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

096-2025-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°096	Fecha: 24-04-2025
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Nueva campaña de esteganografía explota una vulnerabilidad de MS Office para distribuir AsyncRAT		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

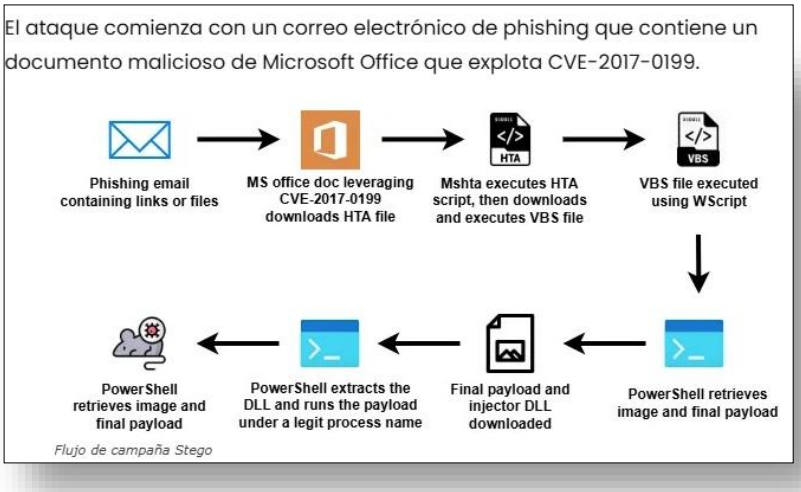
1. ANTECEDENTES:

Una campaña de ciberataque descubierta recientemente ha vuelto a poner la esteganografía en el centro de atención, mostrando los métodos creativos e insidiosos que emplean los atacantes para distribuir malware.

Esta operación, denominada "Stego-Campaign", explota una vulnerabilidad conocida de Microsoft Office, CVE-2017-0199, para iniciar infecciones y, en última instancia, desplegar el famoso malware AsyncRAT.

Un ataque innovador aprovecha cargas útiles ocultas en imágenes

La vulnerabilidad, informada por primera vez en abril de 2017, permite la ejecución remota de código (RCE) sin interacción del usuario más allá de abrir un documento malicioso, lo que la convierte en un potente punto de entrada para ataques basados en phishing.



2. DETALLES:

Una vez abierto, el documento desencadena la descarga de un script HTA malicioso, que a su vez obtiene una versión troyanizada de Prnport.vbs, un script legítimo de Windows para administrar puertos de impresora.

Este script manipulado construye y ejecuta un comando de PowerShell para descargar una DLL de inyector oculta dentro de un archivo de imagen de apariencia inocua mediante esteganografía.

Entrega sofisticada de carga útil mediante scripts troyanizados y vaciamiento de procesos

El inyector codificado en Base64 está incrustado entre marcadores específicos en el código fuente de la imagen y se puede extraer y decodificar utilizando herramientas como CyberChef.

El análisis revela que el espacio de nombres original del inyector es Microsoft.Win32. TaskScheduler, una DLL de 32 bits confirmada mediante herramientas como Detect It Easy y CFF Explorer.

El script de PowerShell carga dinámicamente este inyector a través de la reflexión, invocando un método llamado "VAI" para recuperar la URL de carga útil final, que apunta a un binario AsyncRAT codificado en Base64 invertido.

La carga útil se decodifica y, a través de una técnica conocida como vaciado de proceso (T1055.012), se inyecta en un proceso MSBuild.exe legítimo, lo que permite que el malware se ejecute de forma encubierta bajo un nombre de proceso confiable.

AsyncRAT, una herramienta de acceso remoto de código abierto lanzada en 2019, brinda a las atacantes capacidades como acceso a escritorio remoto, registro de teclas y la capacidad de implementar malware adicional como ransomware.

El uso de esteganografía en esta campaña para ocultar código malicioso dentro de imágenes ejemplifica hasta dónde llegan los actores de amenazas para evadir la detección.

Después de invocar el método VAI, el script de PowerShell revierte y decodifica la URL de carga útil, obtiene el binario AsyncRAT y emplea el vaciado de proceso para ejecutarlo de manera sigilosa.

La carga útil final, marcada por Virus Total, incluye un archivo de configuración que revela la dirección IP de comando y control (C2), lo que subraya la sofisticada infraestructura detrás del ataque.

La esteganografía, aunque no se ve comúnmente en la naturaleza, sigue siendo una técnica fascinante y peligrosa que desafía los mecanismos de defensa tradicionales, ya que las cargas ocultas son difíciles de detectar sin un análisis especializado.

Los defensores deben familiarizarse con dichos flujos de ataque para mitigar amenazas similares de manera efectiva, enfocándose en la prevención de phishing, el monitoreo de puntos finales para detectar comportamientos sospechosos de procesos y la detección de anomalías en el tráfico de la red.

Indicadores de Compromiso (IOC)

Tipo	Valor
Prnport.vbs troyanizado (SHA256)	1105ae14ccb41fedcf556e4c575e34e505e9a571f2021ba89a75fbe5fa12e3c0
URL de entrega de AsyncRAT	hxxps[:///]watchonlinehotvideos[.]sitio/001[.]txt
AsyncRAT (SHA256)	448ae5b8890c17a2efe4985653 1efd62796db52d2ff0ecbb4678334aea2bf776
Dirección C2 de AsyncRAT	148[.]113[.]214[.]176
URL de entrega del inyector	hxxps[:///]1019[.]filemail[.]com/api/file/get?filekey=ZrKTNo-_DMWgm0oonSr97JAkdrUqbICVeG2LmuclzuON2ZavKqsQg0NqChSLT4A&pk_vid=342803d1cc4e3b801741606974b78eb
Inyector (espacio de nombres)	Microsoft.Win32.TaskScheduler
Inyector binario (SHA256)	8CC93827CA7652AFC8E08B9266F6567D06B932AF26B601EB7FDE10F5E5A6CB30
Ruta del proceso inyectado	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

3. RECOMENDACIONES:

- Priorizar controles de acceso sólidos, actualizaciones periódicas del sistema y copias de seguridad seguras para mitigar el riesgo de este tipo de ataques.
- Asegurarse de que el sistema operativo, aplicaciones y software de seguridad estén siempre actualizados para protegerte contra vulnerabilidades.
- Instalar y mantener un programa antivirus confiable que pueda detectar y eliminar malware.
- No abrir correos electrónicos ni archivos adjuntos de remitentes desconocidos, ya que pueden contener malware.
- Descargar software sólo de sitios web oficiales y evita fuentes no verificadas.

Fuente de Información:	• hxxps://gbhackers.com/new-steganography-campaign-exploits-ms-office-vulnerability/ • hxxps://docs.github.com/es/site-policy/acceptable-use-policies/github-active-malware-or-exploits

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°096	Fecha: 24-04-2025
		Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en el controlador Schneider Electric Wiser WHC-5918A		
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 publicado una vulnerabilidad de severidad **CRÍTICA** de tipo exposición de información confidencial a un actor no autorizado que afecta al controlador Wiser Home WHC-5918A de Schneider Electric. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado revelar credenciales confidenciales.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-6407 de tipo exposición de información confidencial a un actor no autorizado que afecta al controlador Wiser Home WHC-5918A, podría permitir a un atacante remoto no autenticado revelar credenciales confidenciales.

La vulnerabilidad de exposición de información podría provocar la divulgación de credenciales cuando se envía un mensaje especialmente diseñado al dispositivo.

A. Productos afectados:

- Controlador Wiser Home WHC-5918A: Todas las versiones.

3. RECOMENDACIÓN:

- Considerar actualizar a la última versión del producto: C-Bus, controlador doméstico, SpaceLogic IP, independiente, 24 V CC, 5200WHC2, o retirar del servicio el controlador Wiser Home Controller WHC-5918ª, ya que Schneider Electric indico que el controlador Wiser Home Controller WHC-5918A ha sido descontinuado y ya no recibe soporte.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-25-112-03

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°096	Fecha: 24-04-2025
		Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades de severidad crítica en TeleControl Server Basic de Siemens		
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:

Siemens ha publicado múltiples vulnerabilidades de severidad **CRÍTICA** de tipo inyección SQL que afecta a TeleControl Server Basic. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado leer y escribir en la base de datos de la aplicación, provocar una condición de denegación de servicio (DoS) y ejecutar código en un shell del sistema operativo.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-27495 de tipo inyección SQL mediante el método interno "CreateTrace", podría permitir que un atacante remoto no autenticado eluda los controles de autorización, lea y escriba en la base de datos de la aplicación y ejecute código con permisos "NT AUTHORITY\NetworkService". Para que el ataque tenga éxito, el atacante debe poder acceder al puerto 8000 de un sistema donde se ejecute una versión vulnerable de la aplicación afectada.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-27539 de tipo inyección SQL mediante el método interno "VerifyUser". Esto podría permitir que un atacante remoto no autenticado eluda los controles de autorización, lea y escriba en la base de datos de la aplicación y ejecute código con permisos "NT AUTHORITY\NetworkService". Para que el ataque tenga éxito, el atacante debe poder acceder al puerto 8000 de un sistema donde se ejecute una versión vulnerable de la aplicación afectada.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-27540 de tipo inyección SQL mediante el método interno "Authenticate". Esto podría permitir que un atacante remoto no autenticado eluda los controles de autorización, lea y escriba en la base de datos de la aplicación y ejecute código con permisos "NT AUTHORITY\NetworkService". Para que el ataque tenga éxito, el atacante debe poder acceder al puerto 8000 de un sistema donde se ejecute una versión vulnerable de la aplicación afectada.

Para las vulnerabilidades de severidad alta se han asignado los siguientes identificadores: CVE-2025-32475, CVE-2025-31353, CVE-2025-31352, CVE-2025-31351, CVE-2025-31350, CVE-2025-31349, CVE-2025-31343, CVE-2025-30032, CVE-2025-30031, CVE-2025-30030, CVE-2025-30003, CVE-2025-30002 y CVE-2025-29905.

A. Productos afectados:

- TeleControl Server Basic: versiones anteriores a V3.1.2.2.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que abordan estas vulnerabilidades.
- Restringir el acceso al puerto 8000 en los sistemas afectados únicamente a direcciones IP confiables.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-25-112-01 • hxxps://www.siemens.com/cert/operational-guidelines-industrial-security • hxxps://www.siemens.com/industrialsecurity

Índice alfabético