SECURESOFT CORPORATION
e-Secure Consulting Group

Reporte Quincenal de Ciberinteligencia Securesoft

Fecha:

26 Octubre de 2020

El presente documento contiene información para la comunidad de ciberseguridad.

Equipo de Ciberinteligencia

CIB-FOR-2020-011

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

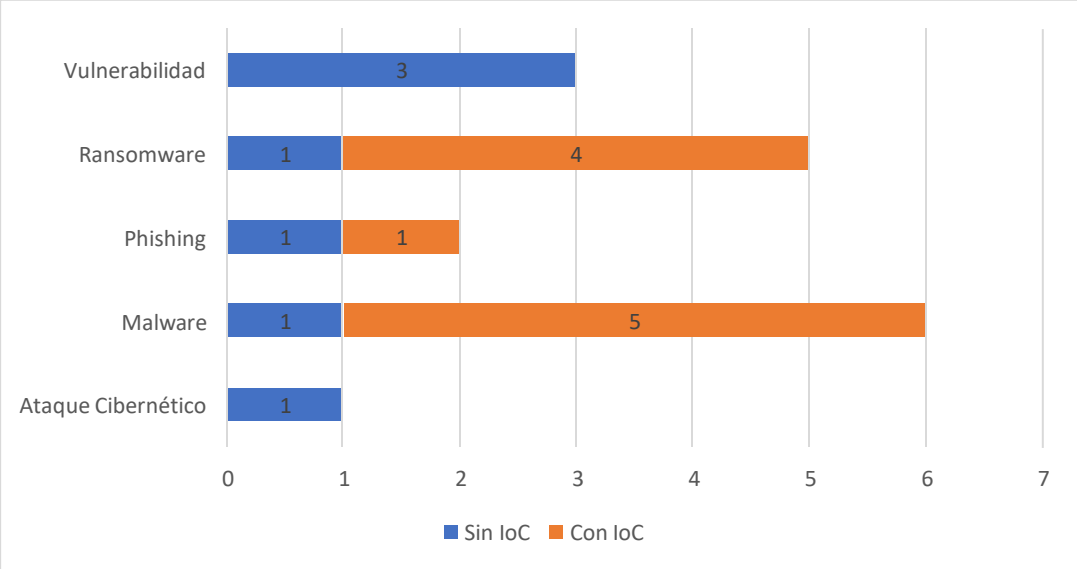
Este documento muestra el resumen, la fecha de publicación, CVE asociado y servicios afectados de vulnerabilidades y amenazas que se han hecho públicas en el transcurso del 08 de octubre hasta el 22 de octubre del 2020.

3. Resumen

En el presente informe se exponen 17 análisis de vulnerabilidad y amenazas, de las cuales 16 tienen una severidad Alta y uno severidad Crítica.

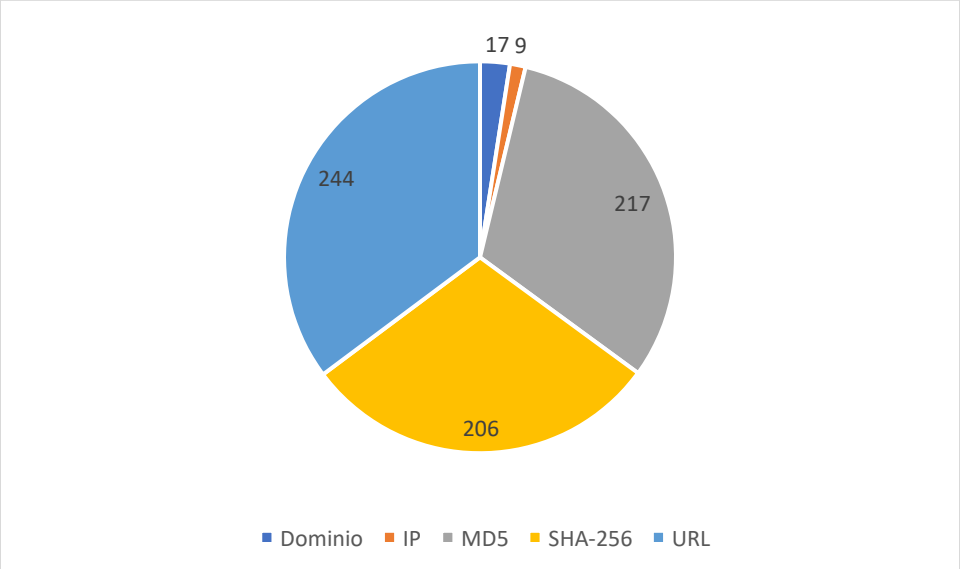
Amenazas analizadas por tipología

En las investigaciones elaboradas para el presente informe se trataron vulnerabilidades, 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 637 IoCs entre Dominios, URL, IP, MD5 y SHA256.



Tendencias en nuevas vulnerabilidades

- De acuerdo con nuestras fuentes de inteligencia, VMware reveló seis vulnerabilidades que afectan a sus productos ESXi, Workstation, Fusion, Cloud Foundation y NSX-T. El CVE-2020-3992 que encabeza la lista con una clasificación de gravedad CVSS de 9,8 sobre 10, es una vulnerabilidad de use-after-free en el hipervisor ESXi que puede explotarse a través de la red para ejecutar código malicioso en el host de destino. Para más información leer el Boletín 2020-318, donde podrá encontrar la actualización para estas vulnerabilidades.
- De acuerdo con nuestras fuentes de inteligencia, Microsoft realizó un lanzamiento de actualizaciones de seguridad del mes de octubre, donde publicó actualizaciones para 28 vulnerabilidades. De las cuales dos son consideradas como críticas, veinticinco como importantes y una como moderada. Para más información leer el Boletín 2020-309, en la cual podrá encontrar la actualización de las vulnerabilidad.
- De acuerdo con nuestras fuentes de inteligencia, Cisco publicó una actualización de seguridad para una vulnerabilidad CVE-2020-3118, considerada de alta severidad para el software Cisco IOS XR que permite a los atacantes ejecutar código arbitrario en el dispositivo afectado. Para más información leer el Boletín 2020-317, donde encontrará la actualización para esta vulnerabilidad.

Actividades maliciosas asociadas a grupo de cibercriminales

- FIN11 es un actor de amenazas con motivaciones económicas conocido por sus campañas de distribución de malware y recientemente se ha centrado en el desarrollo de nuevas tácticas en infección de ransomware y extorsión. De acuerdo con el equipo de inteligencia de amenazas Mandiant de FireEye, el grupo FIN11 se ha involucrado en un patrón de campañas de ciberdelincuencia al menos desde 2016, que implica monetizar su acceso a las redes de las organizaciones, además de implementar malware en POS (Punto de Venta). Dirigido a los sectores financiero, minorista, restaurante y farmacéutico, para más información leer Boletín 2020-308.

4. Detalles

Vulnerabilidades

Boletín	2020-309
Asunto	ACTUALIZACIONES DE SEGURIDAD DE MICROSOFT - OCTUBRE DE 2020
Emisión	14/10/2020
CVE	CVE-2020-16898 y otros
Categoría	Vulnerabilidad
Severidad	Crítico

Servicios Afectados

- Microsoft Windows
- Microsoft Office, Microsoft Office Services y Web Apps
- Microsoft JET Database Engine
- Azure Functions
- Open Source Software
- Microsoft Exchange Server
- Visual Studio
- PowerShellGet
- Microsoft .NET Framework
- Microsoft Dynamics
- Adobe Flash Player
- Microsoft Windows Codecs Library

Descripción

La vulnerabilidad de ejecución remota de código (RCE) asignada al CVE-2020-16898 permite que los atacantes se apoderen de los sistemas Windows, enviando paquetes maliciosos de anuncios de enrutador ICMPv6 a una computadora sin parches a través de una conexión de red.

La vulnerabilidad asignada al CVE-2020-16947 permite aprovechar engañando a un usuario para que abra un archivo especialmente diseñado con una versión afectada del software Microsoft Outlook.

Actualización o Mitigación

Para las recomendaciones y actualizaciones revisar el siguiente link.

Boletín	2020-318
Asunto	VULNERABILIDADES EN PRODUCTOS DE VMWARE
Emisión	22/10/2020
CVE	Varios
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

- VMware ESXi
- VMware Workstation Pro/Player (Workstation)
- VMware Fusion Pro/Fusion (Fusion)
- NSX-T
- VMware Cloud Foundation

Descripción

VMware reveló seis vulnerabilidades que afectan a sus productos ESXi, Workstation, Fusion, Cloud Foundation y NSX-T. El CVE-2020-3992 que encabeza la lista con una clasificación de gravedad CVSS de 9,8 sobre 10, es una vulnerabilidad de use-after-free en el hipervisor ESXi que puede explotarse a través de la red para ejecutar código malicioso en el host de destino.

Actualización o Mitigación

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

Boletín	2020-317
Asunto	CISCO PUBLICA ACTUALIZACIÓN DE SEGURIDAD
Emisión	22/10/2020
CVE	CVE-2020-3118
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Sistema operativo Cisco

Descripción

La vulnerabilidad se debe a una validación incorrecta de la entrada de cadenas de ciertos campos en los mensajes en un protocolo de capa 2. Un atacante podría aprovechar esta vulnerabilidad enviando un paquete de Cisco Discovery Protocol malicioso a un dispositivo afectado, y permitir que un atacante adyacente no autenticado ejecute código arbitrario o provoque una recarga en un dispositivo afectado. Esta vulnerabilidad afecta a todos los productos de routers de white box de Cisco y otros terceros que tienen habilitado el protocolo.

Actualización o Mitigación

Todos los fallos de seguridad han sido solucionados y se recomienda descargar las últimas actualizaciones de software aquí.

Amenazas

Boletín	2020-308
Asunto	GRUPO DE HACKERS FIN11 USA NUEVAS TÉCNICAS EN ATAQUES DE RANSOMWARE
Emisión	14/10/2020
CVE	No tiene
Categoría	Ataque Cibernético
Severidad	Alta

Servicios Afectados

• Sistema operativo Windows

Descripción

El equipo de Mandiant indicó que existe una superposición significativa en los TTP con otro grupo de amenazas que los investigadores de ciberseguridad llaman TA505, que está detrás del troyano bancario Dridex y el ransomware Locky que se entrega a través de campañas de malspam en la botnet Necurs, sin embargo Microsoft orquestó la eliminación de la botnet Necurs a principios de marzo, en un intento de evitar que los operadores registren nuevos dominios para ejecutar más ataques en el futuro.

FIN11, además de aprovechar un mecanismo de distribución de correo electrónico malicioso de alto volumen, ha ampliado su orientación a los señuelos del idioma nativo junto con la información del remitente del correo electrónico manipulada, como los nombres para mostrar y las direcciones del remitente del correo electrónico falsificados, para que los mensajes parezcan más legítimos, con una fuerte inclinación a atacar a las organizaciones alemanas en sus campañas de 2020. También se desencadenó una campaña de correo electrónico con asuntos como "informe de investigación N-[número de cinco dígitos]" y "accidente de laboratorio" en enero de 2020, seguido de una segunda ola en marzo utilizando correos electrónicos de phishing con el asunto ". [nombre de la empresa farmacéutica] Hoja de cálculo de facturación 2020 YTD ".

Según la investigación de Mandiant, las operaciones de FIN11 parecen haber cesado por completo desde mediados de marzo de 2020 hasta finales de mayo de 2020, antes de recuperarse en junio a través de correos electrónicos de phishing que contienen archivos adjuntos HTML maliciosos para entregar archivos maliciosos de Microsoft Office. Los archivos de Office, a su vez, utilizaron macros para recuperar el dropper MINEDOOR y el descargador FRIENDSPEAK, que luego envió el backdoor MIXLABEL al dispositivo infectado.

Boletín	2020-315
Asunto	ESTAFAS DE PHISHING USAN REDIRECCIONAMIENTOS PARA ROBAR CREDENCIALES DE OFFICE 365 Y FACEBOOK
Emisión	21/10/2020
CVE	No tiene
Categoría	Phishing
Severidad	Alta

Servicios Afectados

- Sistema operativo Windows
- Cuentas de Office 365
- Cuentas de Facebook

Descripción

Estas campañas se encuentran activas desde hace una semana, con un gran aumento a partir del 15 de octubre, la operación de Office 365 ha llegado a decenas de miles de bandejas de entrada a través de múltiples campañas conectadas que falsifican aplicaciones conocidas como Microsoft Office, Microsoft Teams y Zoom con el fin de que los usuarios sean engañados para entregar sus nombres de usuario y contraseñas. Entre los objetivos de la operación se han identificado altos ejecutivos y personal financiero, la estafa también tiene como objetivo infectar a las víctimas con JavaScript diseñado para implementar varios malware, incluido el troyano Cryxos.

Las víctimas que hacen click en los enlaces maliciosos de los correos electrónicos son redireccionados directamente al kit de phishing, que parece una página de inicio de sesión, o se dirigen allí a través de dominios redirectores abiertos y los restos subsidiarios que los atacantes han comprometido de marcas globales como Sony, TripAdvisor, RAC, DigitalOcean y Google.

La operación de phishing de Facebook, descubierta por Cyberint, identificó que el señuelo llegaría a través de Facebook Messenger de un contacto conocido cuya cuenta ya ha sido abusada. La comunicación sugiere que el destinatario se parece a la misma persona en un video de YouTube, lo que podría atraer a la víctima potencial a hacer clic en el enlace y ver el video. El enlace en realidad lleva a las víctimas a una página de inicio de sesión de Facebook falsa para que los usuarios ingresen sus credenciales para que puedan ser robadas. Una vez que se completa la estafa de phishing, la víctima es redirigida nuevamente al sitio legítimo de Google Play Store. De acuerdo con lo indicado por Cyberint, Facebook cerró el ataque después de que la compañía fuera notificada del problema.

Boletín	2020-302
Asunto	NUEVA FAMILIA DE RANSOMWARE: EGREGOR
Emisión	08/10/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistema operativo Windows

Descripción

El ransomware Egregor fue detectado por primera vez a mediados de septiembre, se conoce que al menos 13 empresas diferentes fueron afectadas, dentro de las cuales se encuentra incluida la empresa de logística global GEFCO, que sufrió un ciberataque la semana pasada. Se estima que en base a las muestras este malware se ha localizado en Italia, Francia, México, Alemania, Japón, Arabia Saudita y EE. UU.

Se cree que es un derivado del ransomware Sekhmet; ya que, tienen varias similitudes incluidas llamadas a la API, funciones, técnicas de ofuscación y una nota de rescate similar. Además, Egregor puede recibir parámetros adicionales a través de la línea de comandos, como 'nomimikatz', 'killrdp', 'norename', entre otros.

El grupo de ciberatacantes detrás de este malware roba datos confidenciales y luego continúa ejecutando Egregor para cifrar todos los archivos y luego indicar a las víctimas que sus datos afectados serán publicados en un sitio web de noticias en la dark web, en caso de que no se haga efectivo el pago de rescate. Además de esto, implementan una gran cantidad de técnicas anti-análisis, ofuscación de código y cifrado de payload.

Boletín	2020-303
Asunto	AUMENTO DE ATAQUES DE RANSOMWARE EN LOS ÚLTIMOS MESES
Emisión	08/10/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

- Sistema operativo Windows

Descripción

Una de las razones por las que los ataques de ransomware están en aumento es debido al cambio en la forma de trabajo, el trabajo remoto que ha obligado a muchas personas a trabajar desde casa por primera vez, por lo que los hace más vulnerables a los correos electrónicos de phishing y los ataques de malware, especialmente con una red en casa que probablemente no sea tan segura como un entorno empresarial.

Investigar y restaurar la red después de un ataque de ransomware puede llevar semanas o meses, y cuando esto se combina con empleados que trabajan de forma remota, algunas organizaciones simplemente prefieren ceder a las demandas de rescate y pagar cientos de miles o incluso millones de dólares en bitcoins para restaurar su red lo más rápido posible.

Check Point identificó al ransomware Ryuk como una de las familias de ransomware más prolíficas en los últimos meses, y el número de ataques de Ryuk aumentó a alrededor de 20 por semana. Por otra parte, el grupo de respuesta a incidentes IBM Security X-Force señala que las amenazas de ransomware parecieron explotar en junio de 2020, cuando estos ataques llegaron a ser un tercio de todos los eventos de este tipo registrados hasta septiembre, a fines de septiembre, informaron que Maze representó el 12% de todos los ataques de ransomware.

El tercer ransomware más frecuente que IBM observó en 2020 es EKANS (Snake), responsable del 6% de los incidentes, que puede terminar procesos relacionados con las operaciones del sistema de control industrial (ICS).

Boletín	2020-304
Asunto	CAMPAÑA LEMON_DUCK POWERSHELL EN REDES EMPRESARIALES
Emisión	09/10/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

- Sistema operative Windows

Descripción

El criptominer Lemon Duck es uno de los tipos más avanzados de payload debido a que actualizan continuamente el código con nuevos vectores de amenazas y técnicas de ofuscación para evadir la detección. Las computadoras infectadas con este minero también pueden convertirse involuntariamente en atacantes, ya que el malware recupera los contactos de Outlook de la máquina comprometida e intenta enviar correos electrónicos no deseados con el adjunto malicioso a sus amigos y compañeros de trabajo.

Este malware ha comenzado a emplear exploits de EternalBlue para propagarse lateralmente a otras máquinas en la misma red. Algunos de los scripts maliciosos usan el término "$ Lemon_Duck" como variable. La mayoría de los módulos ofensivos utilizados en el script provienen de repositorios de código abierto, los cuales, mantienen su persistencia en las máquinas Windows infectadas mediante tareas programadas. Esta campaña genera aleatoriamente direcciones IP para la segmentación y escaneos de puertos para servicios de escucha en números de puerto específicos, como 445 / TCP (SMB), 1433 / TCP (servidor MS-SQL) o 65529 / TCP (un puerto utilizado por una máquina que ha sido previamente comprometida por este mismo actor de amenazas). Y una vez que el script recibe una respuesta del equipo remoto, prueba la dirección IP en busca de la vulnerabilidad EternalBlue SMB o realiza un ataque de fuerza bruta contra el servicio MS-SQL en un intento de comprometer la máquina.

Boletín	2020-305
Asunto	BAZARBACKDOOR: MALWARE ENCUBIERTO PARTE DEL GRUPO TRICKBOT
Emisión	12/10/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistema operativo Windows

Descripción

El grupo delictivo detrás de Ba zarBackdoor emplea el kit de software de penetración legítimo Cobalt Strike para la explotación a fin de enumerar y recopilar credenciales para hosts de red y directorio activo, cargando software de terceros como Lasagne y BloodHound, además de pivotar dentro del dominio de red ejecutando Ryuk ransomware.

La BazarLoader radica en su componente central sigiloso y su capacidad de ofuscación, el objetivo del malware es plantar en las victimas de alto valor y llegar al servidor actualmente a través del proxy y el algoritmo de generación de dominio en el protocolo de dominio EmerDNS, buscando dominios bazar y resolviendo el servidor a través de la función XOR de la dirección IP de respuesta.

El malware pretendía ser sigiloso y solo cargar funciones más avanzadas a través de componentes de terceros, como las balizas Cobalt Strike. Tal sigilo permite al grupo delictivo mantener la persistencia en el host incluso si el software antivirus detecta el software de terceros.

El malware Bazar utiliza una plataforma de marketing por correo electrónico Send Grid legítima y ampliamente utilizada para enviar sus correos electrónicos de phishing. Una vez que el usuario haya hecho clic en el enlace del correo electrónico de phishing se le dirigirá a la página de vista previa del señuelo, la página intenta engañar al usuario para que descargue archivos ejecutables maliciosos de doble extensión (como PreviewReport.DOC.exe) mostrando que la vista previa del documento no está disponible. Estos archivos ejecutables maliciosos de doble extensión son los archivos BazarLoader firmados con certificados.

Boletín	2020-306
Asunto	NUEVO RANSOMWARE FONIX
Emisión	13/10/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

- Sistema Operativo Windows

Descripción

La forma en que opera el ransomware Fonix es bloqueando los datos de los usuarios y luego de esto exige un rescate por el descifrado. Una vez que ingresa en la computadora, el ransomware cifra los datos del usuario utilizando algoritmos complejos, como resultado de lo cual muchos archivos, incluyendo documentos de texto, planillas, bases de datos, archivos, y mucho más, se vuelven inadecuado para un uso posterior. Una vez finalizada la encriptación, todos los archivos infectados se agregarán con una nueva extensión .XINOF, el fondo del escritorio se cambia al logotipo de .HTAFONIX y la nota de rescate del ransomware será mostrada en la pantalla. Con una venta emergente que contiene la siguiente información: How To Decrypt Files[.]hta y un archivo Help[.]txt donde contiene la dirección de correo electrónico del atacante. Los ciberdelincuentes instan a los usuarios a contactarlos por correo electrónico para conocer el monto del rescate y resolver el problema lo antes posible, pero no hay garantía de que se respeten los acuerdos.

Imagen 1: Aviso de encriptación del ransomware Fonix

Boletín	2020-307
Asunto	ATAQUE APT SIN ARCHIVOS APROVECHA EL SERVICIO DE INFORME DE ERRORES DE WINDOWS
Emisión	13/10/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

- Sistema Operativo Windows

Descripción

Las víctimas suelen infectarse con Qbot a través de otra infección de malware o mediante campañas de phishing utilizando varios señuelos, que incluyen facturas falsas, información bancaria y de pago, documentos escaneados o facturas.

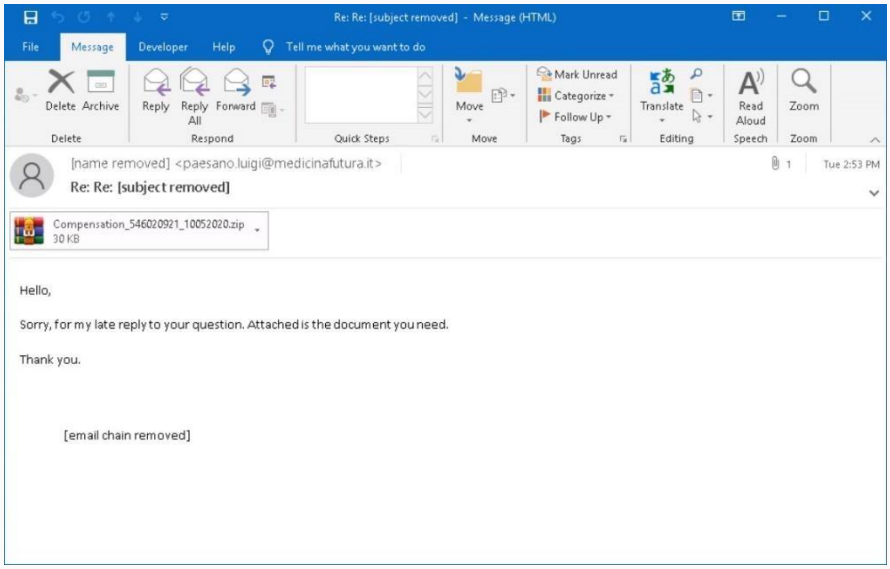


Imagen 1: correo electrónico no deseado de Qbot

Los archivos adjuntos maliciosos de excel (.xls) se adjuntan a estos correos electrónicos no deseados. Una vez abiertos, estos archivos adjuntos le pedirán al usuario que “Habilite el contenido” para que se ejecuten los macros maliciosos para instalar el malware Qbot en la computadora de la víctima. Los autores de amenazas utilizan plantillas de documentos estilizadas que pretenden ser de una organización confiable o de su sistema operativo. El 25 de agosto, Qbot cambió a un nuevo modelo que pretende ser una advertencia de Antivirus de Windows Defender, indicando que el documento está encriptado. Para descifrar el documento, los usuarios deben hacer click en “Activar edición” o “Activar contenido” para descifrarlo utilizando “Microsoft Office Decryption Core”.

Boletín	2020-310
Asunto	LA VARIANTE EKING DE PHOBOS RANSOMWARE
Emisión	15/10/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

- Sistema Operativo Windows

Descripción

De acuerdo con la investigación se observa que al abrir el documento aparece una advertencia que indica a la víctima que haga click en el botón "Habilitar contenido". Dado que las macros pueden contener código malicioso, MS Office Word muestra de forma predeterminada una advertencia de seguridad que advierte a los usuarios que el documento podría ser peligroso.

El código de la macro extrae un bloque codificado en base64 en un archivo local en "C:\Users\Public\Ksh1.xls". Luego decodifica el archivo en otro archivo llamando al comando "Certutil-decode C:\Users\Public\Ksh1.xls C:\Users\Public\Ksh1.pdf". El archivo "Ksh1.pdf" es un archivo decodificado en base64, que es un archivo PE (archivo DLL). La tarea final de la macro es ejecutar el archivo PE decodificado "Ksh1.pdf" ejecutando el comando "Rundll32 C:\Users\Public\Ksh1.pdf". El archivo PE decodificado "Ksh1.pdf" es un archivo DLL con función de exportación "In" que es llamado por "Rundll32.exe" en la línea de comando anterior. Luego descarga un archivo de la URL hxxp://178[.]62[.]19[.]66/campo/v/v en el archivo "C:\Users\Public\cs5\cs5.exe". Y finalmente, ejecuta el archivo descargado "cs5.exe" llamando a la API "CreateProcessA()".

Cuando se ejecuta el archivo "cs5.exe", crea un segundo proceso de sí mismo llamando a la API CreateProcessWithTokenW() junto con un token del proceso explorer.exe para que el segundo proceso se ejecute en el contexto de seguridad del token de explorer.exe. De esta manera, tiene el privilegio necesario para leer y escribir más archivos en el sistema de la víctima.

Boletín	2020-311
Asunto	NUEVA VARIANTE DEL MALWARE AZORULT
Emisión	16/10/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

- Sistema Operativo Windows

Descripción

Este malware de tipo troyano que se originó en uno de los países de la ex URSS, AZORult, busca información útil en la computadora afectada y la envía al servidor C2 para robar potencialmente los datos de la cuenta bancaria de la víctima.

Este malware se actualiza constantemente no debe tomarse a la ligera, ya que sigue siendo una amenaza activa. Una de las características de AZORult es que después de la ejecución, el malware se elimina del sistema debido a la falta de un mecanismo de persistencia. AZORult, en primer lugar, abre un archivo de Microsoft Office y se ejecuta WINWORD[.]EXE con habilitar macros. El malware ejecuta EQNEDT32[.]EXE y descarga un ejecutable malicioso mediante la explotación de la vulnerabilidad CVE-2017-11882 Microsoft Office Equation Editor. Luego, se inicia un archivo 3[.]exe que cambia el valor de ejecución automática en el registro. Posteriormente, procede a realizar cambios en el registro para que el sistema lo ejecute al inicio del sistema. Finalmente, un archivo ejecutable malicioso se inicia y luego procede a robar los datos personales y conectarse al servidor C2 y un archivo ejecutable malicioso inicia cmd[.]exe para borrarse después de un tiempo de espera de 3 segundos.

Boletín	2020-312
Asunto	NUEVOS ATAQUES DE EMOTET UTILIZAN MENSAJES FALSOS DE WINDOWS UPDATE
Emisión	17/10/2020
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

- Sistema Operativo Windows

Descripción

Para evitar que se marquen sus correos electrónicos como "maliciosos" o "spam", el grupo Emotet cambia periódicamente la forma en que se envían estos correos electrónicos y el aspecto de los archivos adjuntos.

En los últimos días se descubrió que Emotet utiliza un nuevo documento, los archivos adjuntos enviados en campañas recientes de Emotet muestran un mensaje falso del servicio Windows Update, en estos mensajes se les indica a los usuarios que la aplicación de Office debe actualizarse y hacer click en 'Habilitar la edición'. Estos documentos maliciosos se envían desde correos electrónicos con identidades falsas, que pueden parecer provenir de conocidos y socios comerciales.

De acuerdo con lo indicado por el grupo Cryptolaemus, estos señuelos Emotet se han enviado spam en cantidades masivas a usuarios ubicados en todo el mundo, en algunos hosts infectados, emotet instaló el troyano TrickBot, de acuerdo con el informe de ZDNet confirma que la botnet TrickBot sobrevivió a un reciente intento de eliminación de Microsoft y sus socios.

Además, Emotet a menudo utiliza una técnica llamada secuestro de conversaciones, a través de la cual roba los hilos de correo electrónico de los hosts infectados, se inserta en el hilo con una respuesta falsificando a uno de los participantes y agregando los documentos de Office maliciosas como archivos adjuntos. La técnica es difícil de aprender, especialmente entre los usuarios que trabajan con correos electrónicos comerciales a diario, por lo que Emotet muy a menudo logra infectar redes corporativas o gubernamentales.

Boletín	2020-313
Asunto	NUEVO MALWARE VIZOM USA ATAQUES DE SUPERPOSICIÓN REMOTA PARA SECUESTRAR CUENTAS BANCARIAS
Emisión	19/10/2020
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

- Sistema Operativo Windows

Descripción

Vizom utiliza tácticas interesantes para permanecer oculto y así poder comprometer los dispositivos de los usuarios en tiempo real, las técnicas usadas son superposición remota y secuestro de DLL. El malware Vizom se propaga a través de una de las campañas de phishing basadas en spam, y se disfraza de software de videoconferencia popular, herramientas que en estos tiempos está siendo muy usada para las empresas y los eventos sociales debido a la pandemia.

Una vez que el malware se encuentra un equipo con Windows vulnerable, Vizom primero atacará el directorio AppData para comenzar la cadena de infección. Al aprovechar el secuestro de DLL, el malware intentará forzar la carga de DLL maliciosas nombrando sus propias variantes basadas en Delphi con los nombres esperados por el software legítimo en sus directorios.

Luego, un dropper iniciará zTscoder.exe a través del símbolo del sistema y una segunda payload, un troyano de acceso remoto (RAT), se extrae de un servidor remoto, con el mismo truco de secuestro realizado en el navegador de Internet Vivaldi. Para establecer la persistencia, los accesos directos del navegador se manipulan y no importa qué navegador intente ejecutar un usuario, el código malicioso de Vivaldi / Vizom se ejecutará en segundo plano.

Como Vizom ya ha implementado las capacidades de RAT, los atacantes pueden hacerse cargo de una sesión comprometida y superponer contenido para engañar a las víctimas para que envíen credenciales de acceso y cuenta para sus cuentas bancarias. Las capacidades de control remoto también abusan de las funciones de la API de Windows, como mover el cursor del mouse, iniciar la entrada del teclado y emular clics. Vizom también puede tomar capturas de pantalla a través de las funciones de impresión y lupa de Windows.

Boletín	2020-314
Asunto	NUEVA VARIANTE DE MALWARE SLUB
Emisión	20/10/2020
CVE	Varios
Categoría	Malware
Severidad	Alta

Servicios Afectados

- Sistema Operativo Windows

Descripción

Esta nueva variante de SLUB interactúa con el servidor Mattermost para realizar un seguimiento de la implementación en múltiples máquinas infectadas. Crea un canal individual para cada máquina para realizar un seguimiento de ellos. Para el vector de infección en Internet Explorer utiliza el CVE-2020-0674, el cual ejecuta un shellcode, que activa algunas etapas de un cargador de PowerShell comprobando si el sistema afectado tiene instalado algún producto antimalware. Si no hay ninguno instalado, PowerShell procede a descargar y ejecutar tres backdoor y el cargador de PowerShell también puede iniciar la descarga y ejecución de un binario de LPE que explota CVE-2019-1458. Para el vector de ataque de Chrome, el exploit usó CVE-2019-5782 y otra vulnerabilidad que no tiene un CVE asignado. Para implementar esta variante, el atacante reutilizó un código POC.

El shellcode solicita el dropper.dll de la red; carga el espacio de direcciones de la carga útil DLL del proceso en ejecución. Tanto las muestras entregadas por el shellcode como el script de PowerShell se conectan a los mismos servidores C&C. Además del comportamiento mencionado anteriormente, también se vio que la campaña explotaba otras vulnerabilidades, como CVE-2016-0189¸ CVE-2019-1458.

Además de SLUB, dos nuevas variantes de malware, denominadas dneSpy y agfSpy, también están vinculadas a esta campaña. Si bien el objetivo de SLUB en esta campaña es exfiltrar información del sistema, las otras dos variantes de malware se implementaron para obtener un control adicional de la máquina del usuario afectado. Al igual que los sitios afectados antes mencionados, los servidores comprometidos utilizan el Sistema de gestión de contenido (CMS) GNUBoard, algunos de ellos en la versión 4 o la versión 5.

Boletín	2020-316
Asunto	PHISHING CON INFORMACIÓN DE COINBASE SECUESTRA CUENTAS DE MICROSOFT
Emisión	21/10/2020
CVE	No tiene
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Office 365 OAuth

Descripción

Las aplicaciones de consentimiento son aplicaciones de Office 365 OAuth que permiten el acceso de terceros a la cuenta de correo electrónico de un usuario que da su consentimiento para realizar acciones en su nombre. Estas aplicaciones se utilizan con fines legítimos, como para el filtrado de correo no deseado, el análisis antivirus o el calendario.

La nueva campaña de phishing utiliza correos con el asunto "Nuevos términos de servicio" donde se les indica a los usuarios de Coinbase leer y aceptar los términos para seguir usando el servicio, si el usuario le da click al enlace lo redirigirá a un sitio de Microsoft legítimo que le pedirá que inicie sesión en su cuenta de Microsoft. La URL solicita los permisos User.Read, Mail.Read y Mail.ReadWrite en la cuenta del usuario objetivo. Si el usuario inicia sesión en su cuenta de Microsoft, se le mostrará un mensaje para permitir que una aplicación de coinbaseterms.app acceda a su cuenta.

Si el usuario acepta la solicitud de la aplicación, se enviará al desarrollador de la aplicación un token de seguridad asociado con el usuario, este token permite a los atacantes acceder a la cuenta de Office 365 del usuario desde sus servidores y aplicaciones, al aceptar la cuenta, pueden realizar acciones o ver datos en base a los permisos de la aplicación. Una vez que el usuario de Office 365 haga clic en el botón 'Sí', los actores de la amenaza tendrán acceso completo para leer el perfil de las cuentas y su correo electrónico.

Los permisos de consentimiento de la aplicación no permiten que los atacantes envíen un correo electrónico en nombre de la víctima, pero el permiso Mail.ReadWrite permite que un atacante actualice un borrador de mensaje creado por el usuario.

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.