El software malicioso bancario llamado Carbanak ha sido identificado en ataques de extorsión digital utilizando métodos renovados.

> *«El software ha evolucionado incorporando proveedores y tácticas de ataque para ampliar su alcance»,* mencionó la entidad de seguridad cibernética NCC Group en un estudio sobre incidentes de extorsión digital de noviembre de 2023.

> *«Carbanak hizo una reaparición el mes anterior a través de nuevas vías de distribución y se ha propagado mediante portales web comprometidos simulando diversos programas de gestión empresarial.»*

Entre las herramientas falsificadas se encuentran software empresarial reconocido como HubSpot, Veeam y Xero.

Desde al menos 2014, Carbanak ha sido detectado por sus funciones de robo de información y control a distancia. Aunque inició como un malware para bancos, ha sido empleado por la organización criminal cibernética FIN7.

En el reciente patrón de ataque analizado por NCC Group, los portales comprometidos albergan archivos de instalación perjudiciales que se camuflan como herramientas legítimas, facilitando la activación de Carbanak.

Esta tendencia surge cuando se registraron 442 incidentes de extorsión digital el mes pasado, un aumento desde los 341 eventos en octubre de 2023. En lo que va del año, se han documentado 4,276 casos, cifra que es *«casi 1,000 eventos menos que la suma de 2021 y 2022 (5,198)».*

Las estadísticas de la firma indican que las áreas más afectadas son las industriales (33%), los sectores de consumo (18%) y el área sanitaria (11%), siendo Norteamérica (50%), Europa

(30%) y Asia (10%) los principales focos de ataque.

En relación a las variantes de extorsión digital más frecuentes, LockBit, BlackCat y Play representaron el 47% (o 206 ataques) de los 442 incidentes. Tras la desarticulación de BlackCat este mes, es incierto el impacto que tendrá en la dinámica de amenazas próximamente.

> *«Con un mes pendiente, ya hemos superado los 4,000 ataques, marcando un incremento notable respecto a 2021 y 2022. Será crucial ver la tendencia el año venidero»*, apuntó Matt Hull, líder global de análisis de amenazas en NCC Group.

El pico de ataques de noviembre fue confirmado por la aseguradora digital Corvus, que reportó 484 nuevas víctimas de extorsión cibernética.

> *«La comunidad de extorsión digital ha virado su enfoque lejos de QBot. La incorporación de técnicas alternativas ha sido fructífera para los grupos extorsionadores»,* comentó Corvus.

Este cambio surge después de la intervención policial contra QBot. Microsoft, recientemente, reveló detalles de una campaña de phishing que diseminaba este malware, evidenciando los desafíos en la erradicación de estos grupos.

Por otro lado, Kaspersky informó que el ransomware Akira obstaculiza su análisis al generar señales de alerta al intentar acceder con herramientas de depuración.

La entidad rusa de seguridad resaltó la explotación de vulnerabilidades en el sistema de registro común de Windows (CLFS) – CVE-2022-24521, CVE-2022-37969, CVE-2023-23376, CVE-2023-28252 (calificación CVSS: 7.8) – para lograr elevación de privilegios.