Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

GHOSTREDIRECTOR SE INFILTRA EN 65 SERVIDORES WINDOWS CON MALWARE AVANZADO

04/ 09 / 2025

CONTENIDO

INTRODUCCIÓN

Un nuevo grupo de cibercriminales llamado GhostRedirector ha comprometido al menos 65 servidores Windows en 11 países, incluyendo Brasil, Tailandia, Vietnam, Perú y EE. UU.

GHOSTREDIRECTOR SE INFILTRA EN 65 SERVIDORES WINDOWS CON MALWARE AVANZADO

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

ID de alerta:	DSOC-CERT_2025_09_04_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	04/09/2025
Es día cero (0 day):	No

RESUMEN

Un nuevo grupo de cibercriminales llamado GhostRedirector ha comprometido al menos 65 servidores Windows en 11 países, incluyendo Brasil, Tailandia, Vietnam, Perú y EE. UU. Su objetivo principal es el fraude SEO (Optimización para Motores de Búsqueda): manipular los resultados de Google para promover sitios de apuestas en línea. Lo más peligroso es que los atacantes usan una combinación de malware personalizado, exploits públicos y tácticas de evasión avanzadas para mantener el control de los sistemas comprometidos durante meses sin ser detectados.

Detalles técnicos del ataque

El modus operandi de GhostRedirector se basa en una serie de pasos cuidadosamente orquestados para obtener y mantener el control de los servidores.

Puerta de entrada y persistencia

Los atacantes obtienen acceso inicial explotando vulnerabilidades en servidores Windows con IIS. Una vez dentro, utilizan exploits de escalada de privilegios como EfsPotato y BadPotato para crear cuentas con privilegios. Luego, modifican registros y configuran tareas programadas para asegurar su permanencia en el sistema, lo que les permite estar activos por largos períodos.

Backdoor Rungan

Este es un backdoor en C++ que proporciona un control remoto pasivo sobre el servidor. Con él, los atacantes pueden ejecutar comandos, instalar nuevas cargas maliciosas o usar el servidor como un pivote para lanzar más ataques dentro de la red.

Módulo Gamshen para IIS

Este es el corazón de la campaña. Es un módulo nativo para IIS que altera los resultados del sitio web solo cuando el tráfico proviene de Googlebot. Para los usuarios normales, el sitio funciona con normalidad, pero los motores de búsqueda ven contenido manipulado que eleva artificialmente la posición de los sitios de apuestas. Este sigilo hace que la campaña sea extremadamente difícil de detectar.

Infraestructura y tácticas de camuflaje

Los atacantes utilizaron certificados digitales legítimos de empresas chinas para firmar sus binarios y aparentar legalidad. El malware contiene comentarios y cadenas en chino, lo que refuerza la hipótesis de su origen. Además, aprovechan servidores comprometidos para alojar los módulos maliciosos y redirigir el tráfico, ocultando su verdadera infraestructura.

Sectores afectados

Los sectores afectados incluyen educación, salud, seguros, transporte, tecnología y comercio minorista.
Impacto real

- SEO fraudulento: Manipulación de los resultados de Google para impulsar sitios web de apuestas.
- Daño a la reputación: Las empresas afectadas pueden ser marcadas por Google por prácticas sospechosas, incluso si no son las responsables directas del fraude.

- Persistencia encubierta: Al operar de forma sigilosa, estos incidentes pueden pasar inadvertidos durante meses, causando un daño prolongado.

¿Qué hace a GhostRedirector único?

- Inyecta directamente en IIS mediante un módulo nativo, a diferencia de simples scripts.
- Utiliza un backdoor propio (Rungan).
- Opera en un modo sigiloso, alterando el contenido solo para Googlebot.
- Refuerza su legitimidad con certificados digitales válidos.

RECOMENDACIONES

- Instala todos los parches de seguridad de Microsoft, especialmente los relacionados con IIS y la escalada de privilegios (exploits tipo Potato).
- Revisa periódicamente qué módulos están cargados en IIS. Elimina cualquier extensión desconocida o no documentada.
- Utiliza herramientas que te permitan comparar cómo se ve tu sitio para un navegador normal versus para Googlebot, para detectar cualquier discrepancia.

NOTICIA COMPLETA

https://devel.group/blog/ghostredirector-se-infiltra-en-65-servidores-windows-con-malware-avanzado/

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