Se ha observador que los atacantes detrás de la familia de ransomware Black Basta, están usando el troyano Qakbot para implementar el marco Brute Ratel C4 como una carga útil de segunda etapa en ataques recientes.

El desarrollo marca la primera vez que el software de simulación de adversarios se entrega a través de una infección de Qakbot, dijo la compañía de seguridad cibernética Trend Micro, en un análisis técnico publicado la semana pasada.

La intrusión, lograda mediante un correo electrónico de phishing que contenía un enlace armado que apuntaba a un archivo ZIP, implicó además el uso de Cobalt Strike para el movimiento lateral.

Aunque estas utilidades legítimas están diseñadas para realizar actividades de pruebas de penetración, su capacidad para ofrecer acceso remoto las ha convertido en una herramienta lucrativa en manos de atacantes que buscan sondear sigilosamente el entorno comprometido sin llamar la atención durante largos períodos de tiempo.

Esto se ha visto agravado por el hecho de que una versión descifrada de Brute Ratel C4 comenzó a circular el mes pasado entre los delincuentes cibernéticos clandestinos, lo que llevó a su desarrollador a actualizar el algoritmo de licencias para que sea más difícil de descifrar.

Qakbot, también llamado QBot y QuackBot, es un ladrón de información y un troyano bancario que se sabe que está activo desde 2007. Pero su diseño modular y su capacidad para actuar como descargador lo han convertido en un candidato atractivo para colocar malware adicional.

Según Trend Micro, el archivo ZIP en el correo electrónico contiene un archivo ISO que, a su vez, incluye un archivo LNK que obtiene la carga útil de Qakbot, lo que ilustra los intentos de parte de los atacantes por adaptarse a otras técnicas después de la decisión de Microsoft de bloquear macros por defecto para documentos descargados de la web.

La infección de Qakbot es reemplazada por la recuperación de Brute Ratel y Cobalt Strike, pero no antes de realizar un reconocimiento automatizado por medio de herramientas de línea de comandos integradas como arp, ipconfig, nslookup, netstat y whoami.

Sin embargo, el ataque se detuvo antes de que el actor de amenazas pudiera tomar cualquier acción maliciosa, aunque se sospecha que el objetivo final puede haber sido la implementación de ransomware en todo el dominio.

En otra cadena de ejecución de Qakbot detectada por la compañía de ciberseguridad, el archivo ZIP se entrega por medio de un método cada vez más popular llamado contrabando de HTML, lo que resulta en la ejecución de Brute Ratel C4 como segunda etapa.

> *«La cadena de eliminación de Qakbot a Brute Ratel a Cobalt Strike está asociada con el grupo detrás del Black Basta Ransomware. Esto se basa en la superposición de TTP e infraestructura observada en los ataques de Black Basta»,* dijeron los investigadores.

Los hallazgos coinciden con un resurgimiento de los ataques de Quakbot en los últimos meses por medio de una variedad de técnicas como archivos adjuntos HTML, carga lateral de DLL y secuestro de hilos de correo electrónico, el último de los cuales implicó la recolección masiva de correos electrónicos de ataques exitosos de ProxyLogon dirigidos a Microsoft.

Los atacantes de IceID diversifican sus métodos de entrega

Quakbot está lejos de ser el único malware de acceso como servicio que se distribuye cada vez más a través de ISO y otros formatos de archivo para sortear las restricciones de macros,

ya que las campañas de Emotet, IceID y Bumblebee han seguido trayectorias similares.

Unit 42 de Palo Alto Networks, a fines de septiembre de 2022, dijo que descubrió un archivo malicioso políglota Microsoft Compiled HTML Help (CHM), que se usa para entregar el malware IceID (también conocido como BokBot).

Otros métodos de entrega y vías de infección destacados han implicado el uso de archivos ZIP protegidos con contraseña que contienen un archivo ISO, que refleja el de Quakbot, con la carga útil propagada por medio de un servicio de pago por instalador conocido como PrivateLoader, según Team Cymru.

Además, Emotet parece estar preparándose para un nuevo conjunto de ataques después de una breve pausa de tres meses para reelaborar su módulo *«systeminfo»* para *«mejorar la orientación de víctimas específicas y distinguir los bots de seguimiento de los usuarios reales»*, reveló ESET.

> *«No hemos visto nuevas oleadas de spam de Emotet desde julio. No está claro por qué es eso»*, dijo Jean-Ian Boutin, diretor de investigación de amenazas de ESET.

> *«Tomaron algunos descansos en el pasado, pero nunca por tanto tiempo. Tal vez este nuevo módulo signifique que están probando módulos y estarán activos nuevamente en un futuro cercano, pero esto, por supuesto, es una especulación».*