Investigadores de seguridad rastrearon las actividades de un nuevo grupo de hackers con motivación financiera que se dirigen a distintas empresas y organizaciones en Alemania, Italia y Estados Unidos, en un intento de infección con malware de puerta trasera, troyano bancario o ransomware.

Estas campañas de malware no están personalizadas para cada organización, pero los actores de la amenaza están más interesados en empresas, servicios de TI, fabricación e industrias de atención médica que cuenten con datos críticos y que probablemente puedan pagar altos costos de rescate.

Según un informe de ProofPoint, los hackers recientemente descubiertos están enviando correos electrónicos de bajo volumen que se hacen pasar por entidades gubernamentales relacionadas con las finanzas con evaluación de impuestos y reembolsan correos electrónicos atraídos a organizaciones seleccionadas.

> *«Las campañas de correo electrónico con temas de impuestos se dirigen a los archivadores de este año, los señuelos relacionados con las finanzas se han utilizado estacionalmente con aumentos en el malware relacionado con los impuestos y las campañas de phishing que conducen a los plazos anuales de presentación de impuestos en diferentes geografías»,* dijeron los investigadores.

En casi todas las campañas de correo electrónico de *spear phishing* que los investigadores observaron entre el 16 de octubre y el 12 de noviembre de este año, los hackers utilizaron archivos adjuntos de documentos de Word maliciosos como un vector inicial para comprometer el dispositivo.

Una vez abierto el documento, se ejecuta una secuencia de comandos macro para ejecutar comandos maliciosos de PowerShell, que luego descarga e instala una de las siguientes cargas útiles en el sistema víctima:

- Maze Ransomware
- IcedID Banking Trojan
- Cobalt Strike Backdoor

> *«Al abrir el documento de Microsoft Word y habilitar las macros, se instala el ransomware Maze en el sistema del usuario, encripta todos sus archivos y se guarda una nota de rescate similar a la siguiente en formato TXT en cada directorio»*, agregaron los investigadores.

Además de la ingeniería social, para hacer que los correos electrónicos de phishing sean más convincentes, los atacantes también utilizan dominios parecidos, además de marcas robadas para suplantar, como:

- Oficina Federal Central de Impuestos, el Ministerio Federal de Hacienda de Alemania
- Agenzia delle Entrate, la Agencia de Ingresos de Italia
- 1 & 1 Internet AG, proveedor de servicios de Internet alemán
- SUPS, el Servicio Postal de Estados Unidos

> *«En Alemania e Italia también se observaron campañas similares que aprovechan las agencias gubernamentales locales. Estos señuelos de ingeniería social indican que los ciberdelincuentes en generar se han vuelto más convincentes y sofisticados en sus ataques».*
>
> *«Aunque estas campañas son pequeñas en volumen, actualmente son importantes por su abuso de marcas confiables, incluidas las agencias gubernamentales, y por su expansión relativamente rápida en múltiples geografías. Hasta ahora, el grupo parece haber apuntado a organizaciones en Alemania, Italia, y más recientemente, Estados Unidos, entregando cargas útiles con orientación geográfica con señuelos en los idiomas locales»*, dijo Christopher Dawson, Líder de Inteligencia de Amenazas

> en ProofPoint.

Cómo protegerse de estos ataques cibernéticos

Algunas de las opciones disponibles para proteger una computadora contra este tipo de ataques son las siguientes:

- Deshabilitar la ejecución de macros en archivos de Office
- Mantener una copia de seguridad periódica de los datos importantes
- Asegurarse de mantener en ejecución algún software antivirus
- No abrir archivos adjuntos de correo electrónico de fuentes desconocidas o no confiables
- No hacer clic en los enlaces de fuentes desconocidas