-16846, CVE-2018-7600
Categoría	Cryptominer
Severidad	Media

Servicios Afectados

• Sistemas operativos Linux y Windows

Descripción

Sysrv-hello es una nueva botnet, reportada por Alibaba Cloud, que busca vulnerabilidades en Windows o Linux para la minería de criptomonedas. El malware de ciberdelincuencia se descubrió por primera vez en febrero, pero está activo desde diciembre de 2020. Fue en marzo cuando tuvo un aumento significativo de actividad. Actualmente se ha actualizado para poder utilizar un único paquete binario capaz de extraer y escabullir malware automáticamente en otros dispositivos.

Escanea en Internet buscando vulnerabilidades, en particular las relacionadas con RCE en PHPUnit, Apache Solar, Confluence, Laravel, JBoss, Jira, Sonatype, Oracle WebLogic y Apache Struts. Una vez que el servidor ha sido vulnerado, Sysrv-hello se propaga por la red a través de ataques de fuerza bruta, utilizando claves privadas SSH que recopila de los servidores infectados. La botnet podría buscar y usar nuevas fallas para expandir sus redes y sus actividades de criptominería debido a la complejidad de su multi-arquitectura y su lenguaje de programación: Golang.

Primero a través de internet busca una maquina vulnerable, luego mediante un empaquetador ejecutable de código abierto compuesto por un lenguaje de programación GOLANG (UPX), se descarga y ejecuta un archivo klr.sh con un código malicioso. Luego al completarse esas acciones, infecta y se propaga por toda la red identificando los usuarios y host al cual lo conllevara a ataques de fuerza fruta utilizando claves privadas SSH, utilizando la información de servidores 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- 178
Asunto	NUEVO ATAQUE DE RANSOMWARE EXPONE VULNERABILIDADES NAS DE QNAP
Emisión	30/04/2021
CVE	CVE-2020-36195 y CVE-2021-28799
Categoría	Ransomware
Severidad	Media

Servicios Afectados

• NAS de QNAP que ejecuta QTS 4.3.3 y QTS 4.3.6

Descripción

Una nueva variedad de ransomware llamada "Qlocker" se dirige a los dispositivos de almacenamiento adjunto a la red (NAS) de QNAP.

Los primeros informes de los archivos comprometidos surgieron el 20 de abril, y los ciberdelincuentes detrás de las operaciones exigieron un pago de bitcoins para compartir la clave de descifrado. En respuesta a los ataques en curso, se publicó un aviso que solicita a los usuarios que apliquen actualizaciones al NAS de QNAP que ejecutan la Consola multimedia, el complemento de transmisión de medios y la sincronización de copia de seguridad híbrida HBS 3 para proteger los dispositivos de cualquier ataque.

Los parches para las tres aplicaciones fueron lanzados por QNAP. El CVE-2020-36195 se refiere a una vulnerabilidad de inyección SQL en el NAS de QNAP que ejecuta la Consola multimedia o media streaming add-on, una explotación exitosa podría brindar como resultado la divulgación de información sensible. Por otro lado, CVE-2021-28799 se refiere a una vulnerabilidad de autorización incorrecta que afecta a QNAP NAS que ejecuta HBS 3 Hybrid Backup Sync que podría ser explotado por un atacante para iniciar sesión en un dispositivo.

Las aplicaciones Consola multimedia, Complemento de transmisión de medios y Sincronización de copia de seguridad híbrida deben actualizarse a la última versión disponible para proteger aún más el NAS de QNAP de los ataques del ransomware.

Actualización o Mitigación

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

Boletín	2021- 179
Asunto	RANSOMWARE HELLO APUNTA A SERVIDORES SHAREPOINT
Emisión	30/04/2021
CVE	CVE-2019-0604
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Microsoft SharePoint

• Sistemas operativos Windows

Descripción

El grupo detrás de los ataques dirigidos a los servidores de SharePoint es una nueva operación de ransomware que se vio por primera vez a fines de 2020. El grupo es rastreado por proveedores de seguridad bajo los nombres en clave de Hello o el ransomware WickrMe, debido a su uso de cuentas de mensajería instantánea encriptadas de Wickr como una forma para que las víctimas se acerquen y negocien la tarifa de rescate.

El error CVE-2019-0604, permite a los atacantes tomar el control del servidor de SharePoint para soltar un webshell, que luego usan para instalar una puerta trasera como una forma de poder ejecutar scripts de PowerShell automatizados que eventualmente descargan e instalan el payload final: el ransomware Hello.

Los primeros ataques de Hello / WickrMe en los que los atacantes utilizaron SharePoint como vector de entrada a la red de una empresa fueron detectados en enero, pero en un informe publicado recientemente, se evidencio que los ataques aún continúan.

Actualización o Mitigación

• Bloquear los indicadores de compromisos (IOC) asociados al boletín emitido, en los dispositivos de seguridad de su infraestructura.

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.