El notorio malware Emotet, en su regreso después de una pausa, se distribuye por medio de archivos adjuntos de correo electrónico de Microsoft OneNote en un intento de eludir las restricciones de seguridad basadas en macros y los sistemas de compromiso.

Emotet, vinculado a un actor de amenazas rastreado como Gold Crestwood, Mummy Spider o TA542, sigue siendo una amenaza potente y resistente a pesar de los intentos de las fuerzas del orden por eliminarlo.

Un derivado del gusano bancario Cridex, que posteriormente fue reemplazado por Dridex casi al mismo tiempo que GameOver Zeus se interrumpió en 2014, Emotet se ha convertido en una *«plataforma monetizada para que otros atacantes ejecuten campañas maliciosas en un pago por instalació (PPI), modelo que permite el robo de datos confidenciales y la extorsión de rescate».*

Aunque las infecciones de Emotet han actuado como un conducto para entregar Cobalt Strike, IceID, Quakbot, Quantum ransomware y TrickBot, su regreso a fines de 2021 fue facilitado por medio de TrickBot.

> *«Emotet es conocido por períodos prolongados de inactividad, que por lo general ocurren varias veces al año, donde la red de bots se mantiene estable pero no envía spam ni malware»,* dice Secureworks.

El malware cuentagotas se distribuye comúnmente por medio de correos electrónicos no deseados que contienen archivos adjuntos maliciosos. Pero con Microsoft tomando medidas para bloquear macros en archivos de Office descargados, los archivos adjuntos de OneNote se han convertido en una vía alternativa atractiva.

> *«El archivo de OneNote es simple pero efectivo para los usuarios de ingeniería social con una notificación falsa que indica que el documento está protegido. Cuando se les indica que hagan doble clic en el botón Ver, las víctimas, sin darse*

> *cuenta, hacen doble clic en un archivo de script incrustado»,* dijo Malwarebytes.

El archivo se script de Windows (WSF) está diseñado para recuperar y ejecutar la carga útil binaria de Emotet desde un servidor remoto. Cyble, IBM X-Force y Unit42 de Palo Alto Networks se han hecho eco de hallazgos similares.

Emotet sigue utilizando documentos con trampas explosivas que contienen macros para entregar la carga útil maliciosa, empleando señuelos de ingeniería social para tentar a los usuarios a permitir que las macros activen la cadena de ataque.

Se ha observado que dichos documentos aprovechan una técnica llamada bomba de descompresión para ocultar un archivo muy grande (más de 550 MB) dentro de archivos adjuntos ZIP para pasar desapercibidos, según múltiples informes de Cyble, Deep Instinct, Hornetsecurity y TrendMicro.

Esto se logra rellenando 00 bytes al final del documento para inflar de forma artificial el tamaño del archivo y superar las limitaciones impuestas por las soluciones antimalware.

El último desarrollo es una señal de la flexibilidad y agilidad de los operadores para cambiar los tipos de archivos adjuntos para la entrega inicial con el fin de evadir las firmas de detección. También se produce en medio de un aumento en los hackers que usan documentos de OneNote para distribuir una amplia gama de malware como AsyncRAT, Icedid, RedLine Stealer, Quakbot y XWorm.

Según Trellix, la mayoría de las detecciones maliciosas de OneNote en 2023 se registraron en Estados Unidos, las finanzas y la energía emergen como los principales sectores objetivo.