Se detectó una nueva campaña de phishing de correo electrónico que aprovecha la táctica del secuestro de conversaciones para enviar el malware de robo de información IceID a las máquinas infectadas mediante el uso de servidores de Microsoft Exchange sin parches y expuestos públicamente.

> *«Los correos electrónicos utilizan una técnica de ingeniería social de secuestro de conversaciones (también conocido como secuestro de hilos). Se está utilizando una respuesta falsificada a un correo electrónico robado anterior como una forma de convencer al destinatario de que abra el archivo adjunto. Esto es notable porque aumenta la credibilidad del correo electrónico de phishing y puede causar una alta tasa de infección»,* dijo la compañía Intezer.

La última ola de ataques, que fue detectada a mediados de marzo de 2022, se dirigió a organizaciones dentro de los sectores de energía, salud, derecho y farmacéutico.

IceID, también conocido como BokBot, al igual que sus contrapartes TrickBot y Emotet, es un troyano bancario que ha evolucionado para convertirse en un punto de entrada para amenazas más sofisticadas, incluido el ransomware operado por humanos y la herramienta de simulación adversaria Cobalt Strike.

Es capaz de conectarse a un servidor remoto y descargar implantes y herramientas de próxima etapa que permiten a los atacantes realizar actividades de seguimiento y moverse lateralmente por medio de las redes afectadas para distribuir malware adicional.

En junio de 2021, la empresa de seguridad empresarial Proofpoint, reveló una táctica en evolución en el programa del cibercrimen en la que se observó a los corredores de acceso inicial infiltrarse en las redes objetivo por medio de cargas útiles de malware de primera etapa como IceID para implementar cargas útiles de ransomware Egregor, Maze y REvil.

Aunque las campañas anteriores de IceID aprovecharon los formularios de contacto del sitio web para enviar enlaces con malware a las organizaciones, la versión actual del ataque se

basa en servidores vulnerables de Microsoft Exchange para enviar correos electrónicos atractivos desde una cuenta secuestrada, lo que indica una mayor evolución del esquema de la ingeniería social.

> *«La carga útil también se ha alejado del uso de documentos de Office al uso de archivos ISO con un archivo LNK de Windows y un archivo DLL. El uso de archivos ISO permite que el actor de amenazas eluda los controles de Mark-of-the-Web, lo que da como resultado la ejecución del malware sin advertir al usuario»,* dijeron los investigadores Joakim Kennedy y Ryan Robinson.

La idea es enviar respuestas fraudulentas a un hilo de correo electrónico ya existente saqueado de la cuenta de la víctima mediante el uso de la dirección de correo electrónico de la persona comprometida para que los correos electrónicos de phishing parezcan más legítimos.

> *«El uso del secuestro de conversaciones es una poderosa técnica de ingeniería social que puede aumentar la tasa de un intento de phishing exitoso. Al usar este enfoque, el correo electrónico parece más legítimo y se transporta por medio de los canales normales que también pueden incluir productos de seguridad»,* finalizaron los investigadores.