Un backdoor previamente desconocido, denominado Msupedge, ha sido empleado en un ciberataque dirigido contra una universidad no especificada en Taiwán.

> *«La característica más destacada de este backdoor es que se comunica con un servidor de comando y control (C&C) a través de tráfico DNS»*, explicó el equipo Symantec Threat Hunter, parte de Broadcom.

Actualmente, se desconocen tanto los orígenes de este backdoor como los objetivos detrás del ataque.

Se cree que el acceso inicial que facilitó la instalación de Msupedge se logró mediante la explotación de una vulnerabilidad crítica recientemente identificada en PHP (CVE-2024-4577, puntuación CVSS: 9.8), la cual podría permitir la ejecución remota de código.

El backdoor en cuestión es una biblioteca de enlace dinámico (DLL) que se instala en las rutas «*csidl_drive_fixed\xampp*» y «*csidl_system\wbem*«. Una de las DLL, wuplog.dll, es ejecutada por el servidor HTTP Apache (httpd), mientras que el proceso asociado a la segunda DLL aún no ha sido identificado.

Lo más significativo de Msupedge es su uso de túneles DNS para comunicarse con el servidor C&C, con un código basado en la herramienta de código abierto dnscat2.

> *«Recibe instrucciones a través de la resolución de nombres. Msupedge no solo recibe órdenes a través del tráfico DNS, sino que también utiliza la dirección IP resuelta del servidor C&C (ctl.msedeapi[.]net) como un comando»,* señaló Symantec.

En particular, el tercer octeto de la dirección IP resuelta actúa como un interruptor que determina el comportamiento del backdoor al restar siete de su valor y usar su notación

hexadecimal para activar las respuestas correspondientes. Por ejemplo, si el tercer octeto es 145, el valor derivado es 138 (0x8a).

Los comandos que soporta Msupedge se detallan a continuación:

- 0x8a: Crear un proceso utilizando un comando recibido a través de un registro DNS TXT
- 0x75: Descargar un archivo utilizando una URL recibida a través de un registro DNS TXT
- 0x24: Dormir durante un intervalo de tiempo predefinido
- 0x66: Dormir durante un intervalo de tiempo predefinido
- 0x38: Crear un archivo temporal «*%temp%\1e5bf625-1678-zzcv-90b1-199aa47c345.tmp*» con un propósito desconocido
- 0x3c: Eliminar el archivo «*%temp%\1e5bf625-1678-zzcv-90b1-199aa47c345.tmp*«

Este desarrollo se produce en un momento en que el grupo de amenazas UTG-Q-010 ha sido vinculado a una nueva campaña de phishing que utiliza señuelos relacionados con criptomonedas y ofertas de empleo para distribuir un malware de código abierto llamado Pupy RAT.

> *«La cadena de ataque incluye el uso de archivos .lnk maliciosos con un cargador DLL integrado, lo que finalmente lleva al despliegue del payload de Pupy RAT. Pupy es un troyano de acceso remoto (RAT) basado en Python que permite la carga reflexiva de DLL y la ejecución en memoria, entre otras funcionalidades»*, explicó Symantec.