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

072-2025-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°072	Fecha: 27-03-2025
		Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Ransomware LokiLocker activo en América Latina, borra datos definitivamente		
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:

Investigadores de BlackBerry Threat Intelligence descubrieron una cepa relativamente nueva del ransomware LokiLocker, el cual lleva activo desde mediados de agosto de 2021.

2. DETALLES:

BlackBerry afirmó que la cepa se vende a afiliados seleccionados y verificados. "Cada afiliado se identifica con un nombre de usuario y se le asigna un número de identificación de chat único. Actualmente, existen alrededor de 30 afiliados 'VIP' diferentes en las muestras de LokiLocker que los investigadores de BlackBerry han encontrado circulando".

Este ransomware está programado para borrar el disco y los datos de los equipos objetivo, eliminando así todos los archivos que no pertenecen al sistema y los registros de arranque (boot) si no se paga un rescate, eliminando así cualquier posibilidad de negociación. Sin embargo, los operadores/afiliados de LokiLocker dan a las víctimas un plazo antes de usar la función de borrado.

LokiLocker utiliza una combinación estándar de AES para el cifrado de archivos y RSA para la protección de claves para bloquear los archivos en el equipo objetivo.

Escrito en .NET y protegido con NETGuard mediante un complemento de virtualización llamado KoiVM, LokiLocker incluso sobrescribe el registro de arranque (MBR). El MBR es básicamente información que permite a un sistema localizar e iniciar el sistema operativo almacenado en el disco de un equipo. Sin el MBR, el disco queda inutilizado y no arranca, a menos que se recupere.

3. RECOMENDACIONES:

- 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.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Implementar el principio del privilegio mínimo para minimizar el impacto potencial de las infecciones de ransomware.
- Invertir en soluciones de seguridad, como sistemas de detección y respuesta de endpoints (EDR), y software de detección y prevención de intrusiones (IDS/IPS), que utilicen inteligencia artificial y aprendizaje automático para la detección proactiva de amenazas, de tal manera que pueda identificar y bloquear comportamientos sospechosos antes de que causen daños significativos.
- 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.
- Desarrollar planes de respuesta y recuperación ante incidentes.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://blog.segu-info.com.ar/2025/03/ransomware-lokilocker-activo-en-america.html

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°072	Fecha: 27-03-2025 Página: 5 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	RedCurl utiliza el nuevo ransomware QWCrypt en ataques a servidores Hyper-V		
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:

Bitdefender Labs ha revelado un cambio en las tácticas operativas del veterano grupo de ciberamenazas conocido como RedCurl. Este grupo ha mantenido históricamente un perfil bajo, recurriendo en gran medida a la exfiltración encubierta de datos. Ahora se le ha vinculado a una nueva campaña de ransomware, lo que marca un cambio drástico en sus actividades. Esta nueva cepa de ransomware, denominada QWCrypt, ataca hipervisores, paralizando eficazmente la infraestructura mientras mantiene una presencia sigilosa.

2. DETALLES:

El vector de ataque de RedCurl sigue siendo consistente con sus campañas anteriores, utilizando ingeniería social y correos electrónicos de phishing que contienen archivos IMG disfrazados de documentos de CV y cartas de presentación, para luego cargar de forma lateral el malware de carga mediante el ejecutable legítimo de Adobe "ADNotificationManager.exe".

La secuencia de ataque detallada por Bitdefender sigue los mismos pasos, utilizando archivos de imagen de disco montables (ISO) camuflados en CV para iniciar un proceso de infección multietapa. Dentro de la imagen de disco hay un archivo que imita un salvapantallas de Windows (SCR), pero que en realidad es el binario ADNotificationManager.exe, utilizado para ejecutar el cargador ("netutils.dll") mediante la carga lateral de DLL.

Después de la ejecución, netutils.dll lanza inmediatamente una llamada ShellExecuteA con el verbo abrir, dirigiendo el navegador de la víctima a hxxps://secure.indeed.com/auth

Esto muestra una página de inicio de sesión legítima de Indeed, una distracción calculada diseñada para engañar a la víctima y hacerle creer que simplemente está abriendo un CV. Esta táctica de ingeniería social proporciona una ventana para que el malware opere sin ser detectado.

El grupo aprovecha las vulnerabilidades de carga lateral de DLL en ejecutables legítimos de Adobe para iniciar la cadena de infección.

El cargador, según Bitdefender, también funciona como descargador de una DLL de puerta trasera de siguiente etapa, a la vez que establece persistencia en el host mediante una tarea programada. La DLL recién recuperada se ejecuta mediante el Asistente de Compatibilidad de Programas (pcalua.exe).

El acceso que brinda el implante facilita el movimiento lateral, lo que permite al atacante navegar por la red, recopilar información y escalar aún más su acceso. Sin embargo, en lo que parece ser un cambio radical en su modus operandi establecido, uno de estos ataques también condujo al despliegue de ransomware por primera vez.

Al cifrar las máquinas virtuales alojadas en los hipervisores, impidiéndoles arrancar, RedCurl desactiva eficazmente toda la infraestructura virtualizada, lo que afecta a todos los servicios alojados.

El proceso de implementación del ransomware implica una serie de scripts por lotes adaptados al entorno de la víctima.

Estos scripts deshabilitan Windows Defender y otras soluciones de seguridad, lo que demuestra el profundo conocimiento que tienen los atacantes de la infraestructura objetivo.

El malware también emplea técnicas Living Off The Land (LOTL), abusando de herramientas legítimas del sistema como pcalua.exe y rundll32.exe para evadir la detección.

La naturaleza altamente específica del ataque de ransomware, centrado exclusivamente en máquinas virtuales alojados en hipervisores y excluyendo máquinas virtuales específicas que actúan como puertas de enlace de red, sugiere un esfuerzo deliberado por limitar el impacto del ataque a los departamentos de TI

3. RECOMENDACIONES:

- 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.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Implementar el principio del privilegio mínimo para minimizar el impacto potencial de las infecciones de ransomware
- Deshabilitar los puertos de acceso remoto/Protocolo de escritorio remoto (RDP) no utilizados y monitorear los registros de acceso/RDP.
- Implementar modelos de seguridad basados en el principio de “cero confianza”, donde se verifica constantemente el acceso y las actividades.
- Invertir en soluciones de seguridad, como sistemas de detección y respuesta de endpoints (EDR), y software de detección y prevención de intrusiones (IDS/IPS), que utilicen inteligencia artificial y aprendizaje automático para la detección proactiva de amenazas, de tal manera que pueda identificar y bloquear comportamientos sospechosos antes de que causen daños significativos.
- 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.
- Habilitar la protección de red para evitar que las aplicaciones o los usuarios accedan a dominios maliciosos y otro contenido malicioso en Internet.
- Habilitar la protección de firewall para monitorear y controlar el tráfico de red entrante y saliente.
- Segmentar redes para restringir el movimiento lateral desde los dispositivos infectados.
- 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.
- Desarrollar planes de respuesta y recuperación ante incidentes que abarquen toda la cadena de suministro.
- Promover la cooperación global en el intercambio de información sobre amenazas, el desarrollo de marcos regulatorios y el fortalecimiento de capacidades de respuesta ante incidentes.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://gbhackers.com/redcurl-unleashes-new-ransomware/ • hxxps://hackread.com/redcurl-uses-qwcrypt-ransomware-hypervisor-attacks/ • hxxps://thehackernews.com/2025/03/redcurl-shifts-from-espionage-to.html

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°072	Fecha: 27-03-2025 Página: 7 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de divulgación de información en Moodle		
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:

Microsoft Corporation ha publicado una vulnerabilidad de severidad **ALTA** de tipo exposición de información confidencial a un actor no autorizado en Moodle. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado obtener acceso a información potencialmente confidencial.

2. DETALLES:

Moodle es un sistema de gestión de aprendizaje (LMS) gratuito y de código abierto, diseñado para crear y gestionar entornos de enseñanza virtual.

La vulnerabilidad de severidad **alta** de tipo exposición de información confidencial a un actor no autorizado en Moodle, podría permitir a un atacante remoto no autenticado obtener acceso a información potencialmente confidencial.

La vulnerabilidad existe debido a la excesiva salida de datos por parte de la aplicación. Un atacante remoto puede recuperar los datos almacenados en la tabla de usuarios mediante un seguimiento de pila devuelto por una llamada a la API.

A. Productos afectados:

- Moodle: 4.5.0 - 4.5.2.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://moodle.org/mod/forum/discuss.php?d=467084 • hxxps://github.com/search?q=repo%3Amoodle%2Fmoodle+MDL-84879&type=commits

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°072	Fecha: 27-03-2025
		Página: 8 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en sandbox de Mozilla Firefox		
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:

Mozilla Corporation ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo escape de sandbox debido a una gestión incorrecta del identificador que afecta a usuarios de Windows en sandbox de Mozilla Firefox. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto engañar a la víctima para que visite un sitio web especialmente diseñado, eludir las restricciones del entorno de pruebas y ejecutar código arbitrario en el sistema.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-2857 de tipo escape de sandbox debido a una gestión incorrecta del identificador, podría permitir a un atacante remoto engañar a la víctima para que visite un sitio web especialmente diseñado, eludir las restricciones del entorno de pruebas y ejecutar código arbitrario en el sistema.

Tras la reciente fuga de seguridad de Chrome (CVE-2025-2783), varios desarrolladores de Firefox identificaron un patrón similar en nuestro código IPC (Inter-Process Communication). Un proceso secundario comprometido podría provocar que el proceso principal devuelva un identificador involuntariamente potente, lo que da lugar a una fuga de seguridad.

A. Productos afectados:

- Firefox 136.0.4.
- Firefox ESR 115.21.1.
- Firefox ESR 128.8.1.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.
- Actualizar sus versiones de Firefox a los últimos parches para mitigar esta vulnerabilidad.

Fuente de Información:	• hxxps[:]//www[.]mozilla[.]org/en-US/security/advisories/mfsa2025-19/; • hxxps[:]//bugzilla[.]mozilla[.]org/show_bug.cgi?id=1956398.

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°072	Fecha: 27-03-2025 Página: 9 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en productos Cisco		
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:

Cisco Systems, Inc. ha publicado una vulnerabilidad de severidad **MEDIA** de tipo acceso a datos no autorizado que afecta a Splunk Enterprise y a la aplicación Splunk Secure Gateway. La explotación exitosa de esta vulnerabilidad podría permitir a un usuario remoto obtenga acceso a información confidencial.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-20230 de tipo acceso a datos no autorizado, podría permitir a un usuario remoto obtenga acceso a información confidencial. Un usuario con privilegios bajos sin roles de "administrador" o "poder" puede editar y eliminar datos de otros usuarios en las colecciones de KVStore porque los datos son propiedad del “nobody” usuario, lo que indica que no se asigna un propietario específico.

La vulnerabilidad existe porque Splunk Secure Gateway expone los tokens de sesión y autorización del usuario en texto sin cifrar en el archivo splunk_secure_gateway.log al llamar al endpoint REST /services/ssg/secrets. Un usuario remoto sin privilegios puede acceder a los tokens de autorización y usarlos para comprometer el sistema afectado.

A. Productos afectados:

- Splunk Enterprise, versiones anteriores a 9.4.1, 9.3.3, 9.2.5 y 9.1.8.
- Splunk Secure Gateway, versiones anteriores a 3.8.38 y 3.7.23.

3. RECOMENDACIONES:

- Actualizar Splunk Enterprise a las versiones 9.4.1, 9.3.3, 9.2.5, 9.1.8 o superiores. Splunk supervisa y aplica parches activamente a las instancias de Splunk Cloud Platform.

Fuente de Información:	• hxxps[:]//advisory[.]splunk[.]com/advisories/SVD-2025-0307

Índice alfabético