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, 20 de junio de 2022

N° 165-2022-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

Vulnerabilidad crítica de omisión de autenticación en múltiples productos HPE 4
CERT-In emite alertas de amenazas para múltiples productos de Adobe, Microsoft y otros....5
Nueva campaña de phishing que suplanta la identidad de AMAZON 6
BRATA Android Malware gana capacidades avanzadas de amenazas móviles 8
Expertos advierten sobre una nueva campaña de ransomware eCh0raix dirigida a los NAS de QNAP 9
Symbiote, un malware de Linux casi imposible de detectar 11
Índice alfabético 13

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 165**	**Fecha: 20-06-2022**
		Página 4 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica de omisión de autenticación en múltiples productos HPE		
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:**

   El equipo de respuesta de seguridad de productos de HPE ha reportado una vulnerabilidad de severidad CRÍTICA de tipo omisión de autenticación en las supercomputadoras HPE Cray EX/Soluciones de sistema Shasta y los conmutadores HPE Slingshot. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto evadir la autenticación de los dispositivos afectados.

2. **Detalles:**

   - La vulnerabilidad **crítica** identificada como CVE-2022-28620 de omisión de autenticación podría permitir a un atacante remoto evadir la autenticación de los dispositivos afectados. Esta vulnerabilidad se debe a cuando un actor afirma tener una identidad dada, el software no prueba o prueba insuficientemente que la afirmación es correcta.
   - Esta vulnerabilidad puede conducir a la exposición de recursos o funcionalidades a actores no deseados, posiblemente proporcionando a los atacantes información confidencial o incluso ejecutando código arbitrario.

3. **Productos afectados:**

   - Cray Legacy Shasta System Solutions: Todas las versiones del firmware del controlador de nodo asociadas con los blades refrigerados por líquido HPE Cray EX y todas las versiones del firmware del controlador de chasis asociadas con los armarios refrigerados por líquido HPE Cray EX anteriores a 1.6.27/1.5.33/1.4.27;
   - Las supercomputadoras HPE Cray EX: Todas las versiones del firmware del controlador de nodo asociadas con las cuchillas refrigeradas por líquido HPE Cray EX, y todas las versiones del firmware del controlador de chasis asociadas con los armarios refrigerados por líquido HPE Cray EX anteriores a 1.6.27/1.5.33/1.4.27;
   - HPE Slingshot: Todas las versiones de Slingshot anteriores a la 1.7.2 - Todos los controladores de conmutador HPE Slingshot.

4. **Solución:**

   HPE recomienda actualizar los productos afectados con la última versión de firmware disponible que corrige está vulnerabilidad:

   - HPE Olympus cCnC Firmware 1.6.22 (incluido en HPC Firmware Pack 22.04);
   - Shasta versión 1.5-FW0522;
   - Shasta versión 1.4.2A-FW0522;
   - HPE Slingshot Software versión 1.7.2.

   Estas versiones se pueden descargar desde el centro de soporte de HPE y, a continuación, seguir las instrucciones de instalación de la sección RESOLUTION del aviso del fabricante.

Fuentes de información	▪ hxxps://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbcr04284en_us ▪ hxxps://www.basquecybersecurity.eus/es/avisos/tecnicos/omision-autenticacion-productos-20220617.html

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 165**	**Fecha: 20-06-2022**
		Página 5 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	CERT-In emite alertas de amenazas para múltiples productos de Adobe, Microsoft y otros		
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:

El Equipo de Respuesta a Emergencias Informáticas Hindú (CERT-In), ha emitido una alerta de amenaza sobre múltiples vulnerabilidades que afectan a productos de Citrix, Adobe, Microsoft y Zimbra. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto eludir los controles de seguridad, generar una condición de denegación de servicio (DoS), obtener privilegios elevados, ejecutar código arbitrario, escribir archivos arbitrarios en el sistema de archivos y provocar pérdidas de memoria en el sistema de destino, así como realizar ataques de suplantación de identidad y ejecutar sistemas específicos.

2. Detalles:

- CERT-In indicó que las vulnerabilidades en Citrix Application Delivery Management (ADM), podría permitir a un atacante remoto eludir la seguridad y denegar el servicio en los sistemas afectados. La vulnerabilidad permite a un atacante solicitar que el sistema se corrompa y restablezca la contraseña del administrador en el próximo reinicio del dispositivo. Las vulnerabilidades también se pueden usar para enviar solicitudes especialmente diseñadas y evitar que se renueven o emitan nuevas licencias y pueden resultar en una denegación de servicios en el sistema afectado.
- Asimismo, las vulnerabilidades en múltiples productos de Adobe, podría permitir a un atacante remoto obtener privilegios elevados, ejecutar código arbitrario, escribir archivos arbitrarios en el sistema de archivos y provocar pérdidas de memoria en el sistema de destino. Estas vulnerabilidades existen debido a una validación de entrada incorrecta, una autorización incorrecta, un desbordamiento de búfer basado en montón que pueden ser aprovechadas por un atacante al persuadir a su víctima para que abra archivos o aplicaciones especialmente diseñados para obtener privilegios elevados y causar fugas de memoria.
- Por otro lado, las vulnerabilidades en Microsoft Windows, Office Microsoft Net Framework, Microsoft Azure, SharePoint Server, SQL Server, Microsoft 365, Microsoft Visual Studio, Microsoft System Center Operations Manager y Microsoft Browser, podrían permitir a un atacante remoto realizar ataques para acceder a información confidencial, eludir las restricciones de seguridad, realizar ataques de denegación de servicio, ataques de suplantación de identidad y ejecutar sistemas específicos.
- Por último, CERT-In informó sobre las vulnerabilidades en el correo web de Zimbra que los atacantes pueden aprovechar para ejecutar código arbitrario de forma remota y obtener información confidencial en los sistemas objetivos. Las vulnerabilidades existen debido al envenenamiento de Memcached con solicitudes no autenticadas y puede explotarse enviando solicitudes especialmente diseñadas al sistema de destino.

3. Productos afectados:

- Citrix Application Delivery Management (ADM);
- Productos Adobe;
- Productos Microsoft: Microsoft Windows, Office Microsoft Net Framework, Microsoft Azure, SharePoint Server, SQL Server, Microsoft 365, Microsoft Visual Studio, Microsoft System Center Operations Manager y Microsoft Browser;
- Correo web de Zimbra, versiones anteriores a la 9.0.0 P24.

4. Solución:

CERT-In recomienda actualizar los productos afectados con la última versión de software disponible que corrigen estas vulnerabilidades.

Fuentes de información	▪ hxxps://www.thehindu.com/sci-tech/technology/cert-in-issues-threat-alerts-for-adobe-microsoft-and-others/article65542485.ece?&web_view=true

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 165	Fecha: 20-06-2022
		Página 6 de 13

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de phishing que suplanta la identidad de AMAZON		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de subfamilia	G02
Clasificación temática familia	Fraude		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de phishing que se difunde por medio de los diferentes navegadores web, suplantando la identidad de la plataforma de comercio electrónico "Amazon", con el objetivo robar credenciales de acceso, datos personales y/o bancarios.

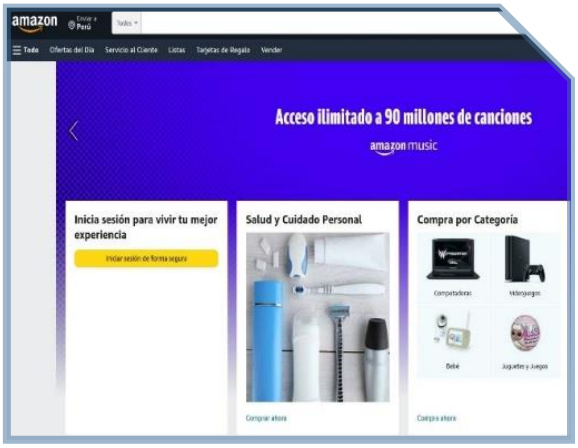
2. Proceso del ataque phishing:

Imagen 1: Sitio web que suplanta la identidad de Amazon, solicita a la víctima ingresar sus credenciales de acceso (correo electrónico y contraseña).

Imagen 2: Después de que, se ingresó las credenciales de acceso, solicita actualizar los datos de la tarjeta de crédito o débito (número de tarjeta, fecha de caducidad y CVC).

Imagen 3: Una vez que, se actualizo los datos de la tarjeta requiere completar el siguiente formulario (ultimo 4 dígitos del SSN, Estado, Ciudad, Código postal, fecha de nacimiento, teléfono y dirección de envió).

Imagen 4: Pasado unos 20 segundos, es redirigido al sitio web oficial de Amazon, aludiendo un aparente error de autenticación, sin embrago; los datos fueron capturado por los ciberdelincuentes.



3. Comparación del sitio web oficial y sitio web fraudulento:

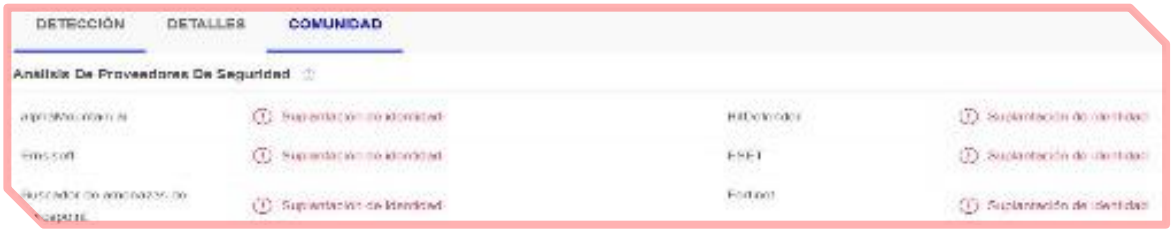
SITIO WEB OFICIAL
URL: https://www.amazon.com/

SITIO WEB FRAUDULENTO
URL: hXXp[:]//azlikwjsj[.]com/amazon-RD292-user-card-detail-em-thank

El sitio apócrifo utiliza el diseño gráfico de Amazon, para engañar a la víctima. La URL hXXp[:]//azlikwjsj[.]com/amazon-RD292-user-card-detail-em-thank del sitio web fraudulento **NO POSEE EL PROTOCOLO DE SEGURIDAD DE RED** (https).

4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo la siguiente información:

- URL : hXXp[:]//azlikwjsj[.]com/amazon-RD292-user-card-detail-em-thank
- Dominio : azlikwjsj[.]com
- IP. : 192[.]185[.]76[.]248
- Tamaño : 8.68 KB
- SHA-256 :d676ed256c90735592555b7fa0d814cbd5348a219548dd3bfc36760bdf6bc45a



5. Referencia:

- Phishing o suplantación de identidad: Es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.

6. Recomendaciones:

- Evitar acceder a enlaces que forman aparte de un contenido de mensajes texto.
- Evitar proporcionar información confidencial por teléfono, WhatsApp, mensaje de texto, correo electrónico o redes sociales, a través de enlaces.
- Verificar la procedencia de los mensajes texto, en fuentes oficiales de la entidad que provee algún servicio o producto.
- Contar con una solución de seguridad, constantemente actualizada tanto en dispositivos de escritorio como en móviles, ya que sirven como barrera inicial protectora ante sitios web maliciosos.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 165	Fecha: 20-06-2022
		Página 8 de 13

Componente que reporta	**EL CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	BRATA Android Malware gana capacidades avanzadas de amenazas móviles		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	Red, Correo, navegación por Internet, Sistema operativo Android		
Código de familia	C	Código de subfamilia	C02
Clasificación temática familia	Código Malicioso		

Descripción

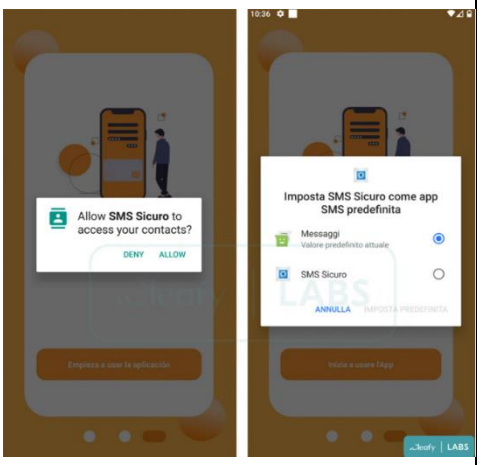
1. **Fecha del evento:**

A través del monitoreo y búsqueda de amenazas en el ciberespacio el 19 de junio del 2022 se tomó conocimiento de la publicación realizada en https://thehackernews.com/ sobre BRATA Android Malware que realiza sus ataques contra las aplicaciones financieras para que sean más sigilosos.

2. **Antecedentes:**

- Acrónimo de "Brazilian Remote Access Tool Android", BRATA se detectó por primera vez en estado salvaje en Brasil a fines de 2018, antes de hacer su primera aparición en Europa en abril pasado, mientras se hacía pasar por software antivirus y otras herramientas de productividad comunes para engañar a los usuarios para que las descargaran. El cambio en el patrón de ataque, que escaló nuevos máximos a principios de abril de 2022, implica adaptar el malware para atacar una institución financiera específica a la vez, cambiando a un banco diferente sólo después de que la víctima comience a implementar contramedidas contra la amenaza.

3. **Detalles:**



- Las aplicaciones no autorizadas también incorporan nuevas características que le permiten hacerse pasar por la página de inicio de sesión de la institución financiera para recopilar credenciales, acceder a mensajes SMS y transferir una carga útil de segunda etapa ("unrar.jar") desde un servidor remoto para registrar eventos. en el dispositivo comprometido.
- "La combinación de la página de phishing con la posibilidad de recibir y leer los sms de la víctima podría usarse para realizar un ataque completo de adquisición de cuenta (ATO)", dijeron los investigadores.
- Además, Cleafy dijo que encontró una muestra de paquete de aplicación de Android separada ("SMSAppSicura.apk") que usaba la misma infraestructura de comando y control (C2) que BRATA para desviar mensajes SMS, lo que indica que los actores de amenazas están probando diferentes métodos para ampliar su alcance. Se dice que la aplicación de robo de SMS identifica específicamente a los usuarios en el Reino Unido, Italia y España, y su objetivo es poder interceptar y filtrar todos los mensajes entrantes relacionados con contraseñas de un sólo uso enviadas por los bancos.
- "Por lo general, se enfocan en entregar aplicaciones maliciosas dirigidas a un banco específico durante un par de meses y luego pasar a otro objetivo".

4. **Recomendaciones:**

- La primera medida de protección frente a este tipo de ataques es tener cuidado de qué tipo de archivo se está descargando y que no se ejecute en segundo plano algún otro proceso.
- Utilizar la plataforma de Virus Total para analizar los archivos que se pretende descargar, así como las direcciones de las páginas web que se visita.
- No abrir ningún archivo de dudosa procedencia, debido a que el malware todavía se sigue desarrollando. Es recomendable descargar aplicaciones directamente de la tienda de aplicaciones.

Fuentes de información	▪ hxxps://thehackernews.com/2022/06/brata-android-malware-gains-advanced.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 165	Fecha: 20-06-2022
		Página 9 de 13

Componente que reporta	**EL CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Expertos advierten sobre una nueva campaña de ransomware eCh0raix dirigida a los NAS de QNAP		
Tipo de ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	IRC, USB, Disco, Red, Correo, navegación por Internet		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. **Fecha del evento:**

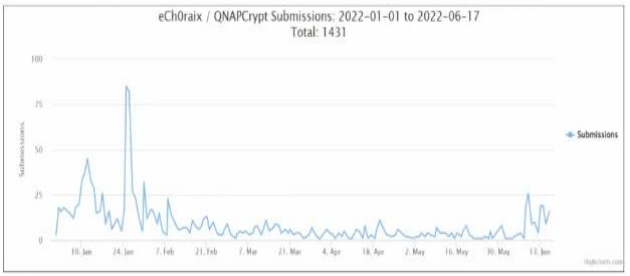
A través del monitoreo y búsqueda de amenazas en el ciberespacio el 19 de junio del 2022 se tomó conocimiento de la publicación realizada en https://securityaffairs.co/ sobre el ransomware ech0raix dirigida a los dispositivos de almacenamiento conectado a la red (NAS) de QNAP.

2. **Antecedentes:**

- Los investigadores de Bleeping Computer y MalwareHunterTeam, citando informes de usuarios y presentaciones de muestra en la plataforma ID Ransomware, advierten sobre una nueva ola de ataques de ransomware ech0raix dirigidos a dispositivos QNAP Network Attached Storage (NAS).

3. **Detalles:**

- El ransomware, rastreado por Intezer como " QNAPCrypt " y " eCh0raix " por Anomali, está escrito en el lenguaje de programación Go y utiliza cifrado AES para cifrar archivos. El código malicioso agrega la extensión encrypt a los nombres de archivo de los archivos cifrados". El ransomware ha estado activo desde al menos 2019, la última ola de ataques ech0raix se descubrió en diciembre de 2021, en el momento en que los operadores de ransomware exigían un aumento de rescate de .024 ($ 1,200) hasta .06 bitcoins ($ 3,000). El proveedor taiwanés fue informado de los continuos ataques de ransomware eCh0raix que infectaron los dispositivos NAS de QNAP usando contraseñas débiles. Expertos independientes observaron un aumento en los informes de infección por eCh0raix entre el 19 y el 26 de abril de 2021.



ech0raix ransomware activity (ID Ransomware)

- En mayo, la empresa emitió la alerta en respuesta a una nueva ola de ataques de ransomware DeadBolt dirigidos a dispositivos NAS que utilizan QTS 4.3.6 y QTS 4.4.1. El proveedor taiwanés pidió a los usuarios que instalaran la última actualización en sus dispositivos NAS y evitaran exponerlos en Internet.
- "QNAP® Systems, Inc. detectó recientemente un nuevo ataque de DEADBOLT Ransomware. Según la investigación realizada por el Equipo de respuesta a incidentes de seguridad de productos de QNAP (QNAP PSIRT), el ataque se dirigió a dispositivos NAS que usaban QTS 4.3.6 y QTS 4.4.1, y los modelos afectados eran principalmente las series TS-x51 y TS-x53". lee el aviso publicado por la empresa. "QNAP insta a todos los usuarios de NAS a verificar y actualizar QTS a la última versión lo antes posible y evitar exponer su NAS a Internet".
- Desde enero, los operadores de ransomware DeadBolt apuntan a los dispositivos NAS de QNAP en todo el mundo, sus operadores afirman la disponibilidad de un exploit de día cero que les permite cifrar el contenido de los sistemas infectados.

4. **Recomendaciones:**

- La primera medida de protección frente a este tipo de ataques es tener cuidado de qué tipo de archivo se está descargando y que no se ejecute en segundo plano algún otro proceso.

- Utilizar la plataforma de Virus Total para analizar los archivos que se pretende descargar, así como las direcciones de las páginas web que se visita.
- No abrir ningún documento de dudosa procedencia, debido a que el malware todavía se sigue desarrollando.

Fuentes de información	▪ hxxps://securityaffairs.co/wordpress/132410/cyber-crime/ech0raix-ransomware-attacks.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 165	Fecha: 20-06-2022
		Página 11 de 13

Componente que reporta	**EL CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Symbiote, un malware de Linux casi imposible de detectar		
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

FECHA DEL EVENTO:

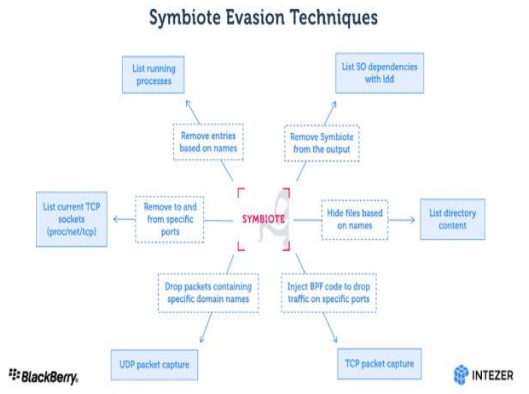
A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 19 de junio del 2022, se tomó conocimiento a través de la publicación realizada en la página web de **"BLEEPING COMPUTER"**, Un malware linux recién descubierto conocido como Symbiote infecta todos los procesos en ejecución en sistemas comprometidos, roba las credenciales de la cuenta y brinda a sus operadores acceso de puerta trasera. Después de inyectarse en todos los procesos en ejecución, el malware actúa como un parásito en todo el sistema, sin dejar signos identificables de infección incluso durante meticulosas inspecciones en profundidad.

ANTECEDENTES:

- El nombre proviene del concepto de simbionte que es un organismo que vive en simbiosis con otro organismo, exactamente como lo hace este implante con los sistemas infectados. Por esta razón, los investigadores de seguridad definieron esta amenaza como casi imposible de detectar.
- Symbiote utiliza la funcionalidad de enganche BPF (Berkeley Packet Filter) para olfatear paquetes de datos de red y ocultar sus propios canales de comunicación de las herramientas de seguridad.

DETALLES:

- Una vez que el malware ha infectado una máquina, se oculta a sí mismo y a cualquier otro malware utilizado por el actor de la amenaza, lo que hace que las infecciones sean muy difíciles de detectar. Realizar análisis forenses en vivo en una máquina infectada puede no mostrar nada, ya que todos los archivos, procesos y artefactos de red están ocultos por el malware.
- Además de la capacidad de rootkit, el malware proporciona una puerta trasera para que el actor de amenazas inicie sesión como cualquier usuario en la máquina con una contraseña codificada y ejecute comandos con los privilegios más altos. Dado que es extremadamente evasivo, es probable que una infección por simbiontes "vuele bajo el radar".
- Cuando un administrador inicia cualquier herramienta de captura de paquetes en la máquina infectada, el código de bytes BPF se inyecta en el kernel que define qué paquetes deben capturarse. En este proceso, Symbiote agrega primero su código de bytes para que pueda filtrar el tráfico de red que no desea que vea el software de captura de paquetes.
- Symbiote puede ser cargado por el enlazador a través de la directiva LD_PRELOAD antes que cualquier otro objeto compartido que permita "secuestrar las



importaciones" de los otros archivos de biblioteca cargados para la aplicación.

RECOMENDACIONES

- Revisar la dirección del remitente de los correos que recibes.
- Evitar hacer clic en anuncios emergentes ya que suelen conducir a la descarga del software malicioso.
- Mantener actualizado el antivirus y asegurarse de contar con protección anti-malware.
- Realizar copias de seguridad frecuentes de los datos, no solo en servicios de nube, sino también en un transporte físico de datos, como una unidad SSD móvil o un disco duro HDD con conexión USB.

Fuentes de información	▪ https://securityaffairs.co/wordpress/132113/malware/symbiote-linux-malware.html

Índice alfabético

ciberdelincuentes 6
ciberespacio 6, 8, 9, 11
código arbitrario 5
denegación de servicio (DoS) 5
firmware 4
malware 8, 11
Malware 8
phishing 6
Phishing 7
ransomware 9
vulnerabilidad 4
vulnerabilidades 5