SECURESOFT CORPORATION
e-Secure Consulting Group

Reporte Quincenal de Ciberinteligencia Securesoft

Fecha:

18 diciembre de 2020

El presente documento contiene información para la comunidad de ciberseguridad.

Equipo de Ciberinteligencia
CIB-FOR-2020-017

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

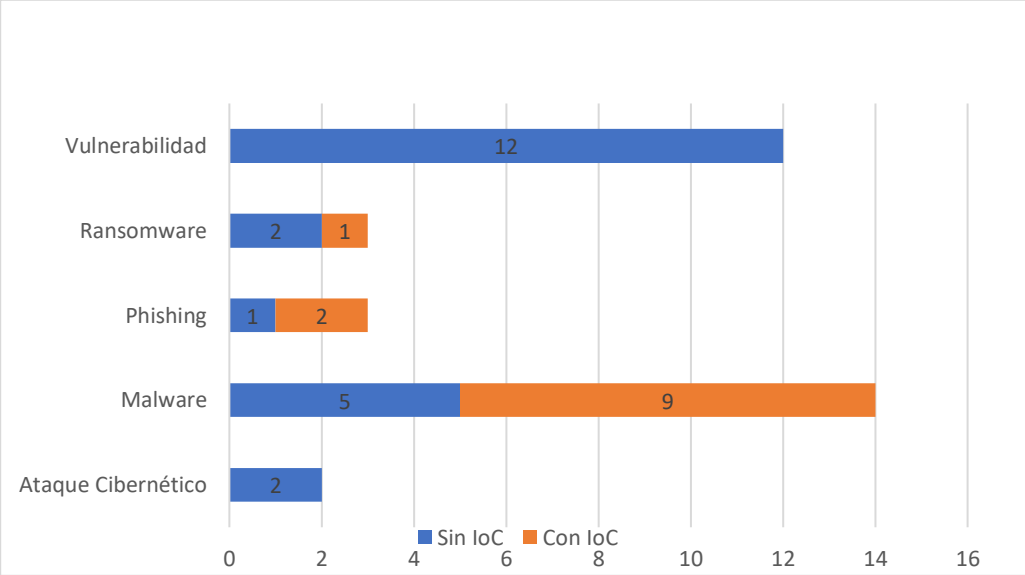
Este documento muestra el resumen, la fecha de publicación, CVE asociado y servicios afectados de vulnerabilidades y amenazas que se han hecho públicas en el transcurso del 01 de diciembre hasta el 17 de diciembre del 2020.

3. Resumen

En el presente informe se exponen 34 análisis de vulnerabilidad y amenazas, de las cuales 33 tienen severidad alta y 1 severidad crítica.

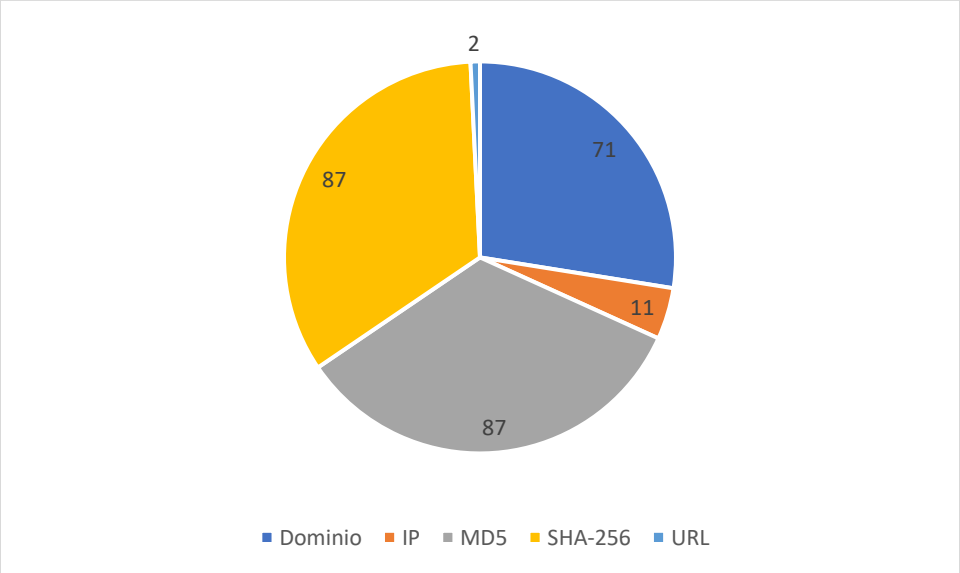
Amenazas analizadas por tipología

En las investigaciones elaboradas para el presente informe se trataron vulnerabilidades, ransomware, malware, ataques cibernéticos y phishing. 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 258 IoCs entre Dominios, URL, IP, MD5 y SHA256.



Tendencias en nuevas vulnerabilidades

- Microsoft hizo público los parches de seguridad correspondiente al mes de diciembre de 2020, en el cual se han corregido un total de 58 vulnerabilidades. Para más información leer el Boletín 2020-420, en la cual podrá encontrar la actualización para estas vulnerabilidades.
- Se hizo público un código de explotación de prueba de concepto para una nueva técnica de ataque, que puede eludir el protocolo de autenticación Kerberos en entornos Windows, y permitir que los intrusos accedan a servicios sensibles conectados a la red. Para más información leer el Boletín 2020-416, en la cual podrá encontrar la actualización de las vulnerabilidad.
- Google publicó una actualización de seguridad de su navegador Chrome que corrige 87 vulnerabilidades de alta gravedad en su navegador Chrome para usuarios de Windows, Mac y Linux. Para más información leer el Boletín 2020-414, en la cual podrá encontrar la actualización para estas vulnerabilidades.

Tendencias en actividades maliciosas

- Se descubrió una campaña generalizada, en el cual los actores detrás de esta campaña obtuvieron acceso a numerosas organizaciones públicas y privadas de todo el mundo. A través del acceso de actualizaciones troyanizadas del software de gestión y supervisión de TI Orion de SolarWind, para más información leer Boletín 2020-422.

- La empresa líder en ciberseguridad FireEye, reveló hoy que recibió un ciberataque por un actor de amenazas de un grupo patrocinado por el estado, se recomienda aplicar las contramedidas publicadas por Fireeye, para más información leer Boletín 2020-411.

- La familia de malware PyMicropsia, basada en Python, recientemente descubierta se dirige a los procesos de Outlook y las credenciales del navegador de las víctimas de Microsoft Windows, para más información leer Boletín 2020-424.

4. Detalles

Vulnerabilidades

Boletín	2020-429
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE CYBERARK
Emisión	17/12/2020
CVE	Varios
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Versiones anteriores a la 12.0 del servidor de PTA y el complemento CPM para PTA.

Descripción

Se ha identificado una vulnerabilidad de CyberArk Privileged Threat Analytics (PTA), lo que puede ocasionar una exposición de la contraseña de administrador de la aplicación PTA y afectar la credibilidad de la salida de detección de la aplicación PTA.

Actualización o Mitigación

El fallo de seguridad ha sido solucionado y se recomienda a los usuarios aplicar la última actualización aquí.

Boletín	2020-430
Asunto	HPE REVELÓ UN ERROR DE DÍA CERO EN EL SOFTWARE SIM PARA WINDOWS Y LINUX
Emisión	17/12/2020
CVE	CVE-2020-7200
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• HPE Systems Insight Manager (SIM) para Windows y Linux.

Descripción

Hewlett Packard Enterprise (HPE) reveló un error de día cero en las últimas versiones de su software patentado HPE Systems Insight Manager (SIM) para Windows y Linux.

Actualización o Mitigación

Se recomienda deshabilitar las funciones de "Busqueda federada" y "Configuración de CMS federado" y realizar el procedimiento para el bloqueo del ataque indicado aquí.

Boletín	2020-426
Asunto	ERRORES CRÍTICOS DEL ANALIZADOR XML DE GOLANG PUEDEN PROVOCAR EL DESVÍO DE LA AUTENTICACIÓN SAML
Emisión	16/12/2020
CVE	CVE-2020-29509, CVE-2020-29510 y CVE-2020-29511
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Paquete encoding/xml en Go

Descripción

Se revelaron 3 vulnerabilidades críticas dentro del analizador XML del lenguaje Go. Estas vulnerabilidades que también afectan a múltiples implementaciones SAML basadas en Go, pueden conducir a una omisión completa de la autenticación SAML que impulsa las aplicaciones web prominentes en la actualidad.

Actualización o Mitigación

Se recomienda instalar el módulo github.com/mattermost/xml-roundtrip-validator que puede detectar construcciones inestables en un documento XML.

Boletín	2020-427
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE MOZILLA
Emisión	16/12/2020
CVE	Varios
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Versiones anteriores a Mozilla Firefox 84

Descripción

Recientemente Mozilla ha publicado actualizaciones de seguridad para el navegador web Firefox, con la finalidad de abordar una vulnerabilidad crítica y errores de alta gravedad. Con la actualización lanzada como Firefox versión 84, se logró un aumento del rendimiento del navegador.

Actualización o Mitigación

Todos los fallos de seguridad han sido solucionados y se recomienda a los usuarios aplicar la última actualización aquí.

Boletín	2020-420
Asunto	MICROSOFT CORRÍGE 58 VULNERABILIDADES EN EL PARCHE DE SEGURIDAD DE DICIEMBRE
Emisión	12/12/2020
CVE	Varios
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

- Microsoft Windows
- Edge
- ChakraCore
- Microsoft Office, Services y Web Apps
- Exchange Server
- Azure DevOps
- Microsoft Dynamics
- Azure SDK
- Visual Studio
- Azure Sphere

Descripción

Microsoft hizo público los parches de seguridad correspondiente al mes de diciembre de 2020, en el cual se han corregido un total de 58 vulnerabilidades.

Actualización o Mitigación

Todos los fallos de seguridad han sido solucionados y se recomienda a los usuarios aplicar la última actualización.

Boletín	2020-416
Asunto	NUEVA TÉCNICA DE ATAQUE QUE PUEDE ELUDIR EL PROTÓCOLO DE AUTENTICACIÓN KERBEROS
Emisión	11/12/2020
CVE	CVE-2020-17049
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

- Windows Server 2012 R2
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2016
- Windows Server 20189
- Windows Server versión 2004, 1903 y 1909
- Windows Server versión 20H2

Descripción

Se publicó un código de explotación de prueba de concepto para una nueva técnica de ataque que puede eludir el protocolo de autenticación Kerberos en entornos Windows, y permitir que los intrusos accedan a servicios sensibles conectados a la red.

Actualización o Mitigación

Todos los fallos de seguridad han sido solucionados y se recomienda a los usuarios aplicar la última actualización.

Boletín	2020-414
Asunto	APACHE LANZA ACTUALIZACIÓN DE SEGURIDAD PARA APACHE STRUTS 2
Emisión	10/12/2020
CVE	CVE-2020-17530
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Apache Struts desde la versión 2.0.0 hasta 2.5.25

Descripción

La Apache Software Foundation ha publicado una actualización de seguridad para abordar una falla de "posible ejecución remota de código" en Struts 2 que está relacionada con la tecnología OGNL. La vulnerabilidad de ejecución de código remoto, rastreada como CVE-2020-17530, reside en la evaluación OGNL forzada cuando se evalúa en la entrada del usuario sin procesar en los atributos de la etiqueta.

Actualización o Mitigación

Se recomienda actualizar a la última versión de acuerdo con la versión del producto afectado.

Boletín	2020-409
Asunto	CISCO PUBLICA ACTUALIZACIÓN DE SEGURIDAD
Emisión	07/12/2020
CVE	CVE-2020-27125 y CVE-2020-27130
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Versiones 4.21 y anteriores de Cisco Security Manager.

Descripción

Cisco ha publicado actualizaciones de seguridad para abordar dos vulnerabilidades con exploits públicos que afectan a Cisco Security Manager, que podrían permitir la ejecución remota de código después de una explotación exitosa.

Actualización o Mitigación

Todos los fallos de seguridad han sido solucionados se recomienda actualizar a la última versión de del producto afectado.

Boletín	2020-410
Asunto	QNAP CORRIGE LAS VULNERABILIDADES DE QTS
Emisión	07/12/2020
CVE	CVE-2020-2495, CVE-2020-2496, CVE-2020-2497 y CVE-2020-2498
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

- QTS hero h4.5.1.1472 compilación 20201031 y posterior
- QTS 4.5.1.1456 compilación 20201015 y posterior
- QTS 4.4.3.1354 compilación 20200702 y posterior
- QTS 4.3.6.1333 compilación 20200608 y posterior
- QTS 4.3.4.1368 compilación 20200703 y posterior
- QTS 4.3.3.1315 compilación 20200611 y posterior
- QTS 4.2.6 compilación 20200611 y posterior

Descripción

QNAP, fabricante de dispositivos de almacenamiento conectado a la red (NAS), lanzó el 7 de diciembre actualizaciones de seguridad para abordar las vulnerabilidades que podrían permitir a los atacantes tomar el control de los dispositivos NAS sin parches después de una explotación exitosa.

Actualización o Mitigación

Todos los fallos de seguridad han sido solucionados se recomienda actualizar a la última versión de del producto afectado aquí.

Boletín	2020-406
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE GOOGLE CHROME
Emisión	04/12/2020
CVE	Varios
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Google Chrome

Descripción

Recientemente Google ha publicado una actualización de seguridad del navegador Chrome que corrige fallas, de los cuales cuatro de ellas son de gravedad de alta. Google publicó Chrome 86.0.4240.183 para usuarios de Windows, Mac y Linux para abordar estas vulnerabilidades.

Actualización o Mitigación

Todos los fallos de seguridad han sido solucionados se recomienda actualizar a la última versión de del producto afectado aquí.

Boletín	2020-404
Asunto	ACTUALIZACIONES DE SEGURIDAD
Emisión	03/12/2020
CVE	CVE-2020-27177
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Xerox DocuShare versión 6.61, 7.0, y 7.5

Descripción

Xerox emitió la solución para dos vulnerabilidades que afectan a su plataforma de gestión de documentos empresariales DocuShare. Los errores, si se explotan, podrían exponer a los usuarios de DocuShare a un ataque que resulte en la pérdida de información confidencial.

Actualización o Mitigación

Se recomienda actualizar a la última versión.

Amenazas

Boletín	2020-398
Asunto	DEFECTO CRÍTICO DE ORACLE WEBLOGIC EXPLOTADO ACTIVAMENTE POR EL MALWARE DARKIRC
Emisión	1/12/2020
CVE	Ninguno
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Oracle WebLogic Server

Descripción

Los ciberdelincuentes vienen apuntando a servidores Oracle WebLogic en peligro ante la vulnerabilidad CVE-2020-14882. Utilizan al menos cinco payloads diferentes, dentro de los cuales, se encuentra el malware para implementar Cobalt Strike que permite el acceso remoto a servidores comprometidos, y en una segunda etapa implementar el payload del malware DarkIRC diseñado a explotar la vulnerabilidad de ejecución remota corregida por Oracle, revisada en el Boletín Nro. 2020-339.

DarkIRC ataca a servidores sin parche mediante un script de PowerShell, ejecutado a través de una solicitud HTTP GET en forma de un binario malicioso que viene con capacidades anti-análisis y anti-sandbox. Antes de desempaquetar el malware final, primero verificará si se está ejecutando en una máquina virtual VMware, VirtualBox, VBox, QEMU o Xen, y detendrá el proceso de infección si detecta un entorno de espacio aislado.

Una vez desempaquetado, DarkIRC se instalará en %APPDATA%\Chrome\Chrome[.]exe y obtendrá persistencia en el dispositivo comprometido mediante la creación de una entrada de ejecución automática. DarkIRC viene realizando diversas actividades dentro de las cuales incluyen, entre otras, registro de teclas, descarga de archivos y ejecución de comandos en el servidor infectado, robo de credenciales, propagación a otros dispositivos a través de MSSQL y RDP (fuerza bruta), SMB o USB, así como el lanzamiento de varias versiones de ataques DDoS**.**

Boletín	2020-411
Asunto	RECIENTE CIBERATAQUE POR UN GRUPO APT ESTADO NACIÓN A FIREEYE
Emisión	08/12/2020
CVE	Varios
Categoría	Ataque Cibernético
Severidad	Alta

Servicios Afectados

- Escritorio remoto de Windows (RDS)
- Microsoft Outlook, Exchange, Sharepoint, Active Directory y Exchange Server
- Citrix Application Delivery Controller y Citrix Gateway
- Fortinet Fortigate SSL VPN
- VPN SSL de Pulse Secure
- ZoHo ManageEngine Desktop Central
- ZoHo ManageEngine ServiceDesk Plus
- Microsoft Windows

Descripción

Recientemente FireEye fue atacado por un actor de amenazas altamente sofisticado, la empresa indicó que la disciplina, seguridad operativa y técnicas llevan a creer que fue un ataque patrocinado por el estado.

El actor de amenazas que se infiltró en las defensas de FireEye se enfocó específicamente en los activos de FireEye y utilizó tácticas diseñadas para contrarrestar tanto el examen forense como las herramientas de seguridad que detectan actividades maliciosas. En base a la investigación realizada hasta la fecha, se descubrió que el atacante apuntó y accedió a ciertas herramientas de evaluación del Red Team que se usan para probar la seguridad de los clientes. Por ello, se informó que ninguna de las herramientas contiene exploits de día cero.

Las herramientas robadas van desde scripts simples utilizados para automatizar el reconocimiento hasta marcos completos que son similares a las tecnologías disponibles públicamente como CobaltStrike y Metasploit, así indicó FireEye en una publicación de su blog Threat Research.

Boletín	2020-400
Asunto	CRUTCH: BACKDOOR DE TURLA UTILIZADO PARA EXFILTRAR DOCUMENTOS VÍA DROPBOX
Emisión	02/12/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistema operativo Windows

Descripción

Turla es un grupo de ciberespionaje activo desde hace más de diez años. Chrutch backdoor cuenta con un conjunto de herramientas que fueron diseñadas para exfiltrar documentos confidenciales y otros archivos hacia cuentas de Dropbox controladas por los operadores de Turla. Los operadores estaban haciendo principalmente reconocimiento, movimiento lateral y espionaje.

La principal actividad maliciosa es la presentación, compresión y exfiltración de documentos y de varios archivos. La exfiltración se realiza mediante otro comando del backdoor y se cargaron archivos zip a las cuentas de Dropbox que controlan. Estos archivos zip contienen comandos para el backdoor y son subidos por los operadores a Dropbox de forma asincrónica desde el momento en que el backdoor lee y ejecuta su contenido.

El primer método consiste en utilizar un implante de primera etapa como Skipper. Luego, los operadores del malware comprometen otras máquinas en la red local moviéndose lateralmente. El segundo método es el uso de PowerShell Empire y los scripts de PowerShell Empire usan OneDrive y Dropbox.

La versión 3 de Crutch incluye un backdoor que se comunica con una cuenta de Dropbox hardcodeada utilizando la API HTTP oficial. Puede ejecutar comandos básicos como leer y escribir archivos, o ejecutar procesos adicionales. Persiste mediante el secuestro de la DLL en Chrome, Firefox o OneDrive. En algunas variantes notamos la presencia de canales de recuperación del C&C usando GitHub o un dominio regular. El segundo binario principal es un monitor de unidad extraíble que busca archivos que tengan una extensión interesante (.pdf, .rtf, .doc, .docx). Luego, coloca los archivos en un archivo cifrado.

Boletín	2020-399
Asunto	PAQUETES MALICIOSOS DE NPM USADOS PARA INSTALAR EL TROYANO NJRAT
Emisión	02/12/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistema operativo Windows

Descripción

NPM es un administrador de paquetes de JavaScript que permite a los desarrolladores y usuarios descargar paquetes e integrarlos en sus proyectos. NPM es un ecosistema abierto, cualquiera puede cargar un nuevo paquete sin ser revisado o analizado en busca de malware. Si bien este entorno ha dado lugar a un depósito de 1 millón de paquetes ricos y diversos, también facilita que los actores de amenazas carguen paquetes maliciosos.

Sonatype descubrió paquetes NPM maliciosos que se hacen pasar por una herramienta legítima para crear bases de datos a partir de archivos JSON, estos paquetes se llamaron 'jdb.js' y 'db-json.js' y NPM los eliminó, pero como puede ver en una captura de pantalla, parecen paquetes inofensivos que podrían usarse para agregar nuevas funciones a un proyecto como se puede ver en el archivo package.json para el paquete db-json.js, tiene otro paquete llamado 'jdb.js' como dependencia. El archivo package.json hace que NPM también instale automáticamente ese paquete al instalar el paquete db-json.js.

Este paquete jdb.js incluye un ejecutable module.js, package.json y patch.exe, cuando se instala, NPM ejecutará automáticamente module.js ya que está configurado para iniciarse automáticamente en la instalación. Este script JS está ofuscado, pero lanzará el ejecutable patch.exe, que es el malware njRAT, cuando se instala, njRAT brinda al actor de amenazas acceso remoto completo al equipo de la víctima, donde puede realizar los siguientes comportamientos maliciosos: modificar el registro de Windows, crea y elimina archivos, subir archivos, ejecutar comandos, obtener información sobre el equipo, toma el control del equipo, etc.

Boletín	2020-402
Asunto	ACTUALIZACIÓN: DEFECTO CRÍTICO DE ORACLE WEBLOGIC EXPLOTADO ACTIVAMENTE POR EL MALWARE DARKIRC
Emisión	03/12/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

- Oracle WebLogic Server

Descripción

El ataque emite una solicitud HTTP GET a un servidor WebLogic vulnerable, que ejecutará un script de PowerShell para descargar y ejecutar un archivo binario alojado en cnc[.]C25e6559668942[.]Xyz. La IP de origen es 83.97.20.90, esta IP se resuelve en el comando y control de este bot, lo que significa que la IP del atacante es la misma que el comando y control. Este payload es un archivo .NET con un tamaño de archivo de 6 MB. El presente boletín es una actualización del Boletín Nro. 2020-398.

El bot se instala en% APPDATA% \ Chrome \ Chrome.exe y crea una entrada de ejecución automática. Entre sus funciones destacan:

- Ladrón de navegador
- Registro de teclas
- Bitcoin Clipper
- DDoS
- Gusano o propagarse en la red
- Descargar archivos
- Ejecutar comandos

Bitcoin Clipper es una función que permite que el malware cambie la dirección de la billetera bitcoin copiada a la dirección de la billetera bitcoin del operador del malware. Básicamente, esto le permite robar transacciones de bitcoins en el sistema infectado.

Boletín	2020-431
Asunto	SKIMMER MEYHOD USADO EN SITIOS DE COMERCIO ELECTRÓNICO
Emisión	17/12/2020
CVE	No tiene
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Sitios web de comercio electrónico

Descripción

Los investigadores de RiskIQ denominaron Meyhod al skimmer utilizado en ataques en sitios de comercio electrónico, esto en honor a una función mal escrita en el código de skimming. Meyhod es simple en comparación con los skimmers Magecart, se indicó que es como la nueva variante del skimmer Grelos y el skimmer Ant and Cockroach. Sin embargo, Meyhod está cuidadosamente diseñado para mezclarse con la apariencia y las funciones de los sitios de las víctimas, lo que indica que los operadores experimentados de Magecart lo manejan.

El skimmer de Meyhod funciona agregando código a recursos JavaScript aparentemente benignos que van desde bibliotecas JavaScript de uso común hasta código personalizado. Estos recursos se han incrustado en el carrito y en las páginas de pago mediante etiquetas de script que podrían confundirse fácilmente con una llamada normal a una biblioteca.

Los operadores de Meyhod ofuscan su lógica de skimmer dividiéndola en más de una docena de funciones, a través de las cuales salta el flujo de control del código. Una de estas funciones, deflateMeyhod, le da a este skimmer su nombre debido al aparente error tipográfico de deflateMethod. Otra, saveData, intenta obtener datos de tarjetas de crédito a través de selectores de jQuery.

Los elementos del código del skimmer varían en los diferentes sitios de las víctimas, y los operadores parecen adaptarlos para que coincidan con los utilizados por cada sitio de la víctima. Los datos desnatados se codifican mediante funciones personalizadas antes de que se envíen al servidor propiedad del atacante mediante una solicitud POST AJAX.

Boletín	2020-428
Asunto	ATACANTES DE RANSOMWARE QUE UTILIZAN MALWARE DE SYSTEMBC CON RAT Y TOR PROXY
Emisión	16/12/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistema operativo Windows

Descripción

SystemBC se puede utilizar en combinación con otros scripts y malware para realizar el descubrimiento, la exfiltración y el movimiento lateral de forma automatizada a través de múltiples objetivos. Estas capacidades de SystemBC originalmente estaban destinadas a la explotación masiva, pero ahora se han incorporado al kit de herramientas para ataques, incluido el ransomware.

SystemBC es un malware proxy que aprovecha el protocolo de Internet SOCKS5 para enmascarar el tráfico a los servidores de comando y control (C2), y descargar el troyano bancario DanaBot. SystemBC RAT ha ampliado su conjunto de herramientas con nuevas características que le permiten usar una conexión Tor para cifrar y ocultar el destino de las comunicaciones C2, proporcionando así a los atacantes un backdoor persistente para lanzar otros ataques.

Los investigadores señalan que SystemBC se ha utilizado en una serie de ataques de ransomware, a menudo junto con otras herramientas posteriores a la explotación como CobaltStrike, para aprovechar su proxy Tor y las funciones de acceso remoto para analizar y ejecutar comandos de shell maliciosos, scripts VBS, BLOBs DLL enviados por el servidor a través de la conexión anónima y otros.

El aumento del malware de productos básicos también apunta a una nueva tendencia en la que el ransomware se ofrece como un servicio a los afiliados, como es el caso de MountLocker, donde los operadores brindan capacidades de doble extorsión a los afiliados para distribuir el ransomware con el mínimo esfuerzo.

Boletín	2020-403
Asunto	GRUPO APT SE ESCONDE DETRÁS DE LAS CAMPAÑAS DE CRIPTOMINERÍA
Emisión	03/12/2020
CVE	No tiene
Categoría	Ataque Cibernético
Severidad	Alta

Servicios Afectados

• Sistema operativo Windows

Descripción

La minería de monedas generalmente se considera un problema de seguridad no crítico, por lo que el método permitió al actor establecer la persistencia y moverse lateralmente en la red comprometida, al mismo tiempo que monetiza el ataque.

Bismuth se dirige regularmente a organizaciones de derechos humanos y civiles, su lista de víctimas incluye también empresas multinacionales, servicios financieros, instituciones educativas y entidades del sector gubernamental. El grupo ha estado ejecutando operaciones de ciberespionaje desde al menos 2012, sus ataques han aumentado en complejidad desde entonces, combinando herramientas personalizadas con herramientas disponibles gratuitamente.

Bismuth utilizó información de fuentes públicas para determinar sus objetivos y personalizar los mensajes, también utilizó la carga lateral de DLL, una técnica ampliamente utilizada que aprovecha la forma en que las aplicaciones de Windows manejan estos tipos de archivos para cargar una DLL maliciosa que falsifíca una legítima.

Boletín	2020-401
Asunto	CAMPAÑAS DE ATAQUES SOFISTICADOS Y DE LARGA DURACIÓN DEL GRUPO CICADA
Emisión	03/12/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistema operativo Linux con Docker instalado.

Descripción

Xanthe se descubrió por primera vez en una campaña que empleaba una botnet multimodular, así como un payload que es una variante del minero de criptomonedas XMRig Monero, el malware utiliza varios métodos para propagarse por la red, incluida la recolección de certificados del lado del cliente para propagarse a hosts conocidos a través de Secure Shell (SSH).

El actor mantiene activamente todos los módulos y ha estado activo desde marzo de este año. Se descubrió por primera vez a Xanthe apuntando a un honeypot, que investigadores crearon con el objetivo de descubrir las amenazas de Docker. Este es un servidor simple que emula ciertos aspectos de la API HTTP de Docker.

Xanthe, que lleva el nombre del título del archivo del script de propagación principal, usa un script de descarga inicial (pop[.]sh) para descargar y ejecutar su módulo de bot principal (xanthe[.]sh). Este módulo luego descarga y ejecuta cuatro módulos adicionales con varias funcionalidades de persistencia y anti-detección.

Estos cuatro módulos adicionales incluyen: Un módulo de ocultación de procesos (libprocesshider[.]so); un script de shell para deshabilitar otros mineros y servicios de seguridad (xesa[.]txt); un script de shell para eliminar los contenedores Docker de troyanos competidores de criptominería dirigidos a Docker (fczyo); y el binario XMRig (así como un archivo de configuración JSON, config[.]json).

Una vez descargado, el módulo principal también es responsable de propagarse a otros sistemas en redes locales y remotas intentando propagarse a otros hosts conocidos robando certificados del lado del cliente y conectándose a ellos sin el requisito de una contraseña.

Xanthe contiene una función de propagación, localgo, que comienza obteniendo una dirección IP visible externamente del host infectado (conectándose a icanhazip.com). Luego, el script usa una utilidad de "búsqueda" para buscar instancias de certificados del lado del cliente, que se usarán para la autenticación en hosts remotos.

Boletín	2020-405
Asunto	GRUPO DE ATACANTES CONTRATADOS UTILIZAN EL MALWARE POWERPEPPER
Emisión	04/12/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

- Sistema Operativo Windows

Descripción

PowerPepper es un backdoor de PowerShell en memoria de Windows que puede ejecutar comandos de shell enviados de forma remota. Siguiendo estrictamente la tradición de DeathStalker, el implante intentará evadir la detección o ejecución de sandboxes con varios trucos como, detectar movimientos del mouse, filtrar las direcciones MAC del cliente y adaptar su flujo de ejecución en función de los productos antivirus detectados.

Destaca la lógica de comando y control (C2) del implante, que se basa en comunicaciones vía DNS sobre HTTPS (DoH), utilizando respondedores CloudFlare, PowerPepper; primero intenta aprovechar Excel de Microsoft como cliente web para enviar solicitudes DoH a un servidor C2, pero recurrirá al cliente web estándar de powershell y, en última instancia, a las comunicaciones DNS regulares, si los mensajes no pueden llegar. El contenido de las comunicaciones C2 entre el implante y los servidores está cifrado. PowerPepper usa una implementación de PowerShell de cifrado AES casi idéntica, con solo el modo de relleno AES y un formato de entrada de función que se cambia.

PowerPepper sondea periódicamente un servidor C2 en busca de comandos para ejecutar. Para ello, el implante envía solicitudes DNS de tipo TXT (con solicitudes DoH o DNS simples si falla la primera) a los servidores de nombres (NS) que están asociados con un nombre de dominio C2 malicioso. Si el objetivo que ejecuta el implante está validado (lo cubriremos más adelante), el servidor responde con una respuesta de DNS, incrustando un comando cifrado. Tanto las solicitudes como las respuestas contienen patrones que pueden detectarse fácilmente con los sistemas de detección de intrusiones en la red, pero los patrones se han modificado en las variantes de implantes. Los investigadores lograron obtener una vista parcial de los países objetivo antes de agosto de 2020, así como en noviembre de 2020.

Boletín	2020-408
Asunto	TÍBET Y TAIWÁN SON OBJETO DE CAMPAÑAS DE SPEARPHISHING QUE UTILIZAN MALWARE MESSAGEMANIFOLD
Emisión	07/12/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

- Sistema operativo Windows

Descripción

La serie de correos electrónicos de spearphishing se centraron en invitaciones a conferencias y contenían un enlace de descarga directa de Google Drive. En total, se utilizaron dos enlaces de Google Drive, que descargaron ejecutables denominados "dalailama-Invitations.exe". En ambos casos, el ejecutable original muestra un mensaje de error de Windows falso y coloca un segundo ejecutable en la carpeta "C: \ Users \ Public" del dispositivo infectado. Los archivos eliminados realizan una solicitud Http POST al servidor de comando y control (C2) utilizando el siguiente patrón de URI “uu = kw & s = 1 & i =% & w =%”.

El malware requiere de una respuesta o un archivo específico del servidor C2 para crear la siguiente etapa. Insikt Group identificó coincidencias cercanas con la actividad dirigida a los legisladores taiwaneses informada por la Oficina de Investigación Criminal de Taiwán y Alienvault en mayo de 2020. Los investigadores creen que esta campaña probablemente fue realizada por el mismo grupo de actividad de amenazas que la reciente Orientación tibetana.

Insikt Group no ha identificado superposiciones con esta actividad ni con ningún grupo de actividad de amenaza conocido en este momento. Sin embargo, el objetivo de las entidades taiwanesas y tibetanas se alinea con los intereses estratégicos chinos, con muchos grupos de actividades de amenazas patrocinados por el estado chino, incluida RedAlpha, que se han dirigido fuertemente a estas entidades en el pasado. Del mismo modo, el carácter focalizado de estas campañas contra entidades de alta importancia estratégica, junto con el bajo volumen de actividad vinculada al grupo dentro del dominio público, es incompatible con la actividad motivada financieramente.

Boletín	2020-407
Asunto	PHISHING DE METAMASK ROBA BILLETERAS DE CRIPTOMONEDAS A TRAVÉS DE ANUNCIOS DE GOOGLE
Emisión	05/12/2020
CVE	No tiene
Categoría	Phishing
Severidad	Alta

Servicios Afectados

- Sistema Operativo Windows

Descripción

MetaMask tiene una comunidad de más de un millón de usuarios, el sitio ofrece una billetera de criptomonedas Ethereum en el navegador a través de una extensión del navegador que permite que las aplicaciones distribuidas lean desde la cadena de bloques. Al instalar la extensión legítima, puede importar una billetera existente o crear una nueva junto con la frase semilla secreta que permite el acceso a la billetera.

La estafa de phishing / publicidad todavía está activa, con un nuevo dominio que se promociona constantemente a través de los anuncios de búsqueda de Google. MetaMask alertó a su comunidad sobre la estafa y recomendó el uso de enlaces directos a la URL legítima de metamask.io y mantenerse alejado de los anuncios patrocinados.

Se determinó que los usuarios iban a una página falsa de phishing MetaMask a través de anuncios de Google. Una vez en la página, se les pedirá que instalen la extensión, lo que les dará la opción de importar una billetera existente o crear una nueva.

Boletín	2020-412
Asunto	CAMPAÑA DE PHISHING SE DIRIGE A 200 MILLONES DE CUENTAS DE MICROSOFT 365
Emisión	09/12/2020
CVE	No tiene
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Microsoft Office 365

Descripción

Esta campaña de phishing a gran escala está dirigida a 200 millones de usuarios de Microsoft 365 en todo el mundo, particularmente en los sectores de servicios financieros, atención médica, seguros, fabricación, servicios públicos y telecomunicaciones.

Los atacantes aprovechan una técnica de suplantación de dominio para crear correos electrónicos que parecen provenir de Microsoft Outlook (no-reply@microsoft[.]com). Estos correos electrónicos intentan usar un lenguaje urgente para engañar a las personas para que utilicen una nueva capacidad de Microsoft 365 permitiendo a los titulares de cuentas reclamar correos electrónicos marcados accidentalmente como phishing o spam.

Un vínculo dentro del correo electrónico promete redirigir a los lectores a un portal de seguridad para que puedan revisar y actuar en los llamados "mensajes de cuarentena" considerados sospechosos por la pila de filtrado de Exchange Online Protection (EOP). A las víctimas que hagan clic en el enlace se les pedirá que ingresen sus credenciales de inicio de sesión de Microsoft en una página de autenticación falsa. Algunos grupos de APT pueden adquirir credenciales de administrador para vulnerar un entorno de destino de Microsoft 365.

Boletín	2020-415
Asunto	NUEVA BOTNET DE MINERÍA DE CRIPTOMONEDAS PGMINE ENTREGADA A TRAVÉS DE POSTGRESQL
Emisión	10/12/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistema operativo Windows, Linux, Unix y programa PostgreSQL

Descripción

PostgreSQL, también conocido como Postgres, se encuentra entre los sistemas de administración de bases de datos relacionales (RDBMS) de código abierto más utilizados para entornos de producción. Se cree que PGMiner es la primera botnet de minería de criptomonedas que se entrega a través de PostgreSQL. Es notable que los actores de malware hayan comenzado a armar no solo los CVE confirmados, sino también los controvertidos.

El payload malicioso se entrega a través de PostgreSQL, que se comunica con los servidores backend C2 a través de proxies SOCKS5. Después de eso, descarga los payloads de minería de monedas según la arquitectura del sistema. Se encontró que PGMiner se reproduce constantemente descargando ciertos módulos de forma recursiva. Una vez que el malware irrumpe con éxito en la base de datos, utiliza la función "copiar desde el programa" de PostgreSQL para descargar y ejecutar los scripts de minería de monedas. La función "copiar desde el programa" ha sido controvertida desde su debut en PostgreSQL 9.3. La función permite que el superusuario local o remoto ejecute un script de shell directamente en el servidor, lo que ha generado una gran preocupación por la seguridad.

En 2019, se asignó un CVE-2019-9193 a esta función, nombrándola como una "vulnerabilidad". Sin embargo, la comunidad de PostgreSQL impugnó esta asignación y el CVE ha sido etiquetado como "disputado". El principal argumento en contra de definir la característica como una vulnerabilidad es que la característica en sí no impone un riesgo siempre que el privilegio de superusuario no se otorgue a usuarios remotos o no confiables, y el sistema de autenticación y control de acceso funcione bien.

Boletín	2020-419
Asunto	RANSOMWARE MOUNTLOCKER AHORA CIFRA MENOS ARCHIVOS
Emisión	11/12/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

- Sistema Operativo Windows

Descripción

La operación de ransomware comenzó en julio de 2020 y está dirigida a redes corporativas, sus operadores roban datos antes de cifrarlos y amenazan a las víctimas con filtrar archivos a menos que se cumplan sus demandas multimillonarias de rescate. En la segunda quincena de noviembre, los investigadores de malware vieron la segunda versión de MountLocker con pistas de que sus operadores se están preparando para la temporada de impuestos.

MountLocker cifra los archivos en las computadoras infectadas usando el cifrado de flujo ChaCha20 y luego la clave de sesión se cifra con una clave pública RSA de 2048 bits incrustada en su código. El equipo de investigación de BlackBerry señala que la nueva variante MountLocker viene con una marca de tiempo de compilación del 6 de noviembre del 2020. Los desarrolladores de malware redujeron el tamaño de la variante de malware de 64 bits a 46 KB, que es aproximadamente un 50% más pequeño que la versión anterior. Para llegar a esto, eliminaron la lista de extensiones de archivo con más de 2600 entradas destinadas al cifrado.

El malware apunta ahora a una lista mucho más pequeña que excluye tipos de archivos fácilmente reemplazables: .EXE, .DLL, .SYS, .MSI, .MUI, .INF, .CAT, .BAT, .CMD, .PS1, .VBS, .TTF, .FON, .LNK. El nuevo código es muy similar al anterior, el mayor cambio es el proceso para eliminar instantáneas de volumen y para finalizar procesos, que ahora se realiza con el script de PowerShell antes de cifrar los archivos.

BlackBerry dice que el 70% del código en el nuevo MountLocker es el mismo que en la versión anterior, incluida la función insegura de la API de Windows GetTickCount del malware para generar una clave de cifrado aleatoria. Los investigadores añaden que el éxito de este esfuerzo depende de conocer el valor del contador de la marca de tiempo durante la ejecución del ransomware.

Boletín	2020-418
Asunto	RANSOMWARE ATACA 85K SERVIDORES MYSQL
Emisión	11/12/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

- Sistema Operativo Windows

Descripción

Se observaron por primera vez los ataques PLEASE_READ_ME en enero del 2020. En esta primera fase, las víctimas debían transferir BTC directamente a la billetera del atacante. La segunda fase de la campaña de ransomware comenzó en octubre. En la segunda fase, el ataque se convirtió en un intento de doble extorsión, dicen los investigadores, lo que significa que los atacantes están publicando datos mientras presionan a las víctimas para que paguen el rescate. Los ataques de ransomware han continuado golpeando hospitales, escuelas y otras organizaciones en 2020. Se cree que los operadores PLEASE_READ_ME están tratando de mejorar su ataque mediante el uso de doble extorsión a escala.

El ataque explota credenciales débiles en servidores MySQL conectados a Internet, de los cuales hay cerca de 5 millones en todo el mundo. Desde que observaron por primera vez la campaña de ransomware en enero, los investigadores dijeron que los atacantes han cambiado sus técnicas para presionar más a las víctimas y automatizar el proceso de pago del rescate.

El ataque comienza con una contraseña de fuerza bruta en el servicio MySQL. Una vez que tiene éxito, el atacante ejecuta una secuencia de consultas en la base de datos, recopilando datos sobre las tablas y los usuarios existentes. Al final de la ejecución, los datos de la víctima desaparecen, se archivan en un archivo comprimido que se envía a los servidores de los atacantes y luego se eliminan de la base de datos.

A partir de ahí, el atacante deja una nota de rescate en una tabla, llamada "ADVERTENCIA", que exige un pago de rescate de hasta 0.08 BTC. La nota de rescate dice a las víctimas: “Sus bases de datos se descargan y se respaldan en nuestros servidores. Si no recibimos su pago en los próximos 9 días, venderemos su base de datos al mejor postor o la usaremos de otra manera”.

Boletín	2020-417
Asunto	CAMPAÑA DE MALWARE ADROZEK ATACÓ NAVEGADORES CHROME, FIREFOX
Emisión	11/12/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

- Sistema Operativo Windows

Descripción

La campaña, que afecta a los navegadores Microsoft Edge, Google Chrome y Mozilla Firefox en Windows, tiene como objetivo insertar anuncios adicionales no autorizados en la parte superior de los anuncios legítimos que se muestran en las páginas de resultados de los motores de búsqueda, lo que lleva a los usuarios a hacer clic a estos anuncios sin darse cuenta.

Microsoft indicó que el malware Adrozek modificador de navegador persistente se ha observado desde mayo de este año, con más de 30.000 dispositivos afectados todos los días en su punto máximo en agosto.

Este malware Adrozek emplea una infraestructura de atacantes dinámica y expansiva que consta de 159 dominios únicos, cada uno de los cuales alberga un promedio de 17.300 URL únicas, que a su vez albergan más de 15.300 malware único.

Una vez que se suelta, instala en los sistemas de destino a través de descargas no autorizadas, Adrozek procede a realizar varios cambios en la configuración del navegador y los controles de seguridad para instalar complementos maliciosos que se hacen pasar por genuinos al reutilizar los ID de extensiones legítimas.

Aunque los navegadores actuales tienen controles de integridad para evitar la manipulación, el malware deshabilita inteligentemente la función, lo que permite a los atacantes eludir las defensas de seguridad y explotar las extensiones para obtener scripts adicionales de servidores remotos para inyectar anuncios falsos y obtener ingresos al dirigir el tráfico a estos anuncios fraudulentos. páginas.

Boletín	2020-421
Asunto	GRUPO APT28 USA SEÑUELOS COVID-19 PARA ENTREGAR MALWARE DE ZEBROCY
Emisión	12/12/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

- Sistema Operativo Windows

Descripción

El señuelo consistió en el documento sobre Sinopharm International Corporation, una compañía farmacéutica, en el documento se indica que la vacuna COVID-19 está pasando actualmente por pruebas clínicas de fase tres. Zebrocy es un malware utilizado por el grupo de amenazas Sofacy, también conocido como Sednit, APT28, Fancy Bear y STRONTIUM. Zebrocy funciona como un descargador y recopila información sobre el host infectado que se carga en el servidor de comando y control (C&C) antes de descargar y ejecutar la etapa siguiente.

La primera versión del descargador se escribió en Delphi y se basó en un malware anterior utilizado por Sofacy. Zebrocy muestras escritas en AutoIT, C ++, C #, Delphi, Go, y VB.NET. La entrega de Zebrocy suele realizarse a través de un correo electrónico de phishing. El correo electrónico incluye documentos o archivos de archivo de Microsoft Office.

Intezer descubrió un archivo de disco duro virtual (VHD) llamado 30-22-243.vhd, VHD es el formato de archivo nativo para discos duros virtuales que utiliza el hipervisor de Microsoft, Hyper-V. Si el usuario hace doble click en el archivo, Windows montará la unidad y aparecerá como un disco duro externo.

Boletín	2020-423
Asunto	CREDENCIALES DE MICROSOFT OFFICE 365 BAJO ATAQUE POR CORREO ELECTRÓNICO DE ALERTA DE FAX
Emisión	14/12/2020
CVE	No tiene
Categoría	Phishing
Severidad	Alta

Servicios Afectados

- Sistema Operativo Windows

Descripción

Los diferentes verticales señalados por el actor de la amenaza incluyen instituciones gubernamentales, financieras, energéticas, alimentarias, sanitarias, educativas, informáticas y legales ubicadas en Chile, Chipre, Alemania, Indonesia, Italia, Singapur, Suiza, Turquía y Estados Unidos.

El uso extensivo de Dark Caracal de Bandook RAT para ejecutar espionaje a escala global fue documentado por primera vez por Electronic Frontier Foundation (EFF) y Lookout a principios de 2018. La cadena de infección es un proceso de tres etapas que comienza con un documento atractivo de Microsoft Word entregado dentro de un archivo ZIP que, cuando se abre, descarga macros maliciosas, que posteriormente procede a soltar y ejecutar una segunda etapa secuencia de comandos de PowerShell cifrada dentro del documento de Word original.

En la última fase del ataque, este script de PowerShell se utiliza para descargar partes ejecutables codificadas de servicios de almacenamiento en la nube como Dropbox o Bitbucket para ensamblar el cargador Bandook, que luego asume la responsabilidad de inyectar el RAT en un nuevo proceso de Internet Explorer. El Bandook RAT, disponible comercialmente a partir de 2007, viene con todas las capacidades típicamente asociadas con los backdoors, ya que establece contacto con un servidor controlado de forma remota para recibir comandos adicionales que van desde capturar capturas de pantalla hasta realizar varias operaciones relacionadas con archivos.

Boletín	2020-413
Asunto	AUMENTO DE ATAQUES DE BOTNET PHORPIEX EN CAMPAÑAS MALICIOSAS DE SPAM
Emisión	09/12/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

- Sistema Operativo Windows

Descripción

La botnet Phorpiex se informó por primera vez en 2010 y en su apogeo controlaba más de un millón de hosts infectados. Phorpiex, conocido por distribuir otras familias de malware a través del spam y por impulsar campañas de spam de sextorsión a gran escala y criptominería, ha vuelto a distribuir el ransomware Avaddon, como se observó a principios del año 2020. Avaddon es una variante relativamente nueva de Ransomware-as-a-Service (RaaS), y sus operadores han estado nuevamente reclutando afiliados para distribuir el ransomware por una parte de las ganancias. Avaddon se ha distribuido a través de archivos JS y Excel como parte de campañas de malspam y puede cifrar una amplia gama de tipos de archivos.

Phorpiex es una de las botnets más antiguas y persistentes, y sus creadores la han utilizado durante muchos años para distribuir otros payloads de malware, como el ransomware GandCrab y Avaddon, o para estafas de sextorsión. Los investigadores de CheckPoint indicaron que esta nueva ola de infecciones ahora está extendiendo otra campaña de ransomware, que muestra cuán efectiva es una herramienta Phorpiex. Phorpiex es el malware más popular con un impacto global del 4% de las organizaciones, seguido de cerca por Dridex e Hiddad, que afectaron al 3% de las organizaciones en todo el mundo.

1. Phorpiex: Es una botnet conocida por distribuir otras familias de malware a través de campañas de spam, así como por impulsar campañas de Sextortion a gran escala.

2. Dridex: Es un troyano que se dirige a la plataforma Windows y, según se informa, se descarga a través de un archivo adjunto de correo electrónico no deseado. Dridex contacta a un servidor remoto y envía información sobre el sistema infectado. También puede descargar y ejecutar módulos arbitrarios recibidos del servidor remoto.

3. Hiddad: Es una infección de malware de Android que vuelve a empaquetar aplicaciones móviles legítimas, y luego las libera en una tienda de terceros. Su función principal es mostrar anuncios, pero también puede obtener acceso a detalles clave de seguridad integrados en el sistema operativo.

Boletín	2020-422
Asunto	CISA EMITE UNA DIRECTIVA DE EMERGENCIA PARA MITIGAR EL COMPROMISO DEL CÓDIGO DE SOLARWINDS ORION
Emisión	14/12/2020
CVE	No tiene
Categoría	Ataque Cibernético
Severidad	Alta

Servicios Afectados

• Sistema operativo Windows

Descripción

Esta campaña puede haber comenzado en la primavera de 2020 y actualmente está en curso. Por ello, la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) emitió una Directiva de Emergencia 21-01, en respuesta a un compromiso conocido que involucra productos SolarWinds Orion que actualmente están siendo explotados por actores maliciosos para las versiones 2019.4 HF 5 hasta 2020.2.1, lanzadas entre marzo de 2020 y junio de 2020.

FireEye ha detectado esta actividad en múltiples entidades en todo el mundo. Las víctimas han incluido entidades gubernamentales, de consultoría, tecnología, telecomunicaciones y extractivas en América del Norte, Europa, Asia y Medio Oriente. Anticipan que habrá víctimas adicionales en otros países y verticales. FireEye ha notificado a todas las entidades que sabemos que se han visto afectadas.

SolarWinds[.]Orion[.]Core[.]BusinessLayer[.]dll es un componente firmado digitalmente de SolarWinds del marco de software de Orion que contiene una puerta trasera que se comunica a través de HTTP a servidores de terceros. Una vez instalada la actualización, el archivo DLL malicioso será cargado por SolarWinds.BusinessLayerHost.exe o SolarWinds.BusinessLayerHostx64.exe legítimo (según la configuración del sistema). Y después de un período de inactividad inicial de hasta dos semanas, recupera y ejecuta comandos, llamados "jobs", que incluyen la capacidad de transferir archivos, ejecutar archivos, perfilar el sistema, reiniciar la máquina y deshabilitar los servicios del sistema. El malware disfraza su tráfico de red como el protocolo del Programa de mejora de Orion (OIP) y almacena los resultados del reconocimiento en archivos de configuración de complementos legítimos, lo que le permite integrarse con la actividad legítima de SolarWinds.

Boletín	2020-425
Asunto	BOTNET WORMABLE GITPASTE-12 REGRESA A LOS SERVIDORES LINUX Y DISPOSITIVOS IOT
Emisión	15/12/2020
CVE	Varios
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistema operativo Windows

Descripción

A principios del mes pasado, los investigadores de Juniper Threat Labs documentaron una campaña de minería criptográfica llamada "Gitpaste-12", que utilizaba GitHub para alojar código malicioso que contenía hasta 12 módulos de ataque conocidos, ejecutándose mediante comandos descargados desde una URL de Pastebin.

Los ataques ocurrieron durante un período de 12 días a partir del 15 de octubre de 2020, antes de que tanto la URL de Pastebin como el repositorio se cerrarán el 30 de octubre de 2020. Y ahora, según indica Juniper, la segunda ola de ataques comenzó el 10 de noviembre, utilizando payloads de un repositorio de GitHub diferente, que, entre otros, contiene un criptominero de Linux ("ls"), un archivo con una lista de contraseñas para fuerza bruta y un exploit de escalamiento de privilegios local para sistemas Linux x86_64.

La infección inicial ocurre a través de X10-unix, un binario escrito en el lenguaje de programación Go, que procede a descargar los payloads de la siguiente etapa desde GitHub.

Este lleva a cabo una amplia serie de ataques dirigidos a aplicaciones web, cámaras IP, routers y más, que comprenden al menos 31 vulnerabilidades conocidas, siete de las cuales también se observaron en la muestra anterior de Gitpaste-12.

En la lista de 31 vulnerabilidades se incluyen fallas de código remoto en la interfaz de usuario de administración de tráfico F5 BIG-IP (CVE-2020-5902), Pi-hole Web (CVE-2020-8816), Tenda AC15 AC1900 (CVE-2020-10987) y vBulletin (CVE-2020-17496), y un error de inyección SQL en FUEL CMS (CVE-2020-17463), todos los cuales salieron a la luz este año.

Boletín	2020-424
Asunto	NUEVO TROYANO PARA WINDOWS ROBA LAS CREDENCIALES DEL NAVEGADOR Y LOS ARCHIVOS DE OUTLOOK
Emisión	15/12/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistema operativo Windows

Descripción

El troyano, llamado PyMicropsia debido a que fue construido con Python ha sido desarrollado por el grupo de amenazas AridViper, que es conocido por atacar organizaciones en el Medio Oriente. Las capacidades de robo de información del troyano incluyen carga de archivos, descarga/ejecución de payloads, robo de credenciales del navegador, tiene la capacidad de borrar el historial y los perfiles de navegación, tomar capturas de pantalla y hacer keylogging. Además, el malware puede recopilar información de listas de archivos, eliminar archivos, reiniciar equipos, recopilar información de la unidad USB y grabar audio; así como recolectar archivos .OST de Outlook y eliminar/deshabilitar los procesos de Outlook.

El troyano ha sido convertido en un ejecutable de Windows por PyInstaller, un paquete de Python que permite que las aplicaciones se conviertan en ejecutables independientes. Una vez descargado, el malware implementa su funcionalidad principal ejecutando un bucle, donde inicializa diferentes hilos y llama a varias tareas periódicamente con la intención de recolectar información e interactuar con el operador de comando y control (C2). El actor de amenazas utiliza tanto bibliotecas Python integradas como paquetes específicos para fines de robo de información, incluido PyAudio que habilita capacidades de robo de audio y mss que permite capacidades de captura de pantalla.

PyMicropsia tiene relación con la familia de malware Micropsia, otro malware AridViper conocido por apuntar a Microsoft Windows. Estos enlaces incluyen superposiciones de código; tácticas, técnicas y procedimientos (TTP) similares, como el uso de rar.exe para comprimir datos para su exfiltración; y estructuras de ruta URI de comunicación C2 similares. En las variables de código de PyMicropsia, se encontraron referencias a múltiples nombres de actores famosos, entre ellos los actores Fran Drescher y Keanu Reeves.

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.