Aunque han habido múltiples esfuerzos por detener las operaciones de TrickBot y se logró interrumpir la mayor parte de su infraestructura, los operadores del malware no permanecen inactivos.

Según nuevos hallazgos de la compañía de seguridad cibernética Netscout, los autores de TrickBot han trasladado partes de su código a Linux, en un intento por ampliar el alcance de las víctimas.

TrickBot es un troyano bancario detectado por primera vez en 2016, ha sido una solución de software delictivo basado en Windows, que emplea diferentes módulos para realizar una amplia gama de actividades maliciosas en las redes objetivo, incluyendo el robo de credenciales y realizar ataques con ransomware.

En las últimas semanas, esfuerzos en conjunto liderados por el Comando Cibernético de Estados Unidos, y Microsoft, han ayudado a eliminar el 94% de los servidores de comando y control (C2) de TrickBot que estaban operando, y la nueva infraestructura que los ciberdelincuentes intentaron poner en línea para reemplazar los servidores desactivados.

A pesar de las medidas tomadas para impedir TrickBot, Microsoft advirtió que los actores de amenazas detrás de la botnet probablemente harían más esfuerzos para reactivar sus operaciones.

Módulo Anchor de TrickBot

A fines de 2019, se descubrió un nuevo marco de puerta trasera de TrickBot llamado Anchor, que utiliza el protocolo DNS para comunicarse con los servidores C2 sigilosamente.

> El módulo *«permite a los actores (clientes potenciales de TrickBot) aprovechar este marco contra víctimas de mayor perfil. La capacidad de integrar sin problemas la APT en un modelo comercial de monetización es evidencia de un cambio cuántico»*, dijo SentinelOne.

IBM X-Force detectó nuevos ataques cibernéticos a principios de abril, que revelaron la colaboración entre FIN6 y los grupos TrickBot para implementar el marco Anchor contra organizaciones con fines de lucro.

La variante, denominada *«Anchor_DNS»*, permite al cliente infectado utilizar el túnel DNS para establecer comunicaciones con el servidor C2, que a su vez transmite datos con IP resueltas como respuesta, según los investigadores de NTT en un informe de 2019.

Pero una nueva muestra descubierta por el investigador de seguridad de Stage 2, Waylon Grange, en julio, encontró que Anchor_DNS se ha portado a una nueva versión de puerta trasera de Linux llamada Anchor_Linux.

> *«A menudo entregado como parte de un zip, este malware es una puerta trasera ligera de Linux. Tras la ejecución, se instala a sí mismo como un trabajo cron, determina la dirección IP pública para el host y luego comienza a emitir señales a través de consultas de DNS a su servidor C2»,* dijo Grange.

La última investigación de Netscout decodifica este flujo de comunicación entre el bot y el servidor C2. Durante la fase de configuración inicial, el cliente envía *«c2_command 0»* al servidor junto con información sobre el sistema comprometido y el ID del bot, que luego responde con el mensaje *«signal/1/»* al bot.

Como reconocimiento, el bot envía el mismo mensaje de vuelta al C2, luego de esto, el servidor emite remotamente el comando se ejecutará en el cliente. En el último paso, el bot envía el resultado de la ejecución al servidor C2.

> *«Cada parte de la comunicación hecha al C2 sigue una secuencia de 3 consultas DNS diferentes»*, dojo la investigadora de Netscout, Suweera De Souza.

Una lista de registros de IP que denota los datos correspondientes a la carga útil es el resultado de la tercera consulta, que posteriormente el cliente analiza para generar la carga útil ejecutable.

El último dato enviado por el servidor C2 corresponde a un rango de comandos (numerados 0-14 en Windows, 0-4, 10-12 y 100 en Linux) para que el bot ejecute la carga útil a través de cmd.exe o inyectándolo en varios procesos de ejecución, como el Explorador de Windows o el bloc de notas.

> *«La complejidad de la comunicación C2 de Anchor y las cargas útiles que el bot puede ejecutar reflejan no solo una parte de las considerables capacidades de los actores de TrickBot, sino también su capacidad para innovar de forma constante, como lo demuestra su cambio a Linux»*, dijo De Souza.