SECURESOFT CORPORATION
e-Secure Consulting Group

Reporte Quincenal de Ciberinteligencia Securesoft

Fecha:

04 febrero de 2021

El presente documento contiene información para la comunidad de ciberseguridad.

Equipo de Ciberinteligencia

CIB-FOR-2021-003

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

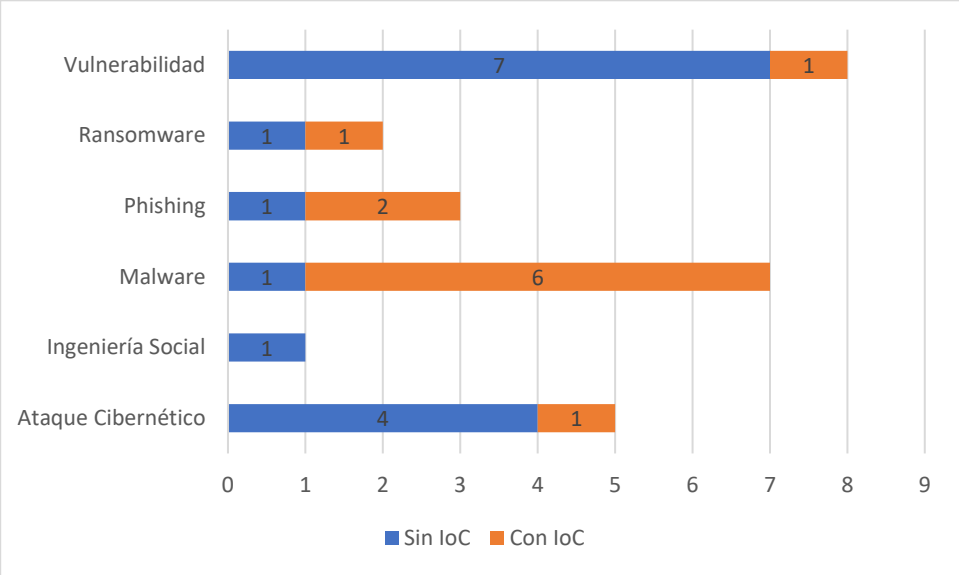
Este documento muestra el resumen, la fecha de publicación, CVE asociado y servicios afectados de vulnerabilidades y amenazas que se han hecho públicas en el transcurso del 15 de enero hasta el 31 de enero del 2021.

3. Resumen

En el presente informe se exponen 26 análisis de vulnerabilidad y amenazas, de las cuales 24 tienen severidad alta y 2 severidad crítica.

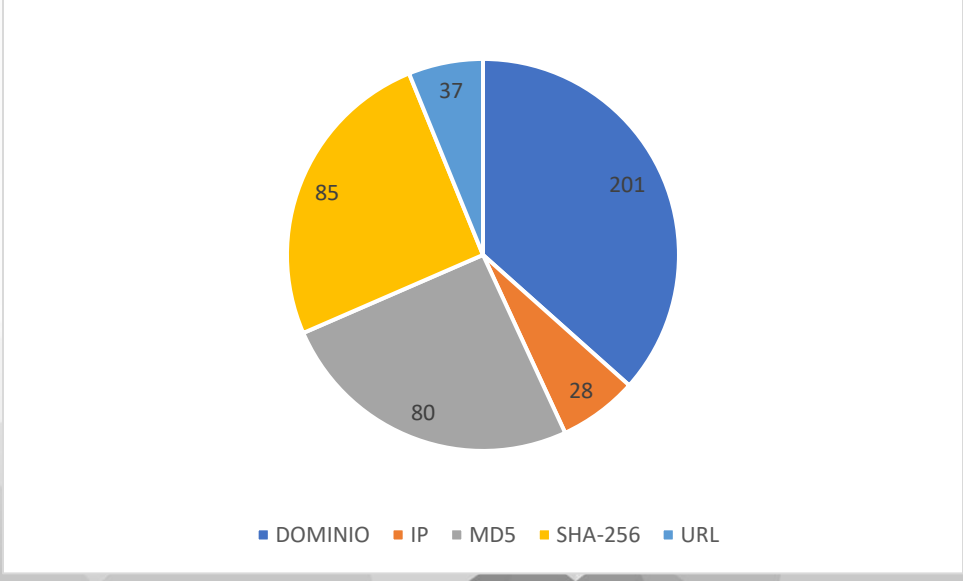
Amenazas analizadas por tipología

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 431 IoCs entre Dominios, URL, IP, MD5 y SHA256.



Tendencias en nuevas vulnerabilidades

- Se identificó una nueva vulnerabilidad que permitiría a un atacante escalar privilegios y escapar del contenedor de Azure Functions Docker al equipo de Docker. Para más información leer el Boletín 2021-042.
- Qualys ha identificado una vulnerabilidad de Sudo como el CVE-2021-3156 que permite a cualquier usuario local obtener privilegios de root, y se activa cuando Sudo elimina incorrectamente las barras diagonales inversas en los argumentos. Para más información leer el Boletín 2021-038, en la cual podrá encontrar la actualización de las vulnerabilidades.
- Recientemente IBM informó que sus productos QRadar SIEM son vulnerables a la lectura arbitraria de archivos. Además, podría permitir que un atacante remoto atraviese directorios en el sistema y que un atacante autenticado envíe solicitudes no autorizadas desde el sistema. Para más información leer el Boletín 2021-040, en la cual podrá encontrar la actualización para estas vulnerabilidades.
- La vulnerabilidad de seguridad de alta gravedad (CVE-2021-1257) permite ataques de falsificación de solicitudes entre sitios (CSRF) en Cisco DNA Center. Para más información leer el Boletín 2021-035, en la cual podrá encontrar la actualización para estas vulnerabilidades.
- Cisco ha publicado actualizaciones de seguridad para abordar las vulnerabilidades de ejecución remota de código (RCE) previa a la autenticación que afectan a varios productos SD-WAN y al software Cisco Smart Software Manager. Para más información leer el Boletín 2021-028, en la cual podrá encontrar la actualización para estas vulnerabilidades.

Tendencias en actividades maliciosas

- Los investigadores de seguridad de AT&T Alien Labs han descubierto que el grupo de ciberdelincuencia TeamTNT actualizó su cripto minería de Linux con capacidades de evasión de detección de código abierto, para más información leer Boletín 2021-041.

- Vadokrist, un troyano bancario, ha estado activo desde el 2018 y se ha dirigido casi exclusivamente a organizaciones en Brasil. Este malware se cree que está conectado con Amavaldo, Casbaneiro, Grandoreiro y Mekotio, otros troyanos bancarios latinoamericanos, para más información leer Boletín 2021-030.

- Grupos cibercriminales detras de ransomware ahora están utilizando ataques DDoS para obligar a víctimas a contactarlos y negociar un rescate, para más información leer Boletín 2021-034.

- Se ha descubierto un nuevo ransomware llamado Vovalex se está distribuyendo a través de un software ilegal que se hace pasar por funciones populares de Windows, como CCleaner, para más información leer Boletín 2021-047.

4. Detalles

Vulnerabilidades

Boletín	2021-042
Asunto	NUEVO ERROR DE ESCAPE DEL CONTENEDOR DOCKER AFECTA LAS FUNCIONES DE MICROSOFT AZURE
Emisión	28/01/2021
CVE	No tiene
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Servicio Microsoft Azure functions

Descripción

Se identificó una nueva vulnerabilidad que permitiría a un atacante escalar privilegios y escapar del contenedor de Azure Functions Docker al equipo de Docker.

Azure Functions es un servicio informático sin servidor que permite a los usuarios ejecutar código sin tener que aprovisionar o administrar la infraestructura. Las funciones de Azure se pueden activar mediante solicitudes HTTP, y están diseñadas para ejecutarse solo durante unos minutos para controlar el evento. El código del usuario se ejecuta en un contenedor administrado por Azure y se sirve sin necesidad de que el usuario administre su propia infraestructura. Si el usuario quiere tomar un atajo, puede hacerlo.

Actualización o Mitigación

Se recomienda a los usuarios aplicar la última actualización de acuerdo con el producto afectado.

Boletín	2021-038
Asunto	NUEVA FALLA DE LINUX SUDO PERMITE A LOS USUARIOS LOCALES OBTENER PRIVILEGIOS ROOT
Emisión	27/01/2021
CVE	CVE-2021-3156
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Sudo versiones heredadas desde 1.8.2 a 1.8.31p2 y versiones anteriores a 1.9.5p2

Descripción

La vulnerabilidad de Sudo (CVE-2021-3156) ahora corregida, habría podido permitir a cualquier usuario local obtener privilegios de root en sistemas operativos similares a Unix sin requerir autenticación.

Sudo es un programa de Unix que permite a los administradores del sistema proporcionar privilegios de root limitados a los usuarios normales que figuran en el archivo sudoers, mientras que al mismo tiempo mantienen un registro de su actividad. Funciona según el principio de privilegio mínimo, en el que el programa otorga a las personas los permisos necesarios para realizar su trabajo sin comprometer la seguridad general del sistema.

Actualización o Mitigación

Los fallos de seguridad han sido solucionados y se recomienda a los usuarios aplicar la última versión de sudo 1.9.5p2.

Boletín	2021-040
Asunto	IBM SOLUCIONA NUEVA VULNERABILIDAD QUE AFECTA A LOS PRODUCTOS SIEM QRADAR
Emisión	27/01/2021
CVE	CVE-2020-4786, CVE-2020-4787 y CVE-2020-4789
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

- IBM QRadar SIEM 7.4.2 GA a 7.4.2 parche 1
- IBM QRadar SIEM 7.4.0 a 7.4.1 parche 1
- IBM QRadar SIEM 7.3.0 a 7.3.3 parche 5

Descripción

Recientemente IBM informo que sus productos QRadar SIEM son vulnerables a la lectura arbitraria de archivos. Además, podría permitir que un atacante remoto atraviese directorios en el sistema y que un atacante autenticado envíe solicitudes no autorizadas desde el sistema.

El CVE-2020-4789 hace referencia a IBM QRadar que podría permitir que un atacante remoto atraviese directorios en el sistema. Un atacante podría enviar una solicitud de URL especialmente diseñada que contenga secuencias de "puntos" (/../) para ver archivos arbitrarios en el sistema.

Actualización o Mitigación

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

Boletín	2021-035
Asunto	ACTUALIZACIÓN DE SEGURIDAD DE CISCO DNA CENTER
Emisión	26/01/201
CVE	No tiene
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Versiones anteriores a 2.1.1.0 de Cisco DNA Center

Descripción

La vulnerabilidad de seguridad de alta gravedad (CVE-2021-1257) permite ataques de falsificación de solicitudes entre sitios (CSRF) en Cisco DNA Center.

La falla, identificada como CVE-2021-1257, existe en la interfaz de administración basada en la web de Cisco DNA Center, que es una plataforma centralizada de administración y orquestación de redes para Cisco DNA. DNA Center permite a los administradores aprovisionar y configurar todos los dispositivos de red, y utiliza inteligencia artificial (AI) y aprendizaje automático (ML) para monitorear, solucionar problemas y optimizar las redes de manera proactiva.

Actualización o Mitigación

Todos los fallos de seguridad han sido solucionados y se recomienda Actualizar a las versines 2.1.1.0, 2.1.2.0, 2.1.2.3 y 2.1.2.4 del software Cisco DNA Center y posteriores.

Boletín	2021-036
Asunto	GOOGLE CORRIGE UNA VULNERABILIDAD GRAVE DE GOLANG WINDOWS RCE
Emisión	26/01/2021
CVE	CVE-2021-3115
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Go versiones anterior a 1.14.14 y 1.15.7

Descripción

La vulnerabilidad RCE, CVE-2021-3115, afecta principalmente a los usuarios de Windows de Go que ejecutan el comando “go get”, debido al comportamiento predeterminado de las búsquedas de Windows PATH.

La vulnerabilidad, registrada como CVE-2021-3115, se deriva de cómo funciona el proceso de compilación cuando un usuario ejecuta el comando "go get" para buscar un repositorio. En los sistemas Windows, un comando de shell del sistema operativo ejecutado por el usuario o un programa hace que el shell busque primero el binario ejecutable asociado con ese comando dentro del directorio actual, seguido de una lista de directorios especificados en la variable PATH del sistema.

Actualización o Mitigación

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

Boletín	2021-028
Asunto	CISCO CORRIGE ERRORES CRÍTICOS PREVIOS A LA AUTENTICACIÓN EN SD-WAN
Emisión	21/01/2021
CVE	Varios
Categoría	Vulnerabilidad
Severidad	Crítica

Servicios Afectados

• Versiones anteriores a 6.3.0 de Cisco Smart Software Manager Satellite y posteriores de Cisco Smart Software Manager On-Prem.

• Versiones anteriores a la 1.3.1.0 del software Cisco DNA Center

Descripción

Cisco publicó parches que abordan ocho vulnerabilidades de SD-WAN de desbordamiento de búfer e inyección de comandos. El más grave de estos defectos podría ser aprovechado por un atacante remoto no autenticado para ejecutar código arbitrario en el sistema afectado con privilegios de root.

Una falla de severidad crítico existe (CVE-2021-1299) en la interfaz de gestión basada en web de Cisco SD-WAN vManage aoftware. Esta falla podría permitir que un atacante remoto autenticado obtenga acceso de nivel raíz a un sistema afectado y ejecute comandos arbitrarios como usuario raíz en el sistema.

La falla de desbordamiento de búfer (CVE-2021-1300) se debe a un manejo incorrecto del tráfico IP, un atacante podría aprovechar la falla enviando tráfico IP diseñado a través de un dispositivo afectado, lo que puede causar un desbordamiento de búfer cuando se procesa el tráfico. Esto permite que un atacante ejecute código arbitrario en el sistema operativo subyacente con privilegios de root.

Actualización o Mitigación

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

Boletín	2021-024
Asunto	BOTNET APROVECHA VULNERABILIDADES RECIENTES DE LINUX
Emisión	19/01/2021
CVE	CVE-2020-28188, CVE-2021-3007 y CVE-2020-7961
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Dispositivos NAS con sistemas operativos Linux

Descripción

Una campaña de malware en curso explota vulnerabilidades reveladas recientemente en dispositivos de almacenamiento conectados a la red (NAS) en sistemas Linux para incorporarlos a una botnet IRC, con ello, lanza ataques distribuidos de denegación de servicio (DDoS) y extrae criptomonedas Monero.

Independientemente de las vulnerabilidades explotadas, el objetivo final del atacante parece ser descargar y ejecutar un script de Python llamado "out.py" utilizando Python 2, que llegó al final de su vida útil el año pasado, lo que implica que el actor de la amenaza está confiando en la posibilidad de que los equipos de la víctima tengan instalada esta versión obsoleta.

Actualización o Mitigación

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

Boletín	2021-025
Asunto	FALLAS DE DNSPOOQ PERMITIRÍAN EL SECUESTRO DE DNS DE MILLONES DE DISPOSITIVOS
Emisión	19/01/2021
CVE	Varios
Categoría	Vulnerabilidad
Severidad	Alta

Servicios Afectados

• Dnsmasq

Descripción

Se ha revelado siete vulnerabilidades en Dnsmasq, conocidas colectivamente como DNSpooq, los cuales, se componen de problemas de desbordamiento de búfer y fallas que permiten ataques de suplantación de DNS. Si se explotan, estas fallas podrían encadenarse para permitir la ejecución remota de código, la denegación de servicio y otros ataques.

El almacenamiento de respuestas por parte del software a consultas DNS previamente solicitadas acelera localmente el proceso de resolución de DNS; sin embargo, también tiene muchos otros usos, incluido el suministro de servicios DNS para admitir puntos de acceso Wi-Fi, redes de invitados empresariales, virtualización y bloqueo de anuncios.

Actualización o Mitigación

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

Amenazas

Boletín	2021-046
Asunto	DOS NUEVAS TÁCTICAS DE PHISHING UTILIZADAS PARA EVADIR LOS FILTROS DE CORREO ELECTRÓNICO
Emisión	30/01/2021
CVE	Ninguno
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Sistemas operativos Windows

Descripción

A principios de enero, se detectó una campaña que aprovechaba las herramientas de encuestas Google para impulsar un diálogo continuo entre el destinatario del correo electrónico y el atacante configurándolos como víctimas de una futura trampa BEC.

Ahora los ciberdelincuentes están empleando dos tipos de tácticas de phishing, la primera es redirigir las respuestas legítimas del tipo de mensaje “out of office (OOO)” y la segunda es “read-receipts”.

En el primer tipo de ataque “out of office (OOO)”, un ciberdelincuente se hace pasar por alguien dentro de la organización mediante la creación de un correo electrónico empresarial. El atacante puede manipular el encabezado del correo electrónico "Reply-To" para que se dirija a otra persona dentro de la organización. Los ataques basados como estos están diseñados para obtener una respuesta urgente de los destinatarios para hacer click en un enlace malicioso y si un usuario hace click en el enlace, hace que el riesgo de su dispositivo pueda permitir que un atacante escale los privilegios en la red de la organización.

En el segundo tipo de ataque “read-receipts”, un ciberdelincuente crea un correo electrónico de extorsión y manipula el encabezado del correo electrónico "Disposition-Notification-To" para generar una notificación de recepción de lectura de Microsoft 365 para el destinatario. El correo electrónico malicioso puede quedar atrapado por la plataforma de seguridad, pero la confirmación de lectura se envía al objetivo de todos modos, esto incluye el texto del correo electrónico original ya que se genera desde el sistema interno.

Boletín	2021-047
Asunto	NUEVO RANSOMWARE VOVALEX ESCRITO EN D
Emisión	30/01/2021
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Vovalex fue descubierto por primera vez por MalwareHunterTeam. Este ransomware puede ser el primer ransomware escrito en lenguaje D, el cual se inspiró en otros lenguajes, en especialmente en C ++.

Cuando se ejecuta, iniciará un instalador CCleaner legítimo y se copiará al nombre de archivo aleatorio en la carpeta% Temp%.

Luego, el ransomware comenzará a cifrar archivos en la unidad y agregará la extensión [.]vovalex a los nombres de los archivos cifrados. Cuando termine, el ransomware creará una nota de rescate llamada README[.]VOVALEX[.]txt mediante el cual los ciberdelincuentes solicitan 0.5 XMR para un descifrador.

Boletín	2021-044
Asunto	GRUPO DE ATACANTES SE DIRIGIÓ A LAS EMPRESAS DE TELECOMUNICACIONES, ALOJAMIENTO E ISP
Emisión	29/01/2021
CVE	CVE-2019-3396, CVE-2019-11581 y CVE-2012-3152
Categoría	Ataque Cibernético
Severidad	Alta

Servicios Afectados

• Sistema operativo Windows

Descripción

Se identificaron al menos 250 servidores web públicos desde principios de 2020 que han sido vulnerados por el actor de amenazas para recopilar inteligencia y robar las bases de datos de la compañía. Las intrusiones orquestadas afectaron a una gran cantidad de empresas ubicadas en los EE. UU., El Reino Unido, Egipto, Jordania, el Líbano, Arabia Saudita, Israel y la Autoridad Palestina, y la mayoría de las víctimas representan a operadores de telecomunicaciones, proveedores de servicios de Internet (SaudiNet, TE Data) y proveedores de servicios de alojamiento e infraestructura.

Documentado por primera vez en 2015, se sabe que el cedro volátil o cedro libanés penetra en una gran cantidad de objetivos utilizando diversas técnicas de ataque, incluido un implante de malware hecho a medida con nombre en código explosivo. La actividad maliciosa descubierta por ClearSky coincidió con las operaciones atribuidas a Hezbollah basadas en superposiciones de código entre las variantes de 2015 y 2020 del explosive RAT, que se implementa en las redes de las víctimas mediante la explotación de vulnerabilidades conocidas en servidores web Oracle y Atlassian sin parches.

Los atacantes usan las fallas en los servidores (CVE-2019-3396, CVE-2019-11581 y CVE-2012-3152) como un vector de ataque para ganar un punto de apoyo inicial, los atacantes luego inyectaron un shell web y un navegador de archivos JSP, ambos se usaron para moverse lateralmente a través de la red, buscar malware adicional y descargar explosive RAT, que viene con capacidades para registrar pulsaciones de teclas, capturar capturas de pantalla y ejecutar comandos arbitrarios. El shell web se utiliza para llevar a cabo varias operaciones de espionaje en el servidor web atacado, incluida la ubicación de activos potenciales para futuros ataques, la configuración del servidor de instalación de archivos y más.

Boletín	2021-045
Asunto	PRO-OCEAN UN NUEVO MALWARE DE CRIPTOJACKING DEL GRUPO ROCKE
Emisión	29/01/2021
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Aplicaciones en la nube

Descripción

Pro-Ocean utiliza vulnerabilidades conocidas para apuntar a aplicaciones en la nube. Pro-Ocean aprovecha las vulnerabilidades de Apache ActiveMQ (CVE-2016-3088), Oracle WebLogic (CVE-2017-10271) y Redis (instancias no seguras). En el caso de que el malware se ejecute en Tencent Cloud o Alibaba Cloud, usará el código exacto del malware de versión anterior para desinstalar los agentes de monitoreo para evitar la detección. Además, intenta eliminar otros malware y mineros, incluidos Luoxk, BillGates, XMRig y Hashfish antes de la instalación. Una vez instalado, el malware elimina cualquier proceso que use mucho el CPU, de modo que pueda usar el 100% del CPU y realizar la mineria de monedas de manera eficiente.

Pro-Ocean tiene como objetivo varias aplicaciones de nube típicas, incluidas Apache ActiveMQ, Oracle Weblogic y Redis, con énfasis en proveedores de nube con sede en China, incluidos Alibaba Cloud y Tencent Cloud. Está escrito en Go y compilado en un binario de arquitectura x64. Contiene cuatro módulos que se despliegan durante la ejecución: ocultación, minería, infección y vigilancia. Cada módulo contiene algunos archivos escritos en varios lenguajes (C, Python o Bash) y un script Bash que lo ejecuta.

Pro-Ocean contiene un módulo de vigilancia escrito en Bash que ejecuta dos scripts Bash con diferentes propósitos. El primer script "program__kill30" repite indefinidamente y busca procesos que utilizan más del 30% del CPU sin incluir los procesos de malware. El objetivo del malware es usar el 100% del CPU y realizar la mineria de monedas de manera eficiente, por lo que elimina cualquier proceso que use el CPU en gran medida. El segundo script llamado "Program_daemonload" se repite indefinidamente y verifica que el malware se esté ejecutando.

Boletín	2021-043
Asunto	ATAQUES DE PHISHING DIRIGIDOS AFECTAN A EJECUTIVOS DE EMPRESAS DE ALTO RANGO
Emisión	28/01/2021
CVE	No tiene
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

La campaña depende de un truco de ingeniería social que implica enviar correos electrónicos a víctimas potenciales que contienen notificaciones falsas de caducidad de contraseñas de Office 365 como señuelos. Los mensajes también incluyen un enlace incrustado para retener la misma contraseña que, cuando se hace click, redirige a los usuarios a una página de phishing para recopilar credenciales.

Los atacantes se dirigen a empleados de alto perfil que pueden no ser tan expertos en tecnología o ciberseguridad, y pueden ser más propensos a ser engañados para hacer clic en enlaces maliciosos. Según los investigadores, las direcciones de correo electrónico específicas se recopilaron principalmente de LinkedIn, aunque señalaron que los atacantes podrían haber comprado dichas listas de objetivos en sitios web de marketing que ofrecen datos de perfil de redes sociales y correo electrónico de CEO/CFO.

El kit de phishing de Office 365, actualmente en su cuarta iteración (V4), se lanzó originalmente en julio de 2019, con características adicionales agregadas para detectar el escaneo de bots o intentos de rastreo y proporcionar contenido alternativo cuando se detectan bots. Curiosamente, el supuesto desarrollador detrás del malware anunció la disponibilidad de V4 en su página de Facebook "comercial" a mediados de 2020. También se ha descubierto que los ciberdelincuentes venden credenciales de cuentas de directores ejecutivos, directores financieros (CFO), miembros del departamento de finanzas y otros ejecutivos de alto perfil en las páginas de las redes sociales.

Las investigaciones descubrieron que al menos ocho sitios de phishing comprometidos que alojaban el kit de phishing V4, lo que plantea la posibilidad de que fueran utilizados por diferentes actores para una amplia gama de campañas de phishing dirigidas contra directores ejecutivos, presidentes, miembros de la junta y fundadores de empresas ubicadas en los EE. UU. el Reino Unido, Canadá, Hungría, los Países Bajos e Israel.

Boletín	2021-039
Asunto	DANABOT MALWARE VUELVE A COBRAR RELEVANCIA
Emisión	27/01/2021
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

DanaBot es un troyano bancario que primero apuntó a los usuarios en Australia a través de correos electrónicos que contienen URL maliciosas. Luego, los delincuentes desarrollaron una segunda variante y apuntaron a empresas estadounidenses, como parte de una serie de campañas a gran escala. Una tercera variante apareció en febrero de 2019 que se mejoró significativamente con la funcionalidad de comando y control remoto (C2).

Si bien la cuarta versión más reciente, encontrada por Proofpoint, es única, no está claro qué nuevas capacidades específicas, tiene el malware. En comparación con campañas anteriores, indicaron que esta variante más reciente viene empaquetada principalmente con el mismo arsenal de herramientas que se han presentado antes. Las características principales incluyen un componente ToR para anonimizar las comunicaciones entre los malos y un hardware infectado.

El malware DanaBot está configurado como un 'malware como servicio' en el que un actor de amenazas controla un panel e infraestructura de comando y control global (C&C) y luego vende el acceso a otros actores de amenazas conocidos como afiliados. La cadena de infección de múltiples etapas de DanaBot comienza con un gotero que desencadena una evolución en cascada de hacks. Estos incluyen el robo de solicitudes de red, el desvío de credenciales de aplicaciones y servicios, la exfiltración de datos de información confidencial, la infección por ransomware, el espionaje de capturas de pantalla de escritorio y la caída de un criptominero.

Los archivos LNK (o archivos de acceso directo de Windows) son archivos creados por Windows automáticamente, cada vez que un usuario abre sus archivos. Windows utiliza estos archivos para conectar un tipo de archivo a una aplicación específica que se utiliza para ver o editar contenido digital.

Boletín	2021-041
Asunto	MALWARE DE LINUX UTILIZA HERRAMIENTA DE CÓDIGO ABIERTO PARA EVADIR LA DETECCIÓN
Emisión	27/01/2021
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

El grupo de ciberdelincuencia TeamTNT es conocido por sus ataques basados en la nube, que incluyen dirigirse a las credenciales de Amazon Web Services (AWS) para ingresar a la nube y usarla para extraer la criptomoneda Monero. También se ha dirigido con anterioridad a las instancias en la nube de Docker y Kubernetes.

Libprocesshider se copia de los repositorios de código abierto. La herramienta de código abierto, de 2014, se ha ubicado en Github y se describe que tiene capacidades para ocultar un proceso en Linux utilizando el precargador de ld. Si bien la nueva funcionalidad de Libprocesshider es evadir la detección y otras funciones básicas, actúa como un indicador a considerar cuando se busca actividad maliciosa en el nivel del host. Libprocesshider se entrega dentro de un script codificado en base64, oculto en el binario de criptomineros TeamTNT, a través de su bot de Internet Relay Chat (IRC), llamado TNTbotinger, que es capaz de ataques distribuidos de denegación de servicio (DDoS).

En la cadena de ataque, una vez que se descarga el script codificado en base64, se ejecuta a través de varias tareas. Estos incluyen modificar la configuración de DNS de la red, establecer la persistencia (a través de systemd), descargar la última configuración del bot de IRC, borrar la evidencia de actividades y eliminar y activar libprocesshider. La herramienta se coloca como un archivo oculto (también conocido como formato Tar) en el disco y luego se descomprime mediante el script y se escribe en “/usr/local/lib/systemhealt”.

Libprocesshider usa un proceso llamado precarga para ocultar su actividad de 'ps' y 'lsof'. Este proceso permite que el sistema cargue una biblioteca compartida personalizada antes de que se carguen otras bibliotecas del sistema. Si la biblioteca compartida personalizada exporta una función con la misma firma de una ubicada en las bibliotecas del sistema, la versión personalizada la anulará. La biblioteca compartida personalizada cargada permite que la herramienta implemente la función readdir(). Esta función es utilizada por procesos como 'ps' para leer el directorio /proc para encontrar procesos en ejecución. Utiliza esta función para modificar el valor de retorno, en caso de que 'ps' encuentre el proceso malicioso, con el fin de ocultarlo.

Boletín	2021-037
Asunto	NUEVA FAMILIA DE MALWARE BASADO EN LINUX LLAMADA BOTNET DREAMBUS
Emisión	26/01/2021
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas operativos Lunix

Descripción

El malware tiene una estructura modular y sus módulos tienen una tasa de detección baja. El bot DreamBus tiene un comportamiento similar a un gusano que es altamente efectivo, puede propagarse a sistemas que no están expuestos directamente a Internet mediante el escaneo de rangos de subred privados RFC 1918 en busca de sistemas vulnerables.

Estas técnicas incluyen numerosos módulos que explotan la confianza implícita, las contraseñas débiles y las vulnerabilidades de ejecución remota de código (RCE) no autenticado en aplicaciones populares, incluido Secure Shell (SSH), herramientas de administración de TI, una variedad de aplicaciones basadas en la nube y bases de datos.

Algunos módulos se han diseñado para realizar ataques de fuerza bruta contra SSH, PostgreSQL, Redis, Hadoop YARN, Apache Spark, HashiCorp Consul y SaltStack. La botnet apunta a aplicaciones empresariales que se ejecutan en sistemas Linux. En algunos casos, las aplicaciones son atacadas con comandos maliciosos enviados a puntos finales de API expuestos o mediante exploits para vulnerabilidades más antiguas.

La característica principal del bot DreamBus fue extraer el minero de criptomonedas XMRig Monero, también se puede emplear para implementar otros payloads para llevar a cabo otras actividades maliciosas. Los sistemas infectados se comunican con el servidor C2 a través del nuevo protocolo DNS-over-HTTPS (DoH) para evitar la detección, que es una característica poco común del malware. El servidor C2 de la botnet DreamBus está alojado en la red Tor para evitar su adquisición.

Boletín	2021-033
Asunto	ATAQUE A SONICWALL CON ERRORES DE DÍA 0 EN SU PRODUCTO VPN
Emisión	23/01/2021
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• VPN NetExtender versión 10.x
• Secure Mobile Access (SMA) versión 10.x

Descripción

Recientemente, SonicWall identificó un ataque coordinado en sus sistemas internos por parte de actores de amenazas altamente sofisticados que explotaban probables vulnerabilidades de día cero en ciertos productos de acceso remoto seguro de SonicWall. Se recibió informes de que los sistemas internos de SonicWall fallaron a principios de esta semana el martes y que los atacantes accedieron al código fuente alojado en el repositorio de GitLab de la compañía.

SonicWall no confirmó los informes más allá de la declaración y agregó que proporcionaría actualizaciones adicionales a medida que haya más información disponible. La lista completa de productos afectados incluye:

• Cliente VPN NetExtender versión 10.x (lanzado en 2020) utilizado para conectarse a dispositivos de la serie SMA 100 y firewalls SonicWall
• Secure Mobile Access (SMA) versión 10.x que se ejecuta en dispositivos físicos SMA 200, SMA 210, SMA 400, SMA 410 y el dispositivo virtual SMA 500v

La compañía dijo que su serie SMA 1000 no es susceptible a los días cero y que utiliza clientes diferentes a NetExtender.

Boletín	2021-031
Asunto	BOOTERS DE DDOS UTILIZAN SERVIDORES DE ESCRITORIO REMOTO DE WINDOWS PARA AMPLIFICAR LOS ATAQUES
Emisión	22/01/2021
CVE	No tiene
Categoría	Ataque Cibernético
Severidad	Alta

Servicios Afectados

• Servidores RDP de Windows

Descripción

El servicio Microsoft RDP es un servicio integrado de Windows que se ejecuta en TCP/3389 y UDP/3389 que permite el acceso autenticado a la infraestructura de escritorio virtual (VDI) a servidores y equipos de Windows. Los ataques que aprovechan este nuevo vector de ataque de reflexión/amplificación UDP dirigidos a servidores Windows con RDP que tienen habilitado el puerto UDP/3389 que tienen una relación de amplificación de 85,9:1 y un pico de 750 Gbps.

El tráfico de ataque amplificado consiste en paquetes UDP no fragmentados provenientes de UDP/3389 y dirigidos hacia las direcciones IP de destino y los puertos UDP elegidos por el atacante. A diferencia del tráfico de sesión RDP legítimo, los paquetes de ataque amplificados tienen una longitud constante de 1260 bytes y se rellenan con largas cadenas de ceros.

De acuerdo con lo informado por Netscout, alrededor de 14.000 servidores RDP de Windows vulnerables son accesibles a través de Internet. Como ocurre habitualmente con los nuevos vectores de ataque DDoS, parece que después de un período inicial de empleo por parte de atacantes avanzados con acceso a la infraestructura de ataque DDoS a medida, la reflexión/amplificación de RDP se ha convertido en arma y se ha agregado a los arsenales de los llamados booter/estresores. Servicios de DDoS por alquiler, poniéndolo al alcance de la población general de atacantes.

Boletín	2021-032
Asunto	EXPLOIT PÚBLICO DE SAP SOLMAN
Emisión	06/01/2021
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

SAP SolMan es un administrador del ciclo de vida de las aplicaciones implementado en casi todos los entornos de SAP y está diseñado para ayudar a unificar la administración de todos los sistemas SAP. SolMan también se utiliza como una utilidad administrativa para monitorear y mantener aplicaciones empresariales SAP de misión crítica, que incluyen, entre otros, ERP, BI, CRM, SCM y finanzas de una organización. SAP emitió un parche para CVE-2020-6207 en marzo de 2020.

Esta falla de seguridad crítica se rastrea como CVE-2020-6207 y es causada por una verificación de autenticación faltante en el componente EEM Manager Solman que podría llevar a la toma de control de los sistemas SAP conectados. Puede ser explotado de forma remota en ataques de baja complejidad por atacantes no autenticados con acceso al puerto HTTP (s) de SolMan, sin que se requiera interacción del usuario.

Los ataques que abusen con éxito de esta vulnerabilidad expondrían virtualmente todas las aplicaciones SAP, los procesos comerciales y los datos de una organización a la filtración o manipulación, lo cual pondría poner en peligro todos los sistemas administrados mediante la instancia de SolMan comprometida, mediante la ejecución de las siguientes tareas maliciosas que los atacantes podrían ejecutar después de comprometer un servidor SolMan:

• Apagar cualquier sistema SAP en el panorama (no solo SAP SolMan)
• Causar deficiencias en el control de TI que afecten la integridad financiera y la privacidad que conducen a infracciones de cumplimiento normativo, como Sarbanes-Oxley (SOX), GDPR y otros
• Eliminar cualquier dato en los sistemas SAP, incluidos los datos clave que pueden causar interrupciones comerciales
• Asignar privilegios de superusuario (por ejemplo, SAP_ALL) a cualquier usuario nuevo o existente, lo que permite a esos usuarios ejecutar operaciones comerciales que normalmente requerirían privilegios específicos para eludir otros controles de Segregación de Funciones (SoD)
• Leer datos confidenciales de la base de datos, incluida la información personal de empleados y clientes

Boletín	2021-029
Asunto	CIBERDELINCUENTES ENVÍAN OFERTAS DE TRABAJO FALSAS POR LINKEDIN
Emisión	21/01/2021
CVE	No tiene
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Cuentas bancarias de usuarios

Descripción

Los ciberdelincuentes se hacen pasar por empleados reales de recursos humanos en un intento de atraer a las víctimas para que compartan información bancaria. En diciembre del 2020, un empleado recibió dos mensajes no solicitados en LinkedIn de reclutadores que afirmaban trabajar para una tienda de deportes y una empresa de logística.

El falso reclutador envió un PDF con la descripción del trabajo. El documento pedía que visitara un portal y registrara una "cuenta bancaria válida para funciones de nómina". Otro reclutador que pretendía trabajar para Decathlon y envió un PDF que usaba el mismo idioma sobre cómo registrarse con una "cuenta bancaria válida para funciones de nómina".

Un portavoz de LinkedIn indicó que los trabajos o los perfiles falsos son una violación de sus términos de servicio. El equipo de LinkedIn utiliza múltiples técnicas automatizadas, junto con revisiones humanas e informes de los miembros para tomar medidas rápidas para eliminar trabajos y empresas falsas, así como evitar que se creen este tipo de cuentas falsas. Se puede revisar los siguientes boletines relacionados a casos anteriores de uso de LinkedIn como el Boletín 2020-259, el cual hace refencia al troyano Qbot que ha estado robando correos electrónicos de cadenas de respuestas, las cuales son usados para distribuir malware como parte campañas maliciosas de spam.

El Boletín 2020-190, hace referencia a una campaña de ciberespionaje denominado "Operation In(ter)reception", en el cual, los cibercriminales detrás de esta intentan espiar a los empleados clave de organizaciones seleccionadas y el Boletín 2019-012, donde se informó que RedBanc, la empresa administradora de la Red Bancaria Interconectada de Chile, fue blanco de una amenaza informática.

Boletín	2021-030
Asunto	MALWARE BANCARIO VADOKRIST
Emisión	21/01/2021
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Vadokrist, un troyano bancario de América Latina está escrito en Delphi. Este malware cuando se ejecutan por primera vez recopila el nombre del usuario de la víctima y, a diferencia de la mayoría de otros troyanos bancarios latinoamericanos que lo hacen en el momento de la instalación, lo hace solo después de iniciar un ataque a una institución financiera apuntada.

Para garantizar la persistencia, Vadokrist utiliza una Run key o crea un archivo LNK en la carpeta de inicio. Como backdoor puede manipular el mouse y simular pulsaciones de teclado, registrar pulsaciones del teclado, tomar capturas de pantalla y reiniciar el equipo. También puede impedir el acceso a algunos sitios web, lo que hace de una manera forzada al terminar el proceso del navegador cuando la víctima intenta visitar dichos sitios web.

Los correos de spam recientes que distribuyen Vadokrist contienen dos archivos ZIP anidados que contienen dos archivos: un instalador MSI y un archivo CAB. Si una víctima ejecuta el instalador MSI, localiza el archivo CAB y extrae su contenido (un loader MSI) en el disco. Luego ejecuta un archivo JavaScript embebido que agrega una entrada de Run key, asegurándose de que el loader MSI se ejecute al iniciar el sistema. Finalmente, el script reinicia el equipo. Al iniciarse, el loader MSI ejecuta una DLL incorporada: el troyano bancario Vadokrist. El archivo JavaScript debido a su ofuscación aprovecha cómo funciona el operador de coma (,) en JavaScript y abusa de él para reducir en gran medida la legibilidad y posiblemente para omitir la emulación.

Vadokrist ocasionalmente se apoya en la carga lateral de DLL con un injector específico para descifrar y ejecutar el troyano bancario. Este injector es idéntico al utilizado por Amavaldo e implementa el antes mencionado algoritmo TripleKey para el descifrado de datos. Además, la mayoría de los binarios de Vadokrist implementan un algoritmo criptográfico como en otros troyanos bancarios latinoamericanos (Amavaldo y Casbaneiro) denominado TripleKey. Vadokrist usa este algoritmo para proteger sus strings y, ocasionalmente, también los payloads y las configuraciones remotas.

Boletín	2021-026
Asunto	DESCUBREN RAINDROP: CUARTO MALWARE VINCULADO AL ATAQUE SOLARWINDS
Emisión	20/01/2021
CVE	No tiene
Categoría	Malware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

Symantec, el mes pasado, descubrió más de 2.000 sistemas pertenecientes a 100 clientes que recibieron las actualizaciones de SolarWinds Orion troyanizadas, con objetivos seleccionados infectados con un payload de segunda etapa llamada Teardrop que también se utiliza para instalar Cobalt Strike Beacon. Mientras que Teardrop se usó en computadoras que habían sido infectadas por el troyano Sunburst original, Raindrop apareció en otra parte de la red, siendo utilizado por los atacantes para moverse lateralmente y desplegar payloads en otros equipos.

Los atacantes utilizaron el malware Sunspot exclusivamente contra SolarWinds en septiembre de 2019 para comprometer su entorno de compilación e inyectar el troyano Sunburst en su plataforma de monitoreo de red Orion. El software contaminado se entregó a 18.000 clientes de la empresa.
El análisis de Microsoft del modus operandi de Solorigate el mes pasado encontró que los operadores eligieron cuidadosamente sus objetivos, optando por escalar los ataques solo en un puñado de casos mediante la implementación de Teardrop basado en la información obtenida durante un reconocimiento inicial del entorno objetivo para cuentas de alto valor y bienes.
Ahora Raindrop ("bproxy[.]dll") se une a la mezcla. Si bien Teardrop y Raindrop actúan como goteros para el Cobalt Strike Beacon, también difieren en varias formas.

Para empezar, Teardrop es entregado directamente por un backdoor inicial de Sunburst, mientras que Raindrop parece haber sido implementado con el objetivo de extenderse por la red de víctimas. Además, el malware aparece en redes donde Sunburst ya ha comprometido al menos una computadora, sin indicios de que Sunburst haya activado su instalación.

Las dos cepas de malware también utilizan diferentes empaquetadores y configuraciones de Cobalt Strike. Symantec no identificó las organizaciones afectadas por Raindrop, pero dijo que las muestras se encontraron en un sistema de la víctima que estaba ejecutando software de administración y acceso a computadoras y en una máquina que se encontró que ejecutaba comandos de PowerShell para infectar computadoras adicionales en la organización con el mismo malware.

Boletín	2021-027
Asunto	EL FBI ADVIERTE CONTRA ATAQUES DE PHISHING Y VISHING
Emisión	20/01/2021
CVE	No tiene
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Cuentas de usuario

Descripción

En estos ataques, que según el FBI comenzaron en diciembre de 2019, los actores de amenazas atacarían a los empleados que usaban plataformas VoIP y convencerían a las víctimas de que expongan sus credenciales corporativas a través de sitios de phishing. Durante las llamadas telefónicas, se engañó a los empleados para que iniciaran sesión en una página web de phishing para capturar el nombre de usuario y la contraseña del empleado.

Después de obtener acceso a la red, muchos atacantes descubrieron que tenían un mayor acceso a la red, incluida la capacidad de escalar los privilegios de las cuentas de los empleados comprometidos, lo que les permitió obtener un mayor acceso a la red, lo que a menudo causa un daño financiero significativo.

Un ejemplo de un incidente en el que los atacantes encontraron a un empleado a través de la sala de chat de la empresa y lo convencieron de que iniciara sesión en la página falsa de VPN operada por los atacantes. Una vez que los actores de la amenaza tuvieron las credenciales del empleado, iniciaron sesión en la VPN de la empresa y comenzaron el proceso de localizar a una persona con mayores privilegios.

Boletín	2021-023
Asunto	FOROS DE IOBIT VULNERADOS PARA DIFUNDIR RANSOMWARE A SUS MIEMBROS
Emisión	19/01/2021
CVE	No tiene
Categoría	Ransomware
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows

Descripción

IObit es una empresa desarrolladora de software conocido por la optimización del sistema de Windows y los programas anti-malware, como Advanced SystemCare. Los miembros del foro de IObit comenzaron a recibir correos electrónicos que decían ser de IObit y que indicaban que tenían derecho a una licencia gratuita de 1 año para su software como una ventaja especial de ser miembros del foro.

En el correo electrónico se incluyó un enlace "OBTENERLO AHORA" que redirige a un sitio web malicioso, que descarga un archivo. Este archivo zip contiene archivos firmados digitalmente del programa legítimo IObit License Manager, pero con IObitUnlocker.dll reemplazado por una versión maliciosa sin firmar.

Cuando se ejecuta IObit License Manager.exe, el IObitUnlocker.dll malicioso se ejecutará para instalar el ransomware DeroHE en C:\Archivos de programa (x86)\IObit\iobit.dll y ejecutarlo. Como la mayoría de los ejecutables están firmados con el certificado de IOBit y el archivo zip estaba alojado en su sitio, los usuarios instalaron el ransomware pensando que era una promoción legítima. Según los informes del foro de IObit y otros foros, este es un ataque generalizado dirigido a todos los miembros del foro.

El ransomware mostrará un cuadro de mensaje que dice ser de IObit License Manager que dice: "Espere. Puede que tarde un poco más de lo esperado. ¡Mantenga su computadora funcionando o con la pantalla encendida!" El ransomware muestra esta alerta para evitar que las víctimas apaguen sus dispositivos antes de que finalice el ransomware. Al cifrar a las víctimas, agregará la extensión.

Boletín	2021-022
Asunto	COMANDO FINGER ABUSADO POR PHISHING PARA DESCARGAR MALWARE
Emisión	18/01/2021
CVE	No tiene
Categoría	Phishing
Severidad	Alta

Servicios Afectados

• Sistemas Operativos Windows y Linux

Descripción

El comando 'Finger' es una utilidad que se originó en los sistemas operativos Linux/Unix que permite a un usuario local recuperar una lista de usuarios en un equipo remoto o información sobre un usuario remoto en particular. Además de Linux, Windows incluye un comando finger.exe que realiza la misma funcionalidad. Se descubrió una forma de usar Finger como un LoLBin para descargar malware de un equipo remoto o exfiltrar datos. Los LolBins son programas legítimos que pueden ayudar a los atacantes a eludir los controles de seguridad para buscar malware sin activar una alerta de seguridad en el sistema.

FireEye informó por primera vez sobre el malware MineBridge después de descubrir numerosas campañas de phishing dirigidas a organizaciones surcoreanas. Estos correos electrónicos de suplantación de identidad contienen documentos de Word maliciosos disfrazados de currículums de solicitantes de empleo que instalan el malware MineBridge cuando una víctima hace click en las opciones 'Habilitar edición' o 'Habilitar contenido', se ejecutará una macro protegida con contraseña para descargar el malware MineBridge y ejecutarlo.

El comando ejecutado por la macro usa el comando finger para descargar un certificado codificado en Base64 desde un servidor remoto y lo guarda como AppData%\vUCooUr. El certificado recuperado mediante el comando finger es un ejecutable de descarga de malware codificado en base64. Este certificado se decodifica mediante el comando certutil.exe, se guarda como AppData%\vUCooUr.exe y luego se ejecuta. Una vez ejecutado, el descargador descargará un ejecutable de TeamViewer y usará el secuestro de DLL para descargar una DLL maliciosa, el malware MineBridge. Una vez que se carga MineBridge, los atacantes obtendrán acceso completo al equipo y les permitirán escuchar a través del micrófono del equipo infectado y realizar otras actividades maliciosas.

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.