El actor de amenazas persistentes avanzadas (APT) rastreado como Evilnum, muestra nuevamente signos de actividad renovada dirigida a entidades financieras y de inversión europeas.

> *«Evilnum es una backdoor que se puede usar para el robo de datos o para cargar cargas útiles adicionales. El malware incluye múltiples componentes interesantes para evadir la detección y modificar las rutas de infección en función del software antivirus identificado»,* dijo la compañía Proofpoint.

Los objetivos incluyen organizaciones con operaciones que respaldan el intercambio de divisas, criptomonedas y finanzas descentralizadas (DeFi). Se cree que la última ola de ataques comenzó a fines de 2021.

Los hallazgos también encajan con un informe de Zscaler el mes pasado que detalla campañas de ataques dirigidos de bajo volumen lanzadas contra compañías en Europa y Reino Unido.

Activo desde 2018, Evilnum es rastreado por la comunidad de seguridad cibernética en general utilizando los nombres TA4563 y DeathStalker, con cadenas de infección que culminan en el despliegue de la puerta trasera homónima que es capaz de reconocimiento, robo de datos o recuperación de cargas útiles adicionales.

El último conjunto de actividades marcadas por Proofpoint incorpora tácticas, técnicas y procedimientos (TTP) actualizados, que se basan en una combinación de archivos de Microsoft Word, ISO y Windows Shortut (LNK) enviados como archivos adjuntos de correo electrónico en correos de phishing dirigidos a las víctimas.

Otras variantes de la campaña detectadas a inicios de 2022 han hecho uso de señuelos

financieros para atraer a los destinatarios a abrir archivos .LNK dentro de archivos adjuntos ZIP maliciosos o hacer clic en las URL de OneDrive que contienen un archivo ISO o LNK.

En otro caso, el atacante cambió el modus operandi para entregar documentos de Microsoft Word cargados de macros que arrojan código JavaScript ofuscado diseñado para iniciar el binario de puerta trasera.

Esta metodología se cambió una vez más a mediados de 2022 para distribuir documentos de Word, que intentan recuperar una plantilla remota y conectarse a un dominio controlado por un atacante. Independientemente del vector de distribución empleado, los ataques conducen a la ejecución de la backdoor Evilnum.

Aunque no se identificaron los ejecutables de malware de próxima etapa, se sabe que la puerta trasera actúa como un conducto para entregar cargas útiles del proveedor de malware como servicio (MaaS) Golden Chickens.

> *«Las organizaciones financieras, especialmente las que operan en Europa y tienen intereses en criptomonedas, deben estar al tanto de la actividad de TA4563. El malware del grupo conocido como Evilnum está en desarrollo activo»,* dijo Sherrod DeGrippo, vicepresidente de investigación y detección de amenazas en Proofpoint.