Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°278	Fecha: 21-11-2023
		Página: 4 de 9

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Phishing con tácticas de Qakbot distribuye malware Darkgate y Pikabot		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Se ha detectado una campaña de phishing de gran volumen que entrega malware DarkGate y PikaBot. La campaña está dirigida a una amplia gama de sectores y utiliza las mismas tácticas que se utilizaron anteriormente en los ataques que aprovechaban el troyano QakBot.

2. DETALLES:

Los correos electrónicos de phishing de la campaña contienen una URL trampa que apunta a un archivo ZIP. El archivo ZIP contiene un gotero de JavaScript que, a su vez, se pone en contacto con una segunda URL para descargar y ejecutar el malware DarkGate o PikaBot.

Se ha observado una variante notable de los ataques aprovechando archivos de complementos de Excel (XLL) en lugar de los cuentagotas de JavaScript para entregar las cargas útiles finales.

Los actores de la amenaza utilizan hilos de correo electrónico secuestrados para entregar el malware. Estos hilos de correo electrónico son legítimos, pero han sido alterados por los actores de la amenaza para incluir un enlace malicioso.

Los actores de la amenaza también utilizan técnicas de ingeniería social para hacer que los correos electrónicos de phishing sean más convincentes. Por ejemplo, pueden personalizar los correos electrónicos para que se ajusten a los intereses o la ubicación del destinatario.

Las familias de malware DarkGate y PikaBot son avanzadas y pueden entregar una amplia gama de cargas útiles maliciosas. Estas cargas útiles incluyen:

- Minería de criptomonedas: El malware puede usarse para minar criptomonedas en el dispositivo infectado.
- Robo de credenciales: El malware puede robar credenciales de cuentas, como nombres de usuario y contraseñas.
- Ransomware: El malware puede cifrar los datos del dispositivo infectado y exigir un rescate para desbloquearlos.
- Acceso remoto: El malware puede permitir que los atacantes accedan de forma remota al dispositivo infectado.

Una infección exitosa de DarkGate o PikaBot podría llevar a la entrega de software avanzado de minería criptográfica, herramientas de reconocimiento, ransomware o cualquier otro archivo malicioso que los agentes de la amenaza deseen instalar en la máquina de una víctima.

3. RECOMENDACIONES:

- Verificar detalladamente las URLs que correspondan a sitios web oficiales.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Instalar y mantener actualizados los últimos parches de seguridad de su software.
- Utilizar una solución antivirus licenciada con protección en tiempo real y que te permita eliminar troyanos.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• hxxps://widefense.com/observatorio-de-amenazas/phishing-con-tacticas-de-qakbot-distribuye-malware