Una nueva campaña de malware QBot está aprovechando la correspondencia comercial secuestrada para engañar a las víctimas desprevenidas para que instalen el malware, según las revelaciones de Kaspersky.

La actividad más reciente, que comenzó el 4 de abril de 2023, se centró principalmente en usuarios de Alemania, Argentina, Italia, Argelia, España, Estados Unidos, Rusia, Francia, Reino Unido y Marruecos.

QBot, también conocido como Qakbot o Pinkslipbot, es un troyano bancario que se sabe que está activo desde al menos 2007. Además de robar contraseñas y cookies de los navegadores web, funciona como una puerta trasera para inyectar cargas útiles de siguiente etapa como Cobalt Strike o piezas de ransomware.

Distribuido por medio de campañas de phishing, el malware ha visto actualizaciones constantes durante su vida, que incluyen técnicas anti-VM, anti depuración y anti sandbox para evadir la detección. También se ha convertido en el malware más frecuente durante el mes de marzo de 2023, según Check Point.

> *«Al principio, se distribuía por medio de sitios web infectados y software hackeado. Ahora el banquero se entrega a las víctimas potenciales a través del malware que ya reside en sus computadoras, la ingeniería social y los correos no deseados»,* dijeron los investigadores de Kaspersky.

Los ataques de secuestro de hilos de correo electrónico no son nuevos. Ocurre cuando los ciberdelincuentes se insertan en conversaciones comerciales existentes o inician nuevas conversaciones basadas en información recopilada previamente por cuentas de correo electrónico comprometidas.

El objetivo es atraer a las víctimas para que abran enlaces maliciosos o archivos adjuntos maliciosos, en este caso, un archivo PDF adjunto que se hace pasar por una alerta de Microsoft Office 365 o Microsoft Azure.

Al abrir el documento, se recupera un archivo comprimido de un sitio web infectado que, a su vez, contiene un archivo de script de Windows ofuscado (.WSF). El script, por su parte, incorpora un script de PowerShell que descarga DLL maliciosas desde un servidor remoto. La DLL descargada es el malware QBot.

Los hallazgos surgen cuando Elastic Security Labs descubrió una campaña de ingeniería social de múltiples etapas que emplea documentos de Microsoft Word armados para distribuir Agent Tesla y XWorm por medio de un cargador personalizado basado en .NET.