Un empaquetador basado en shellcode denominado TrickGate ha estado operando con éxito sin llamar la atención durante más de seis años, al mismo tiempo que permite a los hackers implementar una amplia gama de malware como TrickBot, Emotet, AZORult, Agent Tesla, FormBook, Cerber, Maze y REvil a lo largo de los años.

> *«TrickGate logró permanecer bajo el radar por años porque es transformador: sufre cambios periódicamente»,* dijo Arie Olshtein, de Check Point Research.

Ofrecido como un servicio a otros atacantes desde al menos finales de 2016, TrickGate ayuda a ocultar las cargas útiles detrás de una capa de código contenedor en un intento de pasar las soluciones de seguridad instaladas en un host. Los empaquetadores también pueden funcionar como encriptadores al bloquear el malware como un mecanismo de ofuscación.

> *«Los empaquetadores tienen diferentes características que les permiten eludir los mecanismos de detección al aparecer como archivos benignos, ser difíciles de aplicar ingeniería inversa o incorporar técnicas de evasión de sandbox»,* dijo Proofpoint en diciembre de 2020.

Pero las actualizaciones frecuentes del empaquetador comercial como servicio significaron que TrickGate ha sido rastreado con varios nombres, como New Loader, Loncom y Crypter, basado en NSIS desde 2019.

Los datos de telemetría recopilados por Check Point indican que los actores de amenazas que aprovechan TrickGate se han centrado principalmente en el sector manufacturero y, en menor medida, en las verticales de educación, atención médica, gobierno y finanzas.

Las familias de malware más populares usadas en los ataques de los últimos dos meses incluyen FormBook, LokiBot, Agent Tesla, Remcos y Nanocore, con concentraciones significativas reportadas en Taiwán, Turquía, Alemania, Rusia y China.

La cadena de infección implica el envío de correos electrónicos de phishing con archivos adjuntos maliciosos o enlaces con trampas explosivas que conducen a la descarga de un cargador de shellcode que es responsable de descifrar y lanzar la carga real en la memoria.

El análisis de los shellcode de la compañía de seguridad israelí muestran que *«se ha actualizado constantemente, pero las funcionalidades principales existen en todas las muestras desde 2016. El módulo de inyección ha sido la parte más consistente a lo largo de los años y se ha observado en todos los códigos de shell de TrickGate»,* dijo Olshtein.