Los hackers están utilizando un encriptador evasivo basado en .NET llamado DarkTortilla para distribuir una amplia gama de malware básico, así como cargas útiles específicas como Cobalt Strike y Metasploit, probablemente desde el año 2015.

> *«También puede entregar 'paquetes complementarios', como cargas útiles maliciosas adicionales, documentos señuelo benignos y ejecutables. Cuenta con sólidos controles anti-análisis y anti-manipulación que pueden hacer que la detección, el análisis y la erradicación sean un desafío»,* dijo la compañía de ciberseguridad Secureworks.

El malware entregado por el encriptador incluye ladrones de información y troyanos de acceso remoto (RAT) como Agent Tesla, AsyncRat, NanoCore y RedLine Stealer. *«DarkTortilla tiene una versatilidad que un malware similar no tiene»,* dijeron los investigadores.

Los encriptadores son herramientas de software que utilizan una combinación de encriptación, ofuscación y manipulación de código de malware para eludir la detección por parte de las soluciones de seguridad.

La entrega de DarkTortilla ocurre por medio de correos electrónicos no deseados maliciosos que contienen archivos con un ejecutable para un cargador inicial que se utiliza para decodificar y ejecutar un módulo de procesador central, ya sea incrustado dentro de sí mismo o extraído de sitios de almacenamiento de texto como Pastebin.

Después, el procesador central es responsable de establecer la persistencia e inyectar la carga principal de RAT en la memoria sin dejar rastro en el sistema de archivos por medio de un archivo de configuración elaborado, que también permite colocar paquetes adicionales, incluyendo registradores de teclas, ladrones de portapapeles y mineros de criptomonedas.

DarkTortilla es más notable por su uso de controles antimanipulación que aseguran que los procesos utilizados para ejecutar los componentes en la memoria se vuelvan a ejecutar de forma inmediata luego de la finalización.

Específicamente, la persistencia del cargador inicial se logra por medio de un segundo ejecutable denominado WatchDog, que está diseñado para controlar el proceso designado y volver a ejecutarlo en caso de que se elimine.

Esta técnica recuerda a un mecanismo similar adoptado por un atacante llamado Moses Staff, que a inicios de 2022, se apoyó en un enfoque basado en un perro guardián para evitar cualquier interrupción de sus cargas útiles. También se emplean otros dos controles para garantizar la ejecución continua del mismo ejecutable de WatchDog y la persistencia del cargador inicial.

Secureworks dijo que identificó un promedio de 93 muestras únicas de DarkTortilla cargadas en la base de datos de malware VirusTotal por semana durante un período de 17 meses desde enero de 2021 hasta mayo de 2022.

> *«DarkTortilla es capaz de evadir la detección, es altamente configurable y ofrece una amplia gama de malware popular y efectivo. Sus capacidades y prevalencia lo convierten en una amenaza formidable»*, dijeron los investigadores.