Un conocido troyano bancario que roba credenciales y otra información financiera, ha regresado con nuevas características para atacar a los sectores gubernamental, militar y manufacturero en Estados Unidos y Europa.

En un análisis publicado hoy por Check Point Research, la última ola de actividad de Qbot parece haber coincidido con el regreso de Emotet, otro malware basado en correo electrónico detrás de distintas campañas de spam, impulsadas por botnets y ataques de ransomware.

> *«En estos días, Qbot es mucho más peligroso que antes: tiene una campaña activa de malspam que infecta a las organizaciones y se las arregla para utilizar una infraestructura de infección de terceros como la de Emotet, para extender la amenaza aún más»,* dijeron los investigadores.

Documentado por primera vez en 2008, Qbot (también conocido como QuakBot, QakBot o Pinkslipbot) ha evolucionado a lo largo de los años de un simple ladrón de información, a una *«navaja suiza»* experta en distribuir otros tipos de malware, incluido el ransomware Prolock, e incluso, conectarse de forma remota a un sistema Windows objetivo para realizar transacciones bancarias desde la dirección IP de la víctima.

Los atacantes suelen infectar a las víctimas mediante técnicas de phishing para atraer a las víctimas a sitios web que utilizan exploits para inyectar Qbot a través de un cuentagotas.

Una ofensiva de malspam observada por F5 Labs en junio, descubrió que el malware estaba equipado con técnicas de detección y evasión de investigación con el objetivo de evadir el examen forense.

La semana pasada, Morphisec desempaquetó una muestra de Qbot que venía con dos nuevos métodos diseñados para eludir los sistemas de Desarmado y Reconstrucción de Contenido (CDR) y Detección de Respuesta de Endpoint (EDR).

La cadena de infección detallada por Check Point sigue un patrón similar. El primer paso comienza con un correo electrónico de phishing especialmente diseñado que contiene un archivo ZIP adjunto o un enlace a un archivo ZIP que incluye un Visual Basic Script (VBS) malicioso, que luego descarga cargas útiles adicionales responsables de mantener un canal de comunicación adecuado con un atacante.

Particularmente, los correos electrónicos de phishing enviados a las organizaciones objetivo, que toman la forma de señuelos COVID-19, recordatorios de pago de impuestos o reclutamiento de trabajo, no solo incluyen el contenido malicioso, sino que también se insertan con hilos de correo electrónico archivados entre las dos partes para prestar un aire de credibilidad.

Para lograr el objetivo, las conversaciones se recopilan de antemano mediante un módulo de recopilación de correo electrónico, que extrae todos los hilos de correo electrónico del cliente Outlook de la víctima y los carga en un servidor remoto codificado.

Aparte de los componentes de embalaje para obtener contraseñas, cookies del navegador e inyectar código JavaScript en los sitios web de banca, los operadores Qbot han liberado hasta 15 versiones del software malicioso desde el inicio de 2020, con la última versión conocida lanzada el 7 de agosto.

Qbot cuenta con un complemento hVNC que hace posible controlar la máquina víctima a través de una conexión VNC remota.

> *«Un operador externo puede realizar transacciones bancarias sin el conocimiento del usuario, incluso mientras está conectado a su computadora. El módulo comparte un alto porcentaje de código con módulos similares como hVNC de TrickBot»,* dijo Check Point.

Además, Qbot está equipado con un mecanismo separado para reclutar las máquinas comprometidas en una botnet mediante el uso de un módulo proxy que permite que la

máquina infectada se utilice como servidor de control

> *«Nuestra investigación muestra cómo incluso las formas más antiguas de malware pueden actualizarse con nuevas funciones para convertirlas en una amenaza peligrosa y persistente. Los actores de amenazas detrás de Qbot están invirtiendo fuertemente en su desarrollo para permitir el robo de datos a una escala masiva de organizaciones e individuos»*, dijo Yaniv Balmas, de Check Point Research.
>
> *«Hemos visto campañas activas de malspam que distribuyen Qbot directamente, así como el uso de infraestructuras de infección de terceros como la de Emotet para extender la amenaza aún más»*, agregó.

Debido a esto, es necesario tener más precaución al abrir correos electrónicos procedentes de instituciones bancarias, aún siendo legítimos.