Investigadores advierten sobre RAT de Nerbian apuntando a entidades en Italia, España y Reino Unido

Autor: I. Stepanenko

Fecha: Friday 27th of May 2022 01:28:14 PM

Un troyano de acceso remoto (RAT) previamente indocumentado, escrito en el lenguaje de programación Go, fue detectado desproporcionadamente dirigido a entidades en Italia, España y el Reino Unido.

Llamado Nerbian RAT por la compañía de seguridad empresarial Proofpoint, el nuevo malware aprovecha los señuelos con el tema de COVID-19 para propagarse como parte de una campaña de phishing transmitida por correo electrónico de bajo volumen que comenzó el 26 de abril de 2022.

> «El RAT de Nerbian recientemente identificado aprovecha múltiples componentes antianálisis repartidos en varias etapas, incluyendo varias bibliotecas de código abierto», dijeron los investigadores de Proofpoint.

> «Está escrito en el lenguaje de programación Go independiente del sistema operativo (SO), compilado para sistemas de 64 bits y aprovecha varias rutinas de cifrado para evadir aún más el análisis de red».

Los mensajes, que suman menos de 100, pretenden ser de la Organización Mundial de la Salud sobre medidas de seguridad relacionadas con COVID-19, instando a las posibles víctimas a abrir un documento de Microsoft Word con macros para acceder a los *«últimos consejos de salud».*

Habilitar las macros muestra la guía de COVID-19, incluidos los pasos para el autoaislamiento, mientras que, en segundo plano, la macro integrada desencadena una cadena de infección que entrega una carga llamada «UpdateUAV.exe», que actúa como cuentagotas para Nerbian RAT («MoUsoCore.exe») desde un servidor remoto.

El cuentagotas también hace uso del *«marco anti-VM Chacal«* de código abierto para

dificultar la ingeniería inversa, usándolo para llevar a cabo comprobaciones anti-reversa y finalizándose si encuentra algún depurador o programa de análisis de memoria.

El troyano de acceso remoto, por su parte, está equipado para registrar pulsaciones de teclas, realizar capturas de pantalla y ejecutar comandos arbitrarios, antes de filtrar los resultados al servidor.

Aunque se dice que tanto el cuentagotas como el RAT fueron desarrollados por el mismo autor, la identidad del actor de la amenaza aún se desconoce.

Además, Proofpoint advirtió que el cuentagotas podría personalizarse para entregar diferentes cargas útiles en futuros ataques, aunque en su forma actual, solo puede recuperar la RAT de Nerbian.

> «Los autores de malware siguen operando en la intersección de la capacidad de código abierto y la oportunidad criminal», dijo Sherrod DeGrippo, vicepresidente de investigación y detección de amenazas en Proofpoint.