Botnet Qakbot,
cada vez más avanzada y peligrosa: Sophos

CIUDAD DE MÉXICO. 10 de marzo de 2022.- Sophos, líder mundial en ciberseguridad de última generación, publicó un análisis técnico profundo sobre la botnet Qakbot, explicando cómo es cada vez más avanzada y peligrosa para las organizaciones.

El informe detalla el funcionamiento de una campaña reciente de Qakbot que muestra cómo la botnet se propaga a través de la vulneración mediante hilos de correo electrónico y recopila una amplia gama de información de las máquinas infectadas, incluidas las cuentas y permisos de usuario configurados, software instalado, servicios en ejecución y más.

Luego, la botnet descarga una serie de módulos maliciosos adicionales en los equipos, que mejoran para generar mayor control en la computadora central de la red infectada, según Sophos.

El código de malware de Qakbot presenta un cifrado no convencional, que también utiliza para ocultar el contenido de sus comunicaciones. Sophos descifró los módulos maliciosos así como el sistema de comando y control de la botnet, para así interpretar cómo es que emite y recibe las instrucciones entre los equipos infectados.

"Qakbot es una botnet modular multipropósito que se propaga por correo electrónico y que se ha vuelto cada vez más popular entre los atacantes como red de entrega de malware, igual que Trickbot y Emotet", dijo Andrew Brandt, investigador principal de amenazas en Sophos.

"El análisis de Sophos revela que la botnet captura una serie de datos detallados del perfil de la víctima, así como su capacidad para procesar secuencias complejas de comandos y una serie de cargas útiles para ampliar la funcionalidad de su 'motor central'. Los días de pensar en los bots como simples robots quedaron atrás", añade.

De acuerdo con Brandt, los equipos de seguridad deben tomarse cada vez más en serio la presencia de infecciones de Qakbot en su red e investigar y eliminar todo rastro. Añade además, que históricamente toda aparición de una botnet es el precursor lógico de un ataque de ransomware.

"Las redes de bots pueden generar ransomware, pero además los desarrolladores de botnets venden su acceso a las redes violadas posteriormente. Por ejemplo, Sophos encontró muestras de Qakbot que entregan balizas Cobalt Strike directamente a un host infectado. Una vez que los operadores de Qakbot han utilizado la computadora infectada, pueden transferir o vender el acceso a estas balizas a los clientes que las paguen", señala.

- **La cadena de infección y las cargas útiles de Qakbot**

Sophos encontró como Qakbot inserta mensajes maliciosos en las conversaciones de correo electrónico de los usuarios de la red. Esos mails incluyen una oración corta y un enlace para descargar un archivo zip que contiene una hoja de cálculo de Excel maliciosa.

Se le pide al usuario que “habilite el contenido” para activar la cadena de infección. Una vez que la botnet infectó un nuevo objetivo, realiza un análisis detallado del perfil, compartir los datos con su servidor de comando y control, para luego descargar módulos maliciosos adicionales.

En el caso hallado por Sophos, la botnet Qakbot descargó al menos tres cargas maliciosas diferentes en forma de bibliotecas de enlaces dinámicos (DLL). Según Sophos, estas cargas útiles de DLL proporcionan a la botnet una gama más amplia de capacidades.

Las cargas útiles se inyectaron en los navegadores y contenían lo siguiente:

- Un módulo que inyecta código para robar contraseñas en páginas web
- Un módulo que realiza escaneos de red, recopilando datos sobre otras máquinas en las proximidades de la computadora infectada
- Un módulo que identificaba las direcciones de una docena de servidores de correo electrónico SMTP (Protocolo simple de transferencia de correo) para luego conectarse a cada uno de ellos y enviar spam.

- **¿Qué recomendamos?**

Sophos recomienda que los usuarios se acerquen a los correos electrónicos inusuales o inesperados con precaución, incluso cuando parecen ser respuestas a conversaciones de correo electrónico existentes. En la campaña de Qakbot investigada por Sophos, una posible señal de alerta para los destinatarios fue el uso de frases en latín en las URL.

Los equipos de seguridad deben verificar que las protecciones de comportamiento proporcionadas por su proveedor de seguridad alerten a los administradores si un usuario infectado intenta conectarse a una dirección o dominio conocido de comando y control.

Los productos para terminales de Sophos, como Intercept X, protegen a los usuarios al detectar las acciones y los comportamientos de los atacantes.

###

Sobre Sophos

Sophos es un líder mundial en ciberseguridad de próxima generación y protege a más de 500.000 organizaciones y millones de consumidores en más de 150 países de las ciberamenazas más avanzadas de la actualidad. Con tecnología de inteligencia de amenazas, inteligencia artificial y aprendizaje

automático de SophosLabs y SophosAI, Sophos ofrece una amplia cartera de productos y servicios avanzados para proteger a los usuarios, las redes y los puntos finales contra ransomware, malware, exploits, phishing y una amplia gama de otros ciberataques. Sophos proporciona una única consola de gestión integrada basada en la nube, Sophos Central, la pieza central de un ecosistema de ciberseguridad adaptable que cuenta con un lago de datos centralizado que aprovecha un amplio conjunto de API abiertas disponibles para clientes, socios, desarrolladores y otros proveedores de ciberseguridad. Sophos vende sus productos y servicios a través de socios revendedores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Hay más información disponible en www.sophos.com

Síguenos en:
Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/