Los hackers están adoptando cada vez más documentos de Excel 4.0 como un vector de etapa inicial para distribuir malware como ZLoader y Quakbot, según una nueva investigación.

Los hallazgos provienen de un análisis de 160,000 documentos de Excel 4.0 entre noviembre de 2020 y marzo de 2021, de los cuales más del 90% se clasificaron como maliciosos o sospechosos.

> *«El mayor riesgo para las empresas e individuos objetivo es el hecho de que las soluciones de seguridad todavía tienen muchos problemas para detectar documentos maliciosos de Excel 4.0, lo que hace que la mayoría de estos se escapen mediante detecciones convencionales basadas en firmas y reglas YARA descritas por analistas»,* dijeron los investigadores de ReversingLabs.

Las macros de Excel 4.0 (XLM), el precursor de Visual Basic para Aplicaciones (VBA), es una característica heredada incorporada en Microsoft Excel por razones de compatibilidad con versiones anteriores. Microsoft advierte en su documento de soporte que habilitar todas las macros puede provocar la ejecución de *«código potencialmente peligroso»*.

Quakbot, también conocido como QBOT, se descubrió en 2007 y ha estado en constante evolución. Se ha mantenido como un troyano bancario notorio capaz de robar credenciales bancarias y otra información financiera, al mismo tiempo que obtiene características de propagación similares a gusanos.

Normalmente, las variantes de Quakbot se propagan a través de documentos de Office armados y han podido entregar otras cargas útiles de malware, registrar pulsaciones de teclas de los usuarios e incluso, crear una puerta trasera para las máquinas comprometidas.

En un documento analizado por ReversingLabs, el malware no solo engañó a los usuarios para que habilitaran macros con señuelos convincentes, sino que también incluía archivos incrustados que contienen macros XLM que descargan y ejecutan una carga útil maliciosa de

segunda etapa recuperada de un servidor remoto. Otra muestra incluyó una carga útil codificada en Base64 en una de las hojas, que luego intentó descargar malware adicional desde una URL comprometida.

> *«Aunque la compatibilidad con versiones anteriores es muy importante, algunas cosas deberían tener una esperanza de vida y, desde una perspectiva de seguridad, probablemente sería mejor si se desaprobaran en algún momento. El costo de mantener macros de 30 años debe sopesarse con los riesgos de seguridad que conlleva el uso de una tecnología tan obsoleta»,* dijeron los investigadores.