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

081-2025-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

CISA advierte sobre la amenaza del Fast Flux 4
Vulnerabilidad en Microsoft Edge 6
Vulnerabilidad en herramienta de Autodesk 7
Vulnerabilidad en la plataforma TRMTracker de Hitachi Energy 8
Índice alfabético 9

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°081	Fecha: 04-04-2025
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	CISA advierte sobre la amenaza del Fast Flux		
Tipo de Ataque	Botnets	Abreviatura	Botnets
Medios de propagación	IRC, USB, Disco, Red, Correo, Navegacion de Internet		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Un esfuerzo colaborativo de las agencias internacionales de ciberseguridad, incluida la Agencia de Seguridad Nacional (NSA), la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), la Oficina Federal de Investigaciones (FBI), el Centro Australiano de Seguridad Cibernética de la Dirección de Señales de Australia (ACSC de ASD), el Centro Canadiense para la Seguridad Cibernética (CCCS) y el Centro Nacional de Seguridad Cibernética de Nueva Zelanda (NCSC-NZ), ha puesto de relieve un problema de seguridad crítico conocido como Fast Flux.

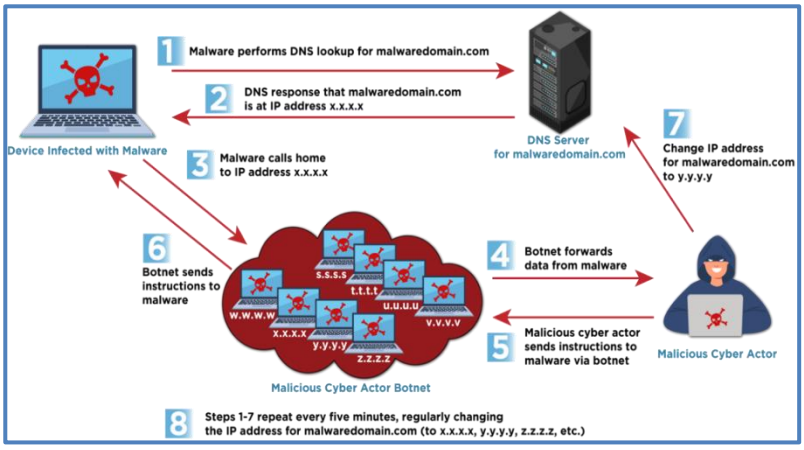
2. DETALLES:

Fast Flux es una técnica de DNS que se utiliza para evadir la detección y mantener una infraestructura resiliente para comando y control (C2), phishing y distribución de malware.

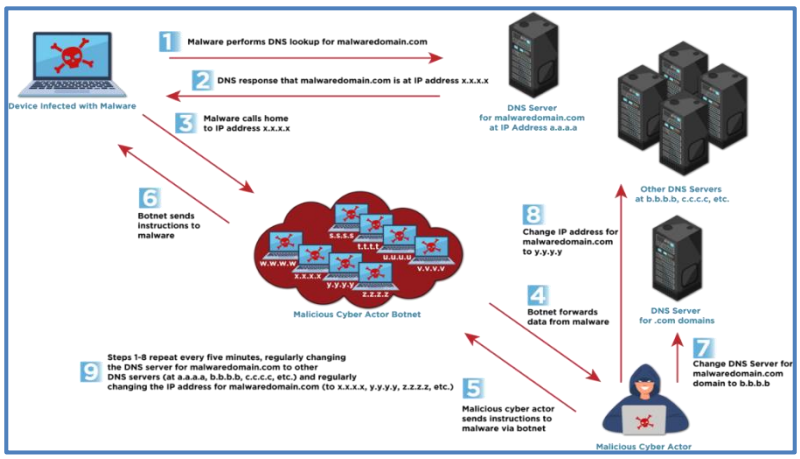
El mecanismo principal de Fast Flux reside en la manipulación dinámica de los registros del Sistema de Nombres de Dominio (DNS). Al alterar rápidamente las direcciones IP asociadas a un solo dominio, los atacantes ocultan eficazmente la ubicación real de sus servidores maliciosos. Esta rápida rotación invalida los métodos tradicionales de bloqueo basados en IP, ya que la dirección IP objetivo queda obsoleta casi de inmediato.

Los actores cibernéticos maliciosos utilizan dos variantes comunes de Fast Flux para realizar operaciones:

A. Flujo único: Un único nombre de dominio está vinculado a numerosas direcciones IP, que se rotan con frecuencia en las respuestas DNS. Esta configuración garantiza que, si una dirección IP se bloquea o se desactiva, el dominio siga siendo accesible a través de las demás direcciones IP.



B. Doble flujo: Además de cambiar rápidamente las direcciones IP como en el flujo simple, los servidores de nombres DNS responsables de resolver el dominio también cambian con frecuencia. Esto proporciona una capa adicional de redundancia y anonimato para dominios maliciosos. Se han observado técnicas de doble flujo utilizando registros DNS de servidor de nombres (NS) y de nombre canónico (CNAME).



Ambas técnicas aprovechan una gran cantidad de hosts comprometidos, generalmente como una botnet de todo Internet que actúa como proxy o punto de retransmisión, lo que dificulta que los defensores de la red identifiquen el tráfico malicioso y bloqueen o desmantelen la infraestructura maliciosa.

CISA enfatiza que Fast Flux no se utiliza únicamente para mantener las comunicaciones C2. Desempeña un papel importante en las campañas de phishing, dificultando el desmantelamiento de sitios web de ingeniería social.

Además, los proveedores de alojamiento a prueba de balas (BPH), que ignoran las solicitudes de las fuerzas del orden, lo ofrecen cada vez más como servicio a sus clientes. Esto permite el funcionamiento fluido de actividades maliciosas como la gestión de botnets, tiendas online falsas y el robo de credenciales, a la vez que proporciona una capa de protección contra la detección y el desmantelamiento. Además, se ha utilizado en ataques de ransomware como Hive y Nefilim. Un proveedor de BPH incluso anunció la capacidad del servicio para eludir las listas de bloqueo de Spamhaus, destacando su atractivo para los ciberdelincuentes.

3. RECOMENDACIONES:

- Aprovechar las fuentes de inteligencia sobre amenazas y los servicios de reputación para identificar dominios de flujo rápido conocidos y direcciones IP asociadas, como en firewalls de límites, solucionadores de DNS y/o soluciones SIEM.
- Implementar sistemas de detección de anomalías en los registros de consultas DNS para identificar dominios con alta entropía o diversidad de IP en las respuestas DNS, así como rotaciones frecuentes de direcciones IP. Los dominios de flujo rápido suelen utilizar decenas o cientos de direcciones IP al día.
- Analizar los valores de tiempo de vida (TTL) en los registros DNS. Los dominios Fast Flux suelen tener valores de TTL inusualmente bajos. Un dominio Fast Flux típico puede cambiar su dirección IP cada 3 a 5 minutos.
- Revisar la resolución DNS para detectar geolocalización inconsistente. Los dominios maliciosos asociados con Fast Flux suelen generar grandes volúmenes de tráfico con información de geolocalización IP inconsistente.
- Utilizar datos de flujo para identificar comunicaciones a gran escala con numerosas direcciones IP diferentes durante períodos cortos.
- Desarrollar algoritmos de detección de flujo rápido para identificar patrones de tráfico anómalos que se desvían del comportamiento habitual del DNS de la red.
- Monitorear las señales de actividades de phishing, como correos electrónicos, sitios web o enlaces sospechosos, y correlacione estos con la actividad de Fast Flux. Fast Flux puede utilizarse para propagar rápidamente campañas de phishing y mantener los sitios web de phishing en línea a pesar de los intentos de bloqueo.
- Implementar la transparencia del cliente y compartir información sobre la actividad de flujo rápido detectada, garantizando alertar a los clientes rápidamente después de confirmarse la presencia de actividad maliciosa.
- Bloquear el acceso a dominios identificados como que utilizan flujo rápido a través de respuestas DNS no enrutables o reglas de firewall.
- Bloquear el tráfico hacia y desde dominios o direcciones IP con mala reputación, especialmente aquellos identificados por participar en actividades maliciosas de fast flux.

Fuente de Información:	• hxxps://hackread.com/nsa-allies-fast-flux-a-national-security-threat/ • hxxps://www.cisa.gov/news-events/cybersecurity-advisories/aa25-093a • hxxps://blog.segu-info.com.ar/2025/04/cisa-advierte-sobre-la-evasion-de-dns.html?m=0 • hxxps://www.fortinet.com/lat/resources/cyberglossary/fast-flux-networks

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°081	Fecha: 04-04-2025 Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en Microsoft Edge		
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 **MEDIA** de tipo representación errónea de la interfaz de usuario que afecta a Microsoft Edge para iOS. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante no autorizado realizar un ataque de suplantación de identidad a través de la red.

2. DETALLES:

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-29796 de tipo representación errónea de la interfaz de usuario en Microsoft Edge para iOS, podría permitir a un atacante no autorizado a realizar un ataque de suplantación de identidad a través de la red.

La vulnerabilidad existe debido al procesamiento incorrecto de los datos proporcionados por el usuario. Un atacante remoto puede engañar a la víctima para que haga clic en una URL especialmente diseñada y falsificar el contenido de la página.

A. Productos afectados:

- Microsoft Edge para iOS, versión anterior a 135.0.3179.54.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps[:]//msrc[.]Microsoft[.]com/update-guide/vulnerability/CVE-2025-29796

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°081	Fecha: 04-04-2025 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en herramienta de Autodesk		
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:

Autodesk Inc. ha publicado una vulnerabilidad de severidad **ALTA** de tipo lectura fuera de límites que afecta a Autodesk Navisworks. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario y obtener acceso a información confidencial.

2. DETALLES:

Autodesk Navisworks es un software de revisión y coordinación de diseño 3D utilizado en los sectores de la arquitectura, la ingeniería y la construcción (AEC). Permite a los usuarios integrar y analizar modelos 3D complejos, optimizando la ejecución y la colaboración en proyectos.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-1658 de tipo lectura fuera de límites, podría permitir a un atacante remoto ejecutar código arbitrario y obtener acceso a información confidencial.

Un archivo DWFX creado con fines maliciosos, al analizarse mediante Autodesk Navisworks, puede forzar una vulnerabilidad de lectura fuera de límites. Un agente malicioso puede aprovechar esta vulnerabilidad para provocar un bloqueo, leer datos confidenciales o ejecutar código arbitrario en el contexto del proceso actual.

A. Productos afectados:

- Autodesk Navisworks: 2025-2025.4.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Instalar las últimas versiones mitigadas de los productos afectados a través de Autodesk Access o el Portal de Cuentas.

Fuente de Información:	• hxxps[:]//www[.]autodesk[.]com/trust/security-advisories/adsk-sa-2025-0002

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°081	Fecha: 04-04-2025 Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en la plataforma TRMTracker de Hitachi Energy		
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:

Hitachi Energy ha publicado una vulnerabilidad de severidad **MEDIA** de tipo ataque de inyección LDAP que afecta a la aplicación TRMTracker de Hitachi Energy. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado inyectar código malicioso en las consultas LDAP.

2. DETALLES:

TRMTracker de Hitachi Energy es una plataforma avanzada de software para la gestión de riesgos y comercialización de materias primas y energía (C/ETRM), diseñada para satisfacer las complejas necesidades de productores, comercializadores y proveedores de energía.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-27631 de tipo ataque de inyección LDAP, podría permitir a un atacante remoto inyectar código malicioso en las consultas LDAP.

La vulnerabilidad existe debido a una validación de entrada incorrecta al procesar consultas DLAP. Un atacante remoto puede enviar una consulta LDAP especialmente diseñada a la aplicación, eludir el proceso de autenticación y obtener acceso no autorizado a la misma.

A. Productos afectados:

- TRMTracker: 6.2 - 6.2.04.
- TRMTracker: 6.3 - 6.3.01.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad.

Fuente de Información:	• hxxps[:]//publisher[.]hitachienergy[.]com/preview?DocumentID=8DBD000210&LanguageCode=en&DocumentPartId=&Action=Launch

Índice alfabético

Botnets 4
Explotación de vulnerabilidades conocidas 6, 7, 8