	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 130	**Fecha: 03-06-2023**
		Página 14 de 27

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Nueva variante de malware “Legion” que recolecta credenciales de SSH y AWS		
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

ANTECEDENTES:

El 30 de mayo del 2023, a través del monitoreo y búsqueda de amenazas en el Ciberespacio, se tomó conocimiento que, el pasado mes de abril, fue descubierto un malware tipo Infostelar que tiene por objetivo obtener la mayor cantidad de información de un sistema, para luego venderla en mercados clandestinos. Este recolector de credenciales fue llamado “Legion”, está programado en Python y según los últimos hallazgos tendría capacidades adicionales para apuntar a servicios en la nube. Estas últimas variantes tienen como objetivo las credenciales asociadas con aplicaciones web de Laravel y los servidores SSH.

DETALLES:

Explotación de servicios en la nube

Según una investigación desarrollada por Cabo Labs, este malware roba las credenciales de los servidores web mal configurados que ejecutan marcos PHP como Laravel, para ello busca los archivos de variables de entorno (.env) en las rutas predeterminadas donde residen estos archivos en la máquina infectada. La variante actualizada incluye varias rutas nuevas para buscar archivos de entorno, estas se detallan a continuación:

/lib/.env	/saas/.env
/lab/.env	/api/.env
/cronlab/.env	/psnlink/.env
/cron/.env	/exapi/.env
/core/app/.env	/site/.env
/core/Datavase/.env(sic)	/web/.env
/database/.env	/en/.env
/config/.env	/tools/.env
/apps/.env	/v1/.env
/uploads/.env	/v2/.env
/sitemaps/.env	/administrator/.env

Si el servidor se encuentra mal configurado y con acceso público a internet, el malware guarda los archivos del entorno. En las últimas muestras analizadas se identifica que el malware intenta recuperar las credenciales de tres servicios específicos: DynamoDB, Amazon CloudWatch y AWS Owl.

La variante anterior ya era capaz de robar credenciales de una gran cantidad de servicios SMTP como:

- Proveedores de correo electrónico.
- Plataformas de pago.
- Bases de datos.
- Sistemas de administración de servidores.
- Otros servicios de proveedores en la nube.

Ataques a servidores SSH

La versión más reciente de "Legion" está equipada con la capacidad de atacar servidores de SSH, de la siguiente forma:

- Hace uso de la biblioteca Paramiko para analizar la lista de credenciales de base de datos exfiltradas y obtener pares disponibles de nombres de usuario y contraseñas.
- Esta lista de credenciales luego es utilizada para iniciar sesión en el host a través de SSH.
- En las variantes anteriores esta funcionalidad no funcionaba correctamente, pero ahora en las últimas v versiones analizadas ya está habilitada.

RECOMENDACIONES:

- Realizar una revisión en detalle de la correcta configuración del servidor independientemente que esté o no expuesto a internet, ya que Legion se aprovecha de estas configuraciones incorrectas como principal método de intrusión.
- Efectuar auditorías periódicas de los dispositivos digitales expuestos a internet, con ello evitamos una posible intrusión.
- Evitar usar rutas y nombres de carpetas predeterminadas para almacenar archivos importantes en el entorno expuesto a internet, esto facilita el reconocimiento automatizado por parte de los ciber actores.
- Implementar medidas de seguridad adicionales para proteger puertos específicos expuestos a internet.

Fuentes de información	▪ hxxps://portal-cci--entel-cl.translate.goog/Threat_Intelligence/Boletines/1606/?_x_tr_sl=auto&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=wapp

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 130	**Fecha: 03-06-2023**
		Página 22 de 27

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Vulnerabilidad de DoS afecta a OpenSSL		
Tipo de ataque	DOS	Abreviatura	DOS
Medios de propagación	Correo electrónico, redes sociales y entre otros		
Código de familia	F	Código de subfamilia	F01
Clasificación temática familia	Código malicioso		

Descripción

ANTECEDENTES:
El 01 de junio del 2023, a través del monitoreo y búsqueda de amenazas en el Ciberespacio, se tomó conocimiento que, una vulnerabilidad de ataque de denegación de servicios que afecta a OpenSSL.

DETALLES:
Las aplicaciones que usan OBJ_obj2txt() directamente o cualquiera de los subsistemas OpenSSL OCSP, PKCS7/SMIME, CMS, CMP/CRMF o TS sin límite de tamaño de mensaje pueden experimentar retrasos notables o muy largos al procesar esos mensajes, lo que puede dar lugar a una denegación de servicio.

Un object identifier se compone de una serie de números y sub identificadores, la mayoría de los cuales no tienen límite de tamaño. OBJ_obj2txt() se puede usar para traducir un object identifier ASN.1 dado en formato de codificación DER (usando el tipo OpenSSL ASN1_OBJECT) a su formato de texto numérico canónico, que son los sub identificadores del object identifier en formato decimal, separados por puntos.
Cuando uno de los sub identificadores en el object identifier es muy grande (estos son tamaños que se consideran absurdamente grandes, ocupando decenas o cientos de KiB), la traducción a un número decimal en el texto puede llevar mucho tiempo, lo que se consideraría como un posible DoS.
Las correcciones para esta vulnerabilidad se han aplicado en las siguientes versiones, entendiendo que OpenSSL 3.0.x y 3.1.x son vulnerables a este problema. En cambio los usuarios de OpenSSL 1.1.1 y 1.0.2 pueden verse afectados por este problema al llamar a OBJ_obj2txt() directamente.

- **OpenSSL 3.0:** Se introdujo el soporte para buscar algoritmos criptográficos usando nombres/identificadores en forma de cadena. Esto incluye el uso de object identifier en formato de texto numérico canónico como identificadores para obtener algoritmos.
- **OpenSSL 3.0 y posteriores:** Para estas versiones afecta a los subsistemas OCSP, PKCS7/SMIME, CMS, CMP/CRMF o TS. También afecta a cualquiera que procese certificados X.509, incluidas tareas simples como verificar su firma.
- **OpenSSL 1.1.1 y 1.0.2:** Estas versiones solo afectan la visualización de diversos objetos como los certificados X.509 a diferencia de las otras versiones mencionadas, por lo cual estas no provocan una situación de denegación de servicio (DoS) disminuyendo así su gravedad.

RECOMENDACIONES:

- Instalar las actualizaciones del fabricante disponibles en medios oficiales del proveedor previo análisis del impacto que podría provocar en los servicios críticos.
- Usar software antimalware u otras herramientas de seguridad capaces de detectar y bloquear variantes conocidas de DOS.
- Supervisar el tráfico de red y buscar indicadores de compromiso, como patrones de tráfico de red inusuales o comunicación con servidores de comando y control conocidos.

Fuentes de información	▪ hxxps://portal.cci-entel.cl/Threat_Intelligence/Boletines/1607/