Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

MOSTERERAT UTILIZA HERRAMIENTAS DE ACCESO REMOTO PARA EVADIR DEFENSAS

08/ 09/ 2025

CONTENIDO

INTRODUCCIÓN

Investigadores descubrieron una nueva y sofisticada campaña de phishing en Japón. Esta campaña distribuye MostereRAT, un troyano de acceso remoto (RAT) que se destaca por su capacidad para evadir las defensas y utilizar herramientas legítimas para pasar desapercibido.

MOSTERERAT UTILIZA HERRAMIENTAS DE ACCESO REMOTO PARA EVADIR DEFENSAS

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_09_08_3
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	08/09/2025
Es día cero (0 day):	No

RESUMEN

Investigadores descubrieron una nueva y sofisticada campaña de phishing en Japón. Esta campaña distribuye MostereRAT, un troyano de acceso remoto (RAT) que se destaca por su capacidad para evadir las defensas y utilizar herramientas legítimas para pasar desapercibido.

Evolución y técnicas del malware

MostereRAT no es un malware común. Originalmente un troyano bancario, ha evolucionado para enfocarse en el espionaje y el control persistente. Su programación en EPL (Easy Programming Language), un lenguaje atípico para el desarrollo de malware dificulta su detección y análisis.

Se propaga a través de correos de phishing que aparecen como consultas de negocios e incluyen archivos maliciosos en formato ZIP o Word con macros. Una vez dentro, MostereRAT utiliza técnicas avanzadas:

- Escalada de privilegios extremos: Duplica los tokens del sistema y opera con los permisos de TrustedInstaller, el nivel de acceso más alto en Windows.
- Desactivación de defensas: Bloquea herramientas de seguridad como Windows Defender, ESET, Kaspersky y McAfee usando técnicas similares a las de las herramientas de Red Team como EDRSilencer.
- Acceso remoto oculto: Instale herramientas legítimas de acceso remoto como AnyDesk, TightVNC o RDP Wrapper para mantener la persistencia y evadir los controles de seguridad tradicionales.
- Comunicaciones seguras con C2: Usa mTLS (mutual TLS) para dificultar la intercepción y la atribución del tráfico malicioso.
- Amplias capacidades de espionaje: Puede realizar registro de pulsaciones de teclas (keylogging), capturas de pantalla, ejecución de comandos, robo de archivos y despliegue de cargas maliciosas adicionales.

Impacto potencial

Actualmente, los gobiernos y empresas en Japón son los principales objetivos de esta campaña, pero el malware tiene el potencial de expandirse a otras regiones.

El uso de herramientas legítimas y de técnicas de evasión avanzadas hace que MostereRAT sea una amenaza de alto riesgo para sectores críticos, ya que permite un control total sin activar alertas inmediatas.

RECOMENDACIONES

- Bloquea las macros en los documentos y refuerza la capacitación de tus empleados para detectar correos de phishing.
- Restringe y monitorea el uso de herramientas de acceso remoto como AnyDesk, TightVNC y RDP Wrapper.
- Implemente controles de privilegio mínimo para evitar que los usuarios escale a niveles de acceso críticos.
- Usa soluciones EDR con monitoreo de comportamiento capaz de detectar inyecciones, keylogging y conexiones anómalas con mTLS.
- Audita procesos y servicios sospechosos, como servicios falsos que se hacen pasar por legítimos (“WpnCoreSvc”).

NOTICIA COMPLETA

https://devel.group/blog/mostererat-utiliza-herramientas-de-acceso-remoto-para-evadir-defensas/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group