Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

QAKBOT REGRESA EN UN NUEVO ASALTO AL SECTOR DE LA HOTELERÍA

18/ 12 / 2023

CONTENIDO

INTRODUCCIÓN

La reaparición de Qakbot, conocido por su versatilidad en la distribución de malware, plantea nuevas preocupaciones, especialmente para la industria hotelera. A pesar de la exitosa desarticulación temporal de la botnet durante la "Operación Duck Hunt" en agosto, los ciberdelincuentes han demostrado su tenacidad al lanzar una reciente y enfocada campaña de phishing. Este resurgimiento destaca la necesidad apremiante de que las organizaciones refuercen sus estrategias de defensa cibernética. Este informe examina de cerca la última ofensiva de Qakbot, ofreciendo insights sobre sus tácticas y proporcionando recomendaciones esenciales para fortalecer las defensas y preservar la integridad de los sistemas en la siempre cambiante lucha contra las amenazas digitales.

QAKBOT REGRESA EN UN NUEVO ASALTO AL SECTOR DE LA HOTELERÍA

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2023_12_18_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	18/12/2023
Es día cero (0 day):	No

RESUMEN

En un giro inesperado, la botnet Qakbot, previamente desbaratada en la Operación Duck Hunt, ha regresado con una nueva y audaz campaña de phishing. Los analistas de amenazas de Microsoft han identificado recientemente esta resurgencia, que marca el retorno del malware conocido también como Qbot.

Qakbot, originalmente un malware bancario que evolucionó para distribuir ransomware, fue derribado por las autoridades en una operación conjunta internacional en agosto, confiscando servidores y desmantelando su infraestructura. Sin embargo, la interrupción parece ser temporal, ya que los ciberdelincuentes han lanzado una nueva campaña dirigida a la industria hotelera.

La campaña, que comenzó el 11 de diciembre de 2023, se describe como de bajo volumen, pero altamente dirigida. Los objetivos recibieron correos electrónicos con archivos PDF fraudulentos, aparentemente provenientes de empleados del IRS. Estos archivos contenían enlaces que descargaban instaladores de Windows firmados digitalmente, desencadenando la ejecución del malware Qakbot.

Microsoft detalló que la carga útil generada para esta campaña presenta la versión inédita 0x500 del malware, sugiriendo una evolución continua de las tácticas de Qakbot para evadir las medidas de seguridad.

Qakbot, no es ajeno a la adaptabilidad. Tras su caída en agosto, los ciberdelincuentes han demostrado una vez más su habilidad para ajustar sus estrategias y atacar con un enfoque renovado.

Este resurgimiento de Qakbot recuerda al caso de Emotet, otra peligrosa botnet que reapareció después de ser desmantelada. Aunque a un nivel menor, estas amenazas persistentes subrayan la importancia de que las organizaciones refuercen sus defensas contra los correos electrónicos no deseados utilizados en las campañas de Qakbot y similares.

Con la ciberseguridad en el centro de la escena, las organizaciones del sector hotelero deben permanecer alerta y fortalecer sus protocolos de seguridad para evitar caer víctimas de esta nueva ofensiva de Qakbot.

RECOMENDACIONES

- Asegúrese de que todos sus programas y aplicaciones estén actualizados. Los ciberdelincuentes a menudo explotan vulnerabilidades en software desactualizado.
- Utilice un firewall para bloquear todo el tráfico no autorizado hacia y desde tu ordenador.
- Utilice una Red Privada Virtual (VPN) cuando te conectes a redes públicas para asegurar tu conexión a Internet.
- Mantenga un registro de toda la actividad de la red. Esto puede ayudarle a detectar cualquier actividad sospechosa.
- Mantenga actualizados sus programas antivirus para proteger tu sistema contra las últimas amenazas.

- Implemente la autenticación de dos factores siempre que sea posible para añadir una capa adicional de seguridad.
- Evite visitar sitios web no seguros o de reputación dudosa. Utilice la navegación segura en tu navegador para bloquear sitios web maliciosos.
- Realice copias de seguridad periódicas de los datos críticos y almacénelos en ubicaciones seguras e independientes. Esto facilitará la recuperación en caso de un ataque de ransomware.

NOTICIA COMPLETA

https://devel.group/blog/qakbot-regresa-en-un-nuevo-asalto-al-sector-de-la-hosteleria/

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20231219_01_QaBotRansomware

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente