PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 28 de abril de 2022

N° 117-2022-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 117	Fecha: 28-04-2022
		Página 3 de 9

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Implementan nuevo cargador de malware: “Bumblebee”		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de subfamilia	C02
Clasificación temática familia	Código Malicioso.		
Descripción			

I. DATOS GENERALES:

Actor de amenazas: TA579, posible identificador del actor de amenazas.
Investigador: Equipo de Proofpoint

Los investigadores descubrieron un nuevo cargador de malware que se usa en la naturaleza. La herramienta se llama "Bumblebee" y está asociada con varios conjuntos de ciberdelincuentes diferentes.

II. EVIDENCIA:

- El equipo que desarmó el nuevo cargador de malware está con la empresa de seguridad Proofpoint mientras estaba rastreando varios "conjuntos de amenazas de software delictivo" que anteriormente usaban un par de cargadores diferentes para propagar malware, llamados "BazaLoader” e "IcedID".
- BazaLoader es otro cargador popular utilizado para entregar malware de cifrado de archivos y desarrollado por la pandilla ahora desaparecida TrickBot, que desde entonces ha sido absorbida por Conti.
- Ahora parece que los equipos que usan BazaLoader han cambiado por completo a usar Bumblebee, ya que Proofpoint no ha detectado una sola instancia de la herramienta anterior desde febrero de 2022.
- Se dice que las campañas que distribuyen el nuevo cargador altamente sofisticado comenzaron en marzo de 2022, mientras se superponen con actividades maliciosas que conducen al despliegue de ransomware Conti y Diavol, lo que aumenta la posibilidad de que el cargador actúe como precursor de ataques de ransomware.

III. TEMA:

- Según Proofpoint, el cargador se puede usar como una herramienta para obtener acceso a una red y entregar cargas útiles secundarias, incluido el ransomware.
- Bumblebee se está utilizando en campañas de correo electrónico maliciosas.
- Las cadenas de ataque que distribuyen Bumblebee han tomado la forma de señuelos de phishing de correo electrónico con la marca DocuSign que incorporan enlaces fraudulentos o archivos adjuntos HTML, lo que lleva a las víctimas potenciales a un archivo ISO comprimido alojado en Microsoft OneDrive.
- El desarrollo también coincide con el hecho de que Conti se hizo cargo de la infame red de bots TrickBot y la cerró para centrarse en el desarrollo del malware BazarLoader y Anchor. No está claro de inmediato si Bumblebee es obra de los actores de TrickBot y si las filtraciones llevaron a la pandilla a abandonar BazaLoader en favor de un malware completamente nuevo.

IV. CONCLUSIÓN

- El investigador de malware de Cybereason, Eli Salem, en un análisis independiente, identificó puntos de similitudes entre Bumblebee y TrickBot, incluido el módulo de inyección web de este último y el uso de la misma técnica de evasión, lo que sugiere que los actores detrás de Bumblebee tienen acceso al código fuente de TrickBot.
- "La introducción del cargador Bumblebee en el panorama de amenazas de crimeware y su aparente reemplazo para BazaLoader demuestra la flexibilidad que tienen los actores de amenazas para cambiar rápidamente los TTP y adoptar nuevo malware", dijo Sherrod DeGrippo, vicepresidente de investigación y detección de amenazas en Proofpoint.
- "Además, el malware es bastante sofisticado y demuestra estar en desarrollo activo y continuo, introduciendo nuevos métodos para evadir la detección", agregó DeGrippo.

V. RECOMENDACIÓN

- Concientizar al equipo de trabajo en todos los niveles de la institución.
- Contar con soluciones de ciberseguridad vigentes y actualizadas.
- Contar con un plan de respuesta ante incidentes.

Fuentes de información	▪ hxxps://www.enhacke.com/2022/04/los-ciberdelincuentes-usan-el-nuevo-cargador-de-malware-bumblebee-en-estado-salvaje/ ▪ hxxps://www.cyclonis.com/es/los-piratas-informaticos-implementan-un-nuevo-cargador-de-malware-llamado-bumblebee/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 117	Fecha: 28-04-2022
		Página 5 de 9

Componente que reporta	**COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS**		
Nombre de la alerta	Agencias de ciberseguridad revelan las principales vulnerabilidades explotadas de 2021		
Tipo de ataque	Explotación de vulnerabilidades	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. El 17 de abril del 2022, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tuvo conocimiento que, en asociación con la NSA y el FBI, las autoridades de ciberseguridad de todo el mundo han publicado hoy una lista de las 15 principales vulnerabilidades explotadas de forma rutinaria por los actores de amenazas durante 2021.

2. A nivel mundial, se ha observado que los actores maliciosos concentran sus ataques en los sistemas que se enfrentan a Internet, incluidos los servidores de correo electrónico y de red privada virtual (VPN), utilizando exploits dirigidos a las vulnerabilidades recientemente reveladas. Con amplios objetivos, incluidos las organizaciones del sector público y privado.

3. Esto podría deberse a que los actores maliciosos y los investigadores de seguridad lanzaron exploits de prueba de concepto (POC) dentro de las dos semanas posteriores a la divulgación inicial de la mayoría de los principales errores explotados durante 2021. Así mismo, los atacantes centraron algunos de sus ataques en vulnerabilidades más antiguas parcheadas años antes, lo que demuestra que algunas organizaciones no actualizan sus sistemas incluso cuando hay un parche disponible.

4. La lista de las 15 fallas de seguridad más explotadas está disponible a continuación, con enlaces a las entradas de la base de datos nacional de vulnerabilidades y el malware asociado.

CVE	Vulnerabilidad	Proveedor y Producto	Tipo
CVE-2021-44228	Log4Shell	apache log4j	Ejecución remota de código (RCE)
CVE-2021-40539		Zoho ManageEngine AD SelfService Plus	RCE
CVE-2021-34523	ProxyShell	Servidor de Microsoft Exchange	Elevación de privilegio
CVE-2021-34473	ProxyShell	Servidor de Microsoft Exchange	RCE
CVE-2021-31207	ProxyShell	Servidor de Microsoft Exchange	Omisión de funciones de seguridad
CVE-2021-27065	ProxyLogon	Servidor de Microsoft Exchange	RCE
CVE-2021-26858	ProxyLogon	Servidor de Microsoft Exchange	RCE
CVE-2021-26857	ProxyLogon	Servidor de Microsoft Exchange	RCE
CVE-2021-26855	ProxyLogon	Servidor de Microsoft Exchange	RCE
CVE-2021-26084		Centro de datos y servidor de Atlassian Confluence	Ejecución de código arbitrario

CVE-2021-21972		Cliente VMware vSphere	RCE
CVE-2020-1472	inicio de sesión cero	Protocolo remoto de inicio de sesión de Microsoft (MS-NRPC)	Elevación de privilegio
CVE-2020-0688		Servidor de Microsoft Exchange	RCE
CVE-2019-11510		Pulso Seguro Pulso Conectar Seguro	Lectura de archivos arbitrarios
CVE-2018-13379		Fortinet FortiOS y FortiProxy	Travesía de ruta

5. Las agencias de seguridad cibernética de EE. UU., Australia, Canadá, Nueva Zelanda y el Reino Unido también identificaron y revelaron 21 vulnerabilidades de seguridad adicionales comúnmente explotadas por ciberdelincuente durante 2021, incluidas las que afectan a Accellion File Transfer Appliance (FTA), Windows Print Spooler y Pulse Secure. El aviso conjunto incluye medidas de mitigación que deberían ayudar a disminuir el riesgo asociado con las principales fallas abusadas detalladas anteriormente.

6. CISA y el FBI también publicaron una lista de las 10 fallas de seguridad más explotadas entre 2016 y 2019 y una lista de las fallas explotadas de manera rutinaria en 2020 en colaboración con el Centro de Seguridad Cibernética de Australia (ACSC) y el Centro Nacional de Seguridad Cibernética del Reino Unido (NCSC).

7. En noviembre de 2021, MITRE también compartió una lista de las fallas de seguridad de programación, diseño y arquitectura más peligrosas que afectan al hardware en 2021 y las 25 debilidades más comunes y peligrosas que afectan al software durante los dos años anteriores.

8. Recomendaciones:

   - Las autoridades de seguridad cibernética instan a las organizaciones en un aviso conjunto a corregir rápidamente estas fallas de seguridad e implementar sistemas de administración de parches para reducir su superficie de ataque.

Fuentes de información	▪ https://www.bleepingcomputer.com/news/security/cybersecurity-agencies-reveal-top-exploited-vulnerabilities-of-2021/ ▪ https://www.cisa.gov/uscert/ncas/alerts/aa22-117a#:~:text=RCE-,Mitigations,-Vulnerability%20and%20Configuration

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 117	Fecha: 28-04-2022
		Página 7 de 9

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Nueva variante de malware BotenaGo dirigida a dispositivos DVR de cámara de seguridad Lilin		
Tipo de ataque	Botnet	Abreviatura	Virus
Medios de propagación	IRC, USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código Malicioso.		

Descripción

FECHA DEL EVENTO:

A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 26 de abril del 2022, se tomó conocimiento de la publicación realizada en la página web de "**THE HACKERS NEW**", Una nueva variante de una botnet de IoT llamada BotenaGo ha surgido en la naturaleza, señalando específicamente los dispositivos DVR de la cámara de seguridad Lilin para infectarlos con malware Mirai.

ANTECEDENTES:

Apodado "Lilin Scanner" por Nozomi Networks, la última versión está diseñada para explotar una vulnerabilidad de inyección de comandos crítica de dos años en el firmware del DVR que fue parcheada por la compañía taiwanesa en febrero de 2020.

Apodado "Lilin Scanner" por Nozomi Networks, la última versión está diseñada para explotar una vulnerabilidad de inyección de comandos crítica de dos años en el firmware del DVR que fue parcheada por la compañía taiwanesa en febrero de 2020.

BotenaGo, documentado por primera vez en noviembre de 2021 por AT&T Alien Labs, está escrito en Golang y presenta más de 30 exploits para vulnerabilidades conocidas en servidores web, enrutadores y otros tipos de dispositivos IoT.

DETALLES:

Desde entonces, el código fuente de la botnet se ha cargado en GitHub, lo que la hace madura para el abuso por parte de otros actores criminales. "Con solo 2.891 líneas de código, BotenaGo tiene el potencial de ser el punto de partida para muchas nuevas variantes y nuevas familias de malware que utilizan su código fuente", dijeron los investigadores este año.

El nuevo malware BotenaGo es el último en explotar vulnerabilidades en dispositivos Lilin DVR después de Chalubo, Fbot y Moobot. A principios de este mes, el Laboratorio de Investigación de Seguridad de Red de Qihoo 360 (360 Netlab) detalló una botnet DDoS de rápida propagación llamada Fodcha que se ha propagado a través de diferentes fallas del Día N y contraseñas Telnet / SSH débiles.

Un aspecto crucial que diferencia a Lillin Scanner de BotenaGo es su dependencia de un programa externo para construir una lista de direcciones IP de dispositivos Lilin vulnerables, explotando posteriormente la falla antes mencionada para ejecutar código arbitrario de forma remota en el objetivo y desplegar cargas útiles Mirai.

Vale la pena señalar que el malware no puede propagarse de una manera similar a un gusano, y solo se puede usar para atacar las direcciones IP proporcionadas como entrada con los binarios de Mirai.

RECOMENDACIONES:

- Limitar el compartir red con otros equipos.
- Utilizar el filtrado de datos.
- Asegurar con capas extras nuestra red.
- Mejorar el monitoreo de red.
- Tener actualizado correctamente el sistema.
- Utiliza contraseñas fuertes y complejas.

Fuentes de información	▪ https://thehackernews.com/2022/04/new-botenago-malware-variant-targeting.html

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 117**	**Fecha: 28-04-2022**
		Página 8 de 9

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades en Cisco Firepower Management Center		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. Resumen:

Cisco ha reportado dos vulnerabilidades de severidad ALTA y MEDIO de tipo carga sin restricciones de archivo con tipo peligroso y secuencias de comandos entre sitios en Firepower Management Center (FMC). La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto autenticado eludir las protecciones de seguridad y cargar archivos maliciosos en el sistema afectado y realizar un ataque de secuencias de comandos entre sitios.

2. Detalles:

- La vulnerabilidad de tipo carga sin restricciones de archivo con tipo peligroso, se refiere a que el software permite al atacante cargar o transferir archivos de tipos peligrosos que pueden procesarse automáticamente dentro del entorno del producto.
- La vulnerabilidad identificada como CVE-2022-20743 de omisión de seguridad de carga de archivos en la interfaz de administración web del software Cisco Firepower Management Center podría permitir que un atacante remoto autenticado eluda las protecciones de seguridad y cargue archivos maliciosos en el sistema afectado. Esta vulnerabilidad se debe a una validación incorrecta de los archivos cargados en la interfaz de administración web del software Cisco FMC. Un atacante podría aprovechar esta vulnerabilidad cargando un archivo creado con fines malintencionados en un dispositivo que ejecute el software afectado. Una explotación exitosa podría permitir que el atacante almacene archivos maliciosos en el dispositivo, a los que podría acceder más tarde para realizar ataques adicionales, incluida la ejecución de código arbitrario en el dispositivo afectado con privilegios de root.
- La vulnerabilidad identificada como CVE-2022-20740 en la interfaz de administración basada en web del software Cisco Firepower Management Center podría permitir que un atacante remoto no autenticado realice un ataque de secuencias de comandos entre sitios. Esta vulnerabilidad se debe a una validación incorrecta de la entrada proporcionada por el usuario a la interfaz de administración basada en web. Un atacante podría explotar esta vulnerabilidad al convencer a un usuario de que haga clic en un enlace diseñado para pasar información maliciosa a la interfaz. Una explotación exitosa podría permitir al atacante realizar ataques de secuencias de comandos entre sitios y obtener acceso a información confidencial basada en el navegador.
- Cisco ha confirmado que estas vulnerabilidades no afectan al software Cisco Adaptive Security Appliance (ASA) ni al software Cisco Firepower Threat Defense (FTD).

3. Productos afectados:

Estas vulnerabilidades afectan a los productos de Cisco si ejecutan una versión vulnerable del software Cisco FMC:

- Firepower Management Center, versión: 6.2.2 y anteriores, 6.2.3, 6.3.0, 6.4.0, 6.5.0, 6.6.0, 6.7.0, 7.0.0 y 7.1.0.

4. Solución:

- Cisco recomienda actualizar el producto afectado a una versión fija disponible que corrige estas vulnerabilidades;
- Las versiones 6.2.2 y anteriores del software FMC y FTD de Cisco, así como las versiones 6.3.0 y 6.5.0, han llegado al final del mantenimiento del software. Se recomienda migrar a una versión compatible que incluya la solución para esta vulnerabilidad.

Fuentes de información	▪ hxxps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-security-bypass-JhOd29Gg ▪ hxxps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-SfpEcvGT

Índice alfabético