Investigadores de seguridad cibernética descubrieron nuevas pruebas de una campaña de espionaje cibernético en curso contra las unidades de defensa de la India y el personal de las fuerzas armadas al menos desde 2019, con el objetivo de robar información confidencial.

Nombrado como «*Operation SideCopy*» por la firma india de ciberseguridad Quick Heal, los ataques de atribuyeron a un grupo de amenazas persistentes avanzadas (APT), que ha logrado mantenerse fuera del radar «copiando» las tácticas de otros actores de amenazas como SideWinder.

El punto de partida de la campaña es un correo electrónico con un archivo adjunto malicioso incrustado, ya sea en forma de archivo ZIP que contiene un archivo LNK o un documento de Microsoft Word, que desencadena una infección a través de una serie de pasos para descargar la carga útil de la etapa final.

Además de identificar tres cadenas de infección diferentes, los que es notable es el hecho de que una de ellas aprovechó la inyección de plantilla y la falla del Editor de Ecuaciones de Microsoft (CVE-2017-11882), un problema de corrupción de memoria de 20 años en Microsoft Office, que al explotar con éxito, permite a los atacantes ejecutar código remoto en una máquina vulnerable aún sin la interacción del usuario.

Microsoft solucionó el problema con un parche lanzado en noviembre de 2017.

Como suele suceder con campañas de malspam, el ataque requiere algo de ingeniería social para inducir al usuario a abrir un documento de Word aparentemente realista, que tiene información sobre la política de producción de defensa del gobierno indio.

Además, los archivos LNK tienen una extensión doble («*Defense-Production-Policy-2020.docs.lnk*») y vienen con iconos de documentos, lo que engaña a la víctima desprevenida para abrir el archivo.

Una vez abiertos, los archivos LNK abusan de «mshta.exe» para ejecutar archivos HTA (Microsoft HTML Applications) maliciosos que están alojados en sitios web fraudulentos, y los

archivos HTA se crean utilizando una herramienta de generación de carga útil de código abierto llamada CACTUSTORCH.

El archivo HTA de primera etapa incluye un documento señuelo y un módulo .NET malicioso que ejecuta dicho documento y descarga un archivo HTA de segunda etapa, que a su vez comprueba la presencia de soluciones antivirus populares antes de copiar la credencial de Microsoft y la utilidad de restauración («credwiz.exe») a una carpeta diferente en la máquina víctima y modificando el registro para ejecutar el ejecutable copiado cada vez que se inicia.

En consecuencia, cuando el archivo se ejecuta, no solo carga un archivo «DUser.dll» malicioso, sino que también inicia el módulo RAT «winms.exe», ambos obtenidos de la etapa 2 de HTA.

> *«Este DUser.dll iniciará la conexión a través de esta dirección IP '173.212.224.110' a través del puerto TCP 6102»,* dijeron los investigadores.
>
> *«Una vez conectado con éxito, procederá a realizar varias operaciones basadas en el comando recibido de C2. Por ejemplo, si C2 envía 0, entonces recopila el nombre de la computadora, el nombre de usuario, la versión del sistema operativo, etc. y lo envía de vuelta a C2».*

Al afirmar que el RAT comparte similitudes a nivel de código con Allakore Remote, un software de acceso remoto de código abierto escrito en Delphi, el equipo de Seqrite de Quick Heal notó que el troyano empleó el protocolo RFB (búfer de tramas remotas) de Allakore para exfiltrar datos del sistema infectado.

Además, se cree que algunas cadenas de ataque han eliminado un RAT basado en .NET nunca antes visto (llamado «Crimsom RAT» por los investigadores de Kaspersky), que viene equipada con una amplia gama de capacidades, que incluyen archivos de acceso, datos del

portapapeles y procesos de eliminación, e incluso ejecutar comandos arbitrarios.

Aunque el modus operandi de nombrar archivos DLL comparte similitudes con el grupo SideWinder, la gran dependencia de la APT del conjunto de herramientas de código abierto y una infraestructura C2 completamente diferente, llevó a los investigadores a concluir con una gran confianza que el actor de la amenaza es de origen paquistaní, específicamente Transparent Tribe Group, que recientemente se ha relacionado con varios ataques contra el ejército y el personal del gobierno de la India.

> *«Por lo tanto, sospechamos que el actor detrás de esta operación es una subdivisión de el grupo APT Transparent Tribe y simplemente está copiando los TTP de otros actores de amenazas para engañar a la comunidad de seguridad»,* dijo Quick Heal.