Un grupo chino de ciberespionaje conocido por apuntar al sudeste asiático, aprovechó las vulnerabilidades en Microsoft Exchange Server que se informaron a inicios de marzo, con el fin de implementar una variante previamente indocumentada de un troyano de acceso remoto (RAT) en sistemas comprometidos.

Al atribuir las intrusiones a un actor de amenazas llamado PKPLUG (también conocido como Mustang Panda y HoneyMyte), el equipo de inteligencia de amenazas de la Unidad 42 de Palo Alto Networks, dijo que identificó una nueva versión del malware modular PlugX, llamado Thor, que se entregó como una herramienta posterior a la explotación a uno de los servidores vulnerados.

PlugX, que se remonta al 2008, es un implante de segunda etapa con capacidades como carga, descarga y modificación de archivos, registro de pulsaciones de teclas, control de cámara web y acceso a un shell de comando remoto.

> *«La variante observada es única porque contiene un cambio en su código fuente central: el reemplazo de su palabra de marca registrada «PLUG» por «THOR»,* dijeron los investigadores de Unit 42, Mike Harbison y Alex Hinchliffe.
>
> *«La primera muestra de THOR descubierta fue de agosto de 2019, y es la primera instancia conocida del código renombrado. Se observaron nuevas características en esta variante, incluidos mecanismos mejorados de entrega de carga útil y abuso de binarios confiables»,* agregaron.

Después de que Microsoft reveló el 2 de marzo que los hackers con sede en China, con nombre en código Hafnium, estaban explotando errores de día cero en el servidor Exchange conocido colectivamente como ProxyLogon para robar datos confidenciales de objetivos seleccionados, múltiples actores de amenazas, como grupos de ransomware (DearCry y Black Kingdom), bandas de cripto minería (LemonDuck) estuvieron trabajando en esta campaña. También se observó que explotaban las vulnerabilidades para secuestrar

servidores Exchange e instalar un shell web que otorgaba la ejecución de código al más alto nivel de privilegios.

PKPLUG ahora se une a la lista, según Unit 42, que descubrió que los atacantes eludían los mecanismos de detección de antivirus para atacar los servidores de Microsoft Exchange aprovechando los ejecutables legítimos como BITSAdmin para recuperar un archivo aparentemente inocuo («aro.dat») de un repositorio GitHub controlado por un atacante.

El archivo, que alberga la carga útil de PlugX cifrada y comprimida, alude a una herramienta avanzada de reparación y optimización disponible de forma gratuita, que está diseñada para limpiar y solucionar problemas en el Registro de Windows.

La última muestra de PlugX está equipada con una variedad de complementos que *«brindan a los atacantes varias capacidades para monitorear, actualizar e interactuar con el sistema comprometido para cumplir con sus objetivos»,* dijeron los investigadores.

Los enlaces de THOR a PKPLUG surgen de unir la infraestructura de comando y control, así como de las superposiciones en los comportamientos maliciosos detectados entre otros artefactos PlugX recientemente descubiertos.

Aquí se pueden encontrar indicadores adicionales de compromiso asociados con el ataque. Unit 42 también puso a disposición un script Python que puede descifrar y descomprimir cargas útiles PlugX cifradas sin tener los cargadores PlugX asociados.