Telegram es la favorita de ciberdelincuentes para robar datos

El correo electrónico sigue siendo el canal preferido para el robo de datos en las campañas de ‘phishing’ pero el servicio de mensajería Telegram ha experimentado un importante crecimiento en 2022 para este mismo fin.

La firma de ciberseguridad Group-IB ha analizado más de 6.000 kits de ‘phishing’ extraídos en los años 2021 y 2022, y ello le ha permitido constatar el crecimiento del uso de herramientas de control de acceso y de técnicas avanzadas de evasión de detección.

Estos kits son herramientas que se facilitan a los ciber criminales para lanzar sin esfuerzo campañas de ‘phishing’, es decir, ataques que suplantan una fuente legítima y se distribuyen a través de correo electrónico para engañar a las potenciales víctimas.

En 2022 identificaron 3.677 kits de ‘phishing’ únicos, un 25 por ciento más que en 2021. El correo electrónico, con el servicio Gmail de Google a la cabeza (45 %), se presenta como el canal de recopilación de datos preferido en estas campañas, como explican en una publicación en su blog oficial.

Este canal ha experimentado un crecimiento del 22 por ciento respecto de 2021, con la identificación de 3.278 kits basados en el ‘email’. Otros 1.516 kits se basaban en servidores locales (crecimiento del 17 %), aunque el principal crecimiento lo experimenta Telegram, que pese a ser el tercer canal de preferencia, con 623 kits, ha aumentado en un 68 por ciento.

Desde la firma de seguridad explican que el crecimiento de Telegram puede deberse a que “la flexibilidad y conveniencia [del servicio de mensajería] permiten a los ciberdelincuentes procesar y administrar información comprometida casi en tiempo real”.

De los kits analizados de 2022, 1.824 usaban mecanismos de control de acceso, un 92 por ciento más que en el año anterior. Destacan los archivos de acceso de hipertexto, los archivos robots.txt y los índices vacíos.

Otros 2.060 kits usaron técnicas avanzadas de evasión de

detección, lo que supone un aumento del 26 por ciento respecto de los detectados en 2021. Desde Group-IB alertan del crecimiento de este tipo de tácticas, en las que se incluyen las técnicas antibot y la aleatorización, ya que, entienden, “plantea un desafío importante para los sistemas de detección convencionales y prolonga la vida útil de las campañas de phishing”.

Con información de Primicia