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

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

181-2024-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 Aéreadel 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 lasempresas 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°181	Fecha: 07-08-2024
		Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Presencia del ransomware Akira en redes del Ecuador		
Tipo de Ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

El malware Akira de tipo ransomware fue identificado en marzo de 2023 y es operado por un grupo que ha estado activo desde entonces realizando diferentes campañas donde ha impactado a muchas víctimas, la mayoría de ellas localizadas en los Estados Unidos, Europa y Australia; así también han sido afectadas por estos ataques algunas industrias que incluye educación, finanzas, bienes raíces, construcción, salud; prestadores de Servicios de Telecomunicaciones, entre otras. En abril de 2023, tras un enfoque inicial en los sistemas Windows, los actores de amenazas de Akira implementaron una variante de Linux dirigida a las máquinas virtuales VMware ESXi. Al 1 de enero de 2024, el grupo de ransomware ha afectado a más de 250 organizaciones y ha obtenido aproximadamente 42 millones de dólares en ganancias por ransomware.

2. DETALLES:

El grupo de ransomware tiene como estrategia la doble extorsión donde no solo cifran los datos, sino que también exfiltran información sensible, amenazando con venderla o filtrarla públicamente si no se cumple con el pago del rescate. Esta estrategia aumenta las posibilidades de pago de las víctimas y, para apoyarla técnicamente, el grupo cuenta con un sitio web de estilo retro en la red Tor, donde hacen públicos los datos robados si las víctimas no pagan el rescate demandado. Además, en dicho sitio web también ofrecen una función de chat para que las víctimas puedan comunicarse con ellos utilizando un ID único que incluyen para cada una en la nota de rescate.

Al igual que la mayoría de ransomware, Akira utiliza criptografía simétrica y asimétrica para cifrar los ficheros en los equipos de sus víctimas. En concreto, cuando se ejecuta Akira calcula una clave de cifrado y vector de inicialización aleatorios para el algoritmo Chacha20. Estos valores son cifrados con RSA a través de una clave pública que se encuentra embebida en el propio código y que los actores cambian por cada víctima. A diferencia de Conti, en el que se basa su código, y de la mayoría de ransomware, Akira calcula una única clave de cifrado que es utilizada para cifrar todos los ficheros. Por tanto, si se averigua esta clave, se podrían llegar a descifrar.

El FBI y los investigadores de ciberseguridad han observado que los actores de amenazas de Akira obtienen acceso inicial a las organizaciones a través de un servicio de red privada virtual (VPN) sin autenticación multifactor (MFA) configurada, principalmente utilizando vulnerabilidades conocidas de Cisco CVE-2020-3259 y CVE-2023-20269. Los métodos adicionales de acceso inicial incluyen el uso de servicios externos como el Protocolo de escritorio remoto (RDP), phishing selectivo y el abuso de credenciales válidas.

Una vez obtenido el acceso inicial, los actores de amenazas de Akira intentan abusar de las funciones de los controladores de dominio mediante la creación de nuevas cuentas de dominio para establecer la persistencia. En algunos casos, el FBI identificó a los actores de amenazas de Akira creando una cuenta administrativa denominada itadm.

Los actores de amenazas de Akira aprovechan herramientas como FileZilla, WinRAR, WinSCP y RClone para exfiltrar datos. Para establecer canales de comando y control, los actores de amenazas aprovechan herramientas fácilmente disponibles como AnyDesk, MobaXterm, RustDesk, Ngrok y Cloudflare Tunnel, lo que permite la exfiltración a través de varios protocolos como el Protocolo de transferencia de archivos (FTP), el Protocolo de transferencia segura de archivos (SFTP) y servicios de almacenamiento en la nube como Mega para conectarse a servidores de exfiltración.

INDICADORES DE COMPROMISO

Nombre del Archivo	Hash (SHA-256)	Descripción
w.exe	d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca	Akira ransomware
Win.exe	dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e	Cifrador del ransomware Akira
AnyDesk.exe	bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138	Aplicación de escritorio remoto
Gcapi.ddl	73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf	Archivo DLL que ayuda a ejecutar AnyDesk.exe
Sysmon.exe	1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386	Herramienta Ngrok para persistencia
Config.yml	Varies by use	Archivo de configuración Ngrok
Rclone.exe	aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9	Herramienta de exfiltración
Winscp.md	7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4	Programa de transferencia de archivos de red
WinSCP-6.1.2-Setup.exe	36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c068b13c	Programa de transferencia de archivos de red
Akira_V2	3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75 0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c	Akira_v2 ransomware
Megazord	ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fc dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198 131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07 9f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e04426c 9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065 2f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c83 7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be 95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a 0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d C9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0	Akira “Megazord” ransomware

Nombre del Archivo	Hash (SHA-256)	Descripción
VeeamHax.exe	aaa6041912a6ba3cf167ecdb90a434a62feaf08639c59705847706b9f492015d	Herramienta de filtración de credenciales de texto sin formato
Veeam-Get-Creds.ps1	18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88	Script de PowerShell para obtener y descifrar cuentas de servidores Veeam
PowershellKerberosTicketDumper	5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a307d32	Herramienta de volcado de tickets Kerberos desde caché LSA
sshd.exe	8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee002d694	Backdoor OpenSSH
Ipscan-3.9.1-setup.exe	892405573aa34dfc49b37e4c35b655543e88ec1c5e8ffb27ab8d1bbf90fc6ae0	Escáner de red que escanea direcciones IP y puertos

Nombre del Archivo	Hash (MDA)	Descripción
Winrar-x64-623.exe	7a647af3c112ad805296a22b2a276e7c	Programa de transferencia de archivos en red

Hash (SHA-256)

- 0b5b31af5956158bfbd14f6cbf4f1bca23c5d16a40dbf3758f3289146c565f43
- 0d700ca5f6cc093de4abba9410480ee7a8870d5e8fe86c9ce103eec3872f225f
- a2df5477cf924bd41241a3326060cc2f913aff2379858b148ddec455e4da67bc
- 03aa12ac2884251aa24bf0ccd854047de403591a8537e6aba19e822807e06a45
- 2e88e55cc8ee364bf90e7a51671366efb3dac3e9468005b044164ba0f1624422
- 40221e1c2e0c09bc6104548ee847b6ec790413d6ece06ad675fff87e5b8dc1d5
- 5ea65e2bb9d245913ad69ce90e3bd9647eb16d992301145372565486c77568a2
- 643061ac0b51f8c77f2ed202dc91afb9879f796ddd974489209d45f84f644562
- 6f9d50bab16b2532f4683eeb76bd25449d83bdd6c85bf0b05f716a4b49584f84
- fef09b0aa37cbdb6a8f60a6bd8b473a7e5bffdc7fd2e952444f781574abccf64

3. RECOMENDACIONES:

- Realizar el bloqueo de los indicadores de compromiso listados.
- Deshabilitar los puertos de acceso remoto/Protocolo de escritorio remoto (RDP) no utilizados y monitorear los registros de acceso/RDP.
- Ejecutar la estrategia 3-2-1-1-0 de copias de seguridad, que consiste en realizar periódicamente tres copias de seguridad de los datos, en mínimo dos medios de almacenamiento diferentes, y albergar una de las copias fuera del sitio o en la nube; además una de las copias esté disponible fuera de conexión, y cero copias sin verificar o con errores.

- Cifrar las copias realizadas. Así, incluso si se ven comprometidas, serían indescifrables e inútiles para el atacante.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Habilitar la autenticación multifactor para todos los servicios en la medida de lo posible, en particular para correo web, redes privadas virtuales y cuentas que acceden a sistemas críticos.
- Implementar el principio del privilegio mínimo para minimizar el impacto potencial de las infecciones de ransomware.
- Desactivar las actividades y permisos de línea de comandos y secuencias de comandos. La escalada de privilegios y el movimiento lateral a menudo dependen de utilidades de software que se ejecutan desde la línea de comandos. Si los actores de amenazas no pueden ejecutar estas herramientas, tendrán dificultades para escalar privilegios y/o moverse lateralmente.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad.
- Segmentar las redes para evitar la propagación de ransomware. La segmentación de la red puede ayudar a prevenir la propagación de ransomware al controlar los flujos de tráfico entre varias subredes y el acceso a ellas, y al restringir el movimiento lateral del adversario.
- Revisar los controladores de dominio, servidores, estaciones de trabajo y directorios activos en busca de cuentas nuevas o no reconocidas.
- Filtrar el tráfico de la red al evitar que orígenes desconocidos o no confiables accedan a servicios remotos en sistemas internos. Esto evita que los actores de amenazas se conecten directamente a los servicios de acceso remoto que han establecido para la persistencia.
- Utilizar un software antimalware confiable en sus dispositivos y mantenerlos actualizados. Estos programas pueden detectar y eliminar ransomware y otro software malicioso antes de que puedan cifrar sus archivos.
- Implementar soluciones de seguridad avanzadas, como sistemas de detección y respuesta de endpoints (EDR), y software de detección y prevención de intrusiones (IDS/IPS), para identificar y bloquear comportamientos sospechosos antes de que causen daños significativos.
- Centrar la estrategia de defensa en la detección de movimientos laterales y el bloqueo de actividades fraudulentas de transferencia de datos confidenciales a Internet (fuga de informaciones). Es importante prestar especial atención al tráfico saliente para detectar las conexiones de los ciberdelincuentes en su red.
- Implementar una solución de filtrado de contenido web que bloquee el acceso a sitios web maliciosos o de alto riesgo. Esto puede evitar que los usuarios accedan accidentalmente a páginas que contienen descargas de ransomware o enlaces a sitios comprometidos.
- Considerar agregar un banner de correo electrónico a los correos electrónicos recibidos desde fuera de su organización.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://www.ecucert.gob.ec/wp-content/uploads/2024/08/Ransomware_Akira.pdf

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°181	Fecha: 07-08-2024
		Página: 8 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en Amazon Linux AMI		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **ANTECEDENTES:**

Se ha reportado una vulnerabilidad de severidad **ALTA** de tipo desbordamiento de búfer que afecta a todas las versiones de Amazon Linux AMI. La explotación exitosa de esta vulnerabilidad podría permitir a un a un usuario local aumentar privilegios en el sistema.

2. **DETALLES:**

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-39480 de tipo desbordamiento de búfer que afecta a todas las versiones de Amazon Linux AMI. La vulnerabilidad existe debido a una corrupción de memoria dentro de la función kdb_printf() en kernel/debug/kdb/kdb_io.c. Un usuario local puede aumentar los privilegios en el sistema.

Esta vulnerabilidad puede explotarse localmente. El atacante debe tener credenciales de autenticación y autenticarse correctamente en el sistema.

A. **Productos afectados:**

- Amazon Linux AMI: todas las versiones.
- Kernel de Linux: anterior a la versión 4.14.349-188.564.

3. **RECOMENDACIÓN:**

- Actualizar los paquetes afectados a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxp://alas.aws.amazon.com/ALAS-2024-1945.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°181		Fecha: 07-08-2024
			Página: 9 de 10
Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica de cambio de contraseña local en Cisco Smart Software Manager		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo cambio de contraseña local en Cisco Smart Software Manager. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado cambiar la contraseña de cualquier usuario, incluidos los usuarios administrativos.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-20419 de tipo cambio de contraseña local en el sistema de autenticación de Cisco Smart Software Manager On-Prem (SSM On-Prem) podría permitir que un atacante remoto no autenticado cambie la contraseña de cualquier usuario, incluidos los usuarios administrativos.

Esta vulnerabilidad se debe a una implementación incorrecta del proceso de cambio de contraseña. Un atacante podría aprovechar esta vulnerabilidad enviando solicitudes HTTP diseñadas a un dispositivo afectado. Una explotación exitosa podría permitir a un atacante acceder a la interfaz de usuario web o API con los privilegios del usuario afectado.

Cabe señalar que, Cisco SSM On-Prem y Cisco SSM Satellite son el mismo producto. En las versiones anteriores a la 7.0, este producto se denominaba Cisco SSM Satellite. A partir de la versión 7.0, este producto se denomina Cisco SSM On-Prem.

A. Productos afectados:

- Esta vulnerabilidad afecta a Cisco SSM On-Prem y Cisco Smart Software Manager Satellite (SSM Satellite).

3. RECOMENDACIÓN:

- Actualizar los paquetes afectados a la última versión disponible que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-auth-sLw3uhUy

Índice alfabético