BOLETÍN DE ALERTA

Boletín Número: 2022-16 **Fecha de Publicación:** 29/07/2022

Tema: Backdoor en servidores IIS de Microsoft.

SEVERIDAD: ALTA

DESCRIPCIÓN

El Departamento de Ciberseguridad de la DIGETIC/FFAA, informa sobre una alerta de seguridad referente a un Backdoor en servidores IIS de Microsoft.

Recientemente Microsoft ha alertado a sus usuarios sobre un nuevo método de ataque que permite establecer Backdoors en servidores IIS, mediante extensiones del mismo y que tendrían un muy bajo índice de detección y gran persistencia, esto debido a un trabajo de ocultamiento que simula servicios legítimos para el sistema..

RECURSOS AFECTADOS

- Servidores IIS de Microsoft

DETALLES

Módulo IIS

Dado que IIS se ha diseñado para ser un servidor flexible, es posible añadir o quitar capacidades de mediante módulos configurados en el sistema de acuerdo a las necesidades de cada usuario, permitiendo personalizar los servidores, para que cada solicitud sea procesada por los módulos instalados antes que por el IIS propiamente tal.

Persistencia

De acuerdo a lo mencionado por investigadores, estas técnicas suelen no ser inmediatamente desplegadas luego de un acceso inicial, ya que una de las primera acciones luego de la explotación de vulnerabilidades es la instalación de webshells con las que permiten ganar persistencia en los servidores. Posterior a esto y cuando el acceso está asegurado se procede con la instalación de módulos IIS permitiendo continuar en las siguientes fases del ataque.

Capacidades

Entre las características del ataque es posible extraer credenciales desde la memoria del sistema, recolectar información de las redes y dispositivos conectados a la red, junto con el despliegue de cargas útiles (Payloads) para infectar otros dispositivos.

En algunos de los ataques analizados por Microsoft, observaron que actores maliciosos ganaron acceso a casillas de correo electrónico, sustracción de credenciales e información confidencial mediante la ejecución de comandos remotos.

Posterior a la explotación de las vulnerabilidades y secuestro de información los atacantes despliegan el backdoor en la carpeta C:\inetpub\wwwroot\bin\ mediante

DLL´s con nombres y estructuras similares a los servicios válidos del sistema, permitiendo así alojarse dentro del sistema y ocultando su presencia.

De acuerdo a lo mencionado por el equipo de investigación de Microsoft 365 defender:

"En la mayoría de los casos, la lógica real de la puerta trasera es mínima y no puede considerarse maliciosa sin una comprensión más amplia de cómo funcionan las extensiones legítimas de IIS, lo que también dificulta la determinación del origen de la infección" .

En relación a que este podría no ser precisamente un backdoor si no más bien, el abuso de una capacidad permitida por el sistema pero que no ha sido diseñada con ese objetivo.

Primera visualización

Una de las primeras visualizaciones de este ataque surgió durante enero y mayo de 2022, en donde una campaña género el acceso inicial e instalación de webshell mediante la explotación de ProxyShell en servidores MS Exchange, a lo que luego de un periodo de reconocimiento, exilfracion de credenciales y establecimiento de acceso remoto, se procedió con la instalación de Backdoor IIS que posteriormente permitió enumerar casillas de correo y exfiltrarlas.

Panorama

En base a lo descrito anteriormente y las habilidades que mantienen los atacantes para cada vez vulnerar los dispositivos generando el menor ruido posible, es esperable que sigan desarrollando técnicas de ocultamiento tanto o más complejas, por lo que, es indispensable mantener controles de seguridad en constante desarrollo que permitan adaptarse constantemente a los nuevos hallazgos y técnicas de penetración.

Si bien no se ha identificado el origen de los atacantes ni su motivación, no sería raro que actualmente se mantengan con financiamiento de alguna entidad, ya que estas técnicas elaboradas suelen ser diseñadas de manera sigilosa, específicamente para llevar a cabo operaciones de largo aliento en las que no solo se desea extraer información de usuarios, sino permanecer indetectables por el mayor tiempo posible en modo de "espionaje", esto es usualmente generado por las APT´s.

RECOMENDACIÓN

- Mantener Servidores Exchange actualizados.
- Mantener habilitadas las soluciones anti malware y de seguridad en general.
- Revisar constantemente roles y grupos sensibles.
- Restringir el acceso a directorios virtuales IIS.
- Priorizar alertas e inspeccionar los archivos de configuración en carpetas BIN.
- Instalar las actualizaciones del fabricante disponibles en medios oficiales del proveedor, previo análisis del impacto que podría provocar en los servicios críticos para el negocio de su organización. Para ello consulte con su personal técnico o áreas resolutorias correspondientes.

REFERENCIAS

https://www.microsoft.com/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1315/