Los piratas informáticos están abusando cada vez más de Telegram, como un sistema de *«comando y control»* para distribuir malware en organizaciones, que luego podrían utilizarse para capturar información confidencial de sistemas específicos.

«Incluso cuando Telegram no está instalado o en uso, el sistema permite a los hackers enviar comandos y operaciones maliciosas de forma remota a través de la aplicación de mensajería instantánea», dijeron los investigadores de Check Point, que identificaron no menos de 130 ataques en los últimos 3 meses, que utilizan un nuevo troyano multifuncional de acceso remoto (RAT) llamado ToxicEye.

El uso de Telegram para facilitar actividades maliciosas no es nuevo. En septiembre de 2019, se descubrió que un ladrón de información llamado Masad Stealer, robaba la información y datos de billeteras comprometidas de computadoras infectadas utilizando Telegram como canal de exfiltración. Después, el año pasado, los grupos de Magecart adoptaron la misma técnica para enviar detalles de pago robados de sitios web comprometidos.

La estrategia conviene a los hackers por distintas razones, comenzando con que Telegram no solo está bloqueado por los motores antivirus empresariales, la aplicación de mensajería también permite a los atacantes permanecer en el anonimato, ya que el proceso de registro solo requiere un número de teléfono móvil, lo que brinda acceso a dispositivos infectados desde prácticamente cualquier lugar del mundo.

La última campaña detectada por Check Point no es diferente. Difundido a través de correos electrónicos de phishing con un archivo ejecutable de Windows malicioso como adjunto, ToxicEye utiliza Telegram para comunicarse con el servidor de comando y control (C2) y cargar datos en él.

El malware también tiene una variedad de exploits que le permiten robar datos, transferir y eliminar archivos, finalizar procesos, implementar un registrador de teclas, secuestrar el micrófono y la cámara de la computadora, e incluso cifrar archivos para obtener un rescate.

De forma específica, la cadena de ataque comienza con la creación de un bot de Telegram

por parte del atacante, que luego se incrusta en el archivo de configuración del RAT, antes de compilarlo en un ejecutable (por ejemplo, «paypal checker by saint.exe»). Este archivo .exe después se inyecta en un documento de señuelo de Word («solution.doc) que, al ser ejecutado, descarga y ejecuta Telegram RAT («C:\Users\ToxicEye\rat.exe»).

> *«Hemos descubierto una tendencia creciente en la que los autores de malware utilizan la plataforma Telegram como un sistema de comando y control listo para usar para la distribución de malware en las organizaciones. Creemos que los atacantes están aprovechando el hecho de que Telegram se usa y se permite en casi todas las organizaciones, utilizando este esquema para realizar nuevos ataques cibernéticos, que pueden eludir las restricciones de seguridad»*, dijo Idan Sharabi, gerente del grupo de I+D de Check Point.