Investigadores de seguridad cibernética descubrieron hoy la forma de operar de un grupo de amenaza evasivo que ataca a entidades militares y diplomáticas de alto perfil en Europa del Este para actividades de espionaje.

Los hallazgos son parte de un análisis colaborativo realizado por la empresa de seguridad cibernética ESET y las empresas afectadas, lo que resulta en una gran revisión de las operaciones de InvisiMole y las tácticas, herramientas y procedimientos (TTP) del grupo.

> *«Los investigadores de ESET realizaron una investigación de estos ataques en cooperación con las organizaciones afectadas y pudieron descubrir los extensos y sofisticados conjuntos de herramientas utilizadas para la entrega, el movimiento lateral y la ejecución de las puertas traseras de InvisiMole»,* dijo la compañía en un informe.

Cooperación con Gamaredon Group

Descubierto por primera vez en 2018, InvisiMole ha estado activo por lo menos desde 2013 en relación con operaciones específicas de espionaje cibernético en Ucrania y Rusia. Luego de pasar desapercibido, el actor de la amenaza regresó a finales del 2019 con un conjunto de herramientas actualizado y tácticas previamente no reportadas para ofuscar el malware.

> *«InvisiMole tiene una arquitectura modular, que comienza su viaje con una DLL de envoltura y realizar sus actividades usando otros dos módulos que están integrados en sus recursos. Ambos módulos son puertas traseras ricas en funciones, que juntas le dan la capacidad de recopilar tanta información sobre el objetivo como sea posible»*, dijeron los investigadores de ESET en 2018.

Se descubrió que el spyware denominado RC2FM y RC2CL, era capaz de realizar cambios en el sistema, escanear redes inalámbricas para rastrear la geolocalización de las víctimas,

recopilar información del usuario e incluso cargar archivos confidenciales ubicados en la máquina comprometida. Pero el mecanismo exacto de entrega de malware seguía sin estar claro hasta ahora.

ESET no solo encontró evidencia de técnicas de «*living off the land*« que explotaban aplicaciones legítimas para llevar a cabo sigilosamente operaciones maliciosas, sino que también descubrió vínculos con un segundo actor de amenaza llamado Gamaredon Group, que tiene una gran historia de ataques cibernéticos contra instituciones ucranianas.

> *«Gamaredon se utiliza para allanar el camino para una carga útil mucho más sigilosa; según nuestra telemetría, un pequeño número de objetivos de Gamaredon se actualiza al malware avanzado InvisiMole, probablemente aquellos considerados particularmente significativos por los atacantes»,* dijeron los investigadores.

También mencionaron que el malware se implementa solo después de que los atacantes obtuvieron privilegios administrativos, ya que muchos de los métodos de ejecución de InvisiMole requieren permisos elevados.

Una vez que se produce el compromiso inicial, InvisiMole explota las vulnerabilidades BlueKeep (CVE-2019-0708) y EternalBlue (CVE-2017-0144) en los protocolos RDP y SMB, o utiliza documentos troyanizados e instaladores de software para propagarse lateralmente por medio de la red.

Además de emplear versiones actualizadas de las puertas traseras RC2L y RC2FM, el malware aprovecha un nuevo descargador TCS para descargar módulos adicionales y un descargador DNS, que a su vez, aprovecha el túnel DNS para enmascarar las comunicaciones a un servidor controlado por el atacante.

> *«Con el túnel DNS, el cliente comprometido no contacta directamente con el servidor C&C; solo se comunica con los servidores DNS benignos con los que la máquina víctima normalmente se comunicaría, donde envía solicitudes para resolver un dominio a su dirección IP. El servidor DNS se pone en contacto con el servidor de nombres responsable del dominio en la solicitud, que es un servidor de nombres controlado por el atacante, y transmite su respuesta al cliente»*, dijeron los investigadores.

Además, las cargas finales, RC2CL y RC2FM, se entregaron a través de no menos de cuatro cadenas de ejecución diferentes que combinaron código malicioso de shell con herramientas legítimas y ejecutables vulnerables.

La puerta trasera RC2CL mejorada admite hasta 87 comandos, con capacidades para encender la cámara web y los dispositivos de micrófono para tomar fotos, grabar video y sonido, capturar la pantalla, recopilar información de la red, enumerar el software instalado y monitorear los documentos a los que la víctima accedió recientemente.

Aunque no se utiliza prominentemente, RC2FM tiene su propio conjunto de comandos de exfiltración de documentos, junto con nuevas características para registrar pulsaciones de teclas y omitir el control de acceso de usuario (UAC).

Además, las nuevas versiones de RC2CL y RC2FM cuentan con sus propios medios para escapar de la detección de antivirus, incluida la inyección en otros procesos inocuos y la supresión de características específicas, como el registro de teclas.

> *«Los objetivos considerados particularmente significativos por los atacantes se actualizan del malware Gamaredon relativamente simple al malware avanzado InvisiMole. Esta cooperación previamente desconocida entre los dos grupos permite que el grupo InvisiMole invente formas creativas de operar bajo el radar»*, dijo Zuzana Hromcová, investigadora de ESET.