	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°094	Fecha: 22-04-2024
		Página: 5 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Nuevo ataque de phishing elude todas las detecciones del software de antivirus		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. **ANTECEDENTES:**

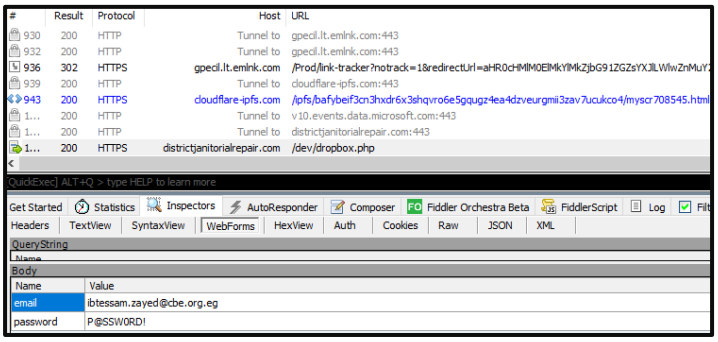
El investigador de ciberseguridad "@doc_guard", ha descubierto un nuevo ataque de phishing que ha evade todas las detecciones del software de antivirus. En esta campaña, los atacantes imitan el panel de inicio de sesión de Outlook que engaña con éxito a sus víctimas para que revelen sus credenciales de inicio de sesión.

2. **DETALLES:**

Investigadores de ciberseguridad han descubierto un nuevo ataque de phishing que ha eludido todas las detecciones de los antivirus. En esta campaña, la página de phishing está diseñada para parecerse exactamente al panel de inicio de sesión de Outlook, con la marca Microsoft y una interfaz de usuario familiar.

La página de phishing está alojada en un dominio diseñado para parecerse mucho a una URL legítima de Microsoft, lo que dificulta que los usuarios detecten la intención maliciosa. La página es casi auténtica a la oficial, lo que hace que sea extremadamente difícil para los usuarios identificarla como una estafa.

Además, está equipada con técnicas avanzadas de ofuscación, que la ayudan a evadir todas las detecciones del software antivirus.



Indicadores de compromiso:

- Nombre de archivo HTML: Nota del personal del departamento de recursos humanos.htm.
- MD5: e1f5cdbac6db809cb06fe0279f2c7594.
- SHA256: 1123395beb29a3715550cb165fb095694ef806e1c30968870d7450ca3e7a9f4d.
- URL: https[:]//districtjanitorialrepair.com/dev/dropbox.php–https[:]//cloudflare-ipfs.com/ipfs/bafybeif3cn3hxdr6 x3shqvro6e5gqugz4ea4dzveurgmii3zav7ucukco4/myscr708545.html.

3. **RECOMENDACIONES:**

- Concientizar a los empleados sobre los riesgos del phishing mediante sesiones de formación en seguridad y mantenerse al tanto de las últimas tácticas de phishing.
- Estar atento y desconfiar de correos electrónicos, mensajes o llamadas sospechosas que soliciten información confidencial.
- Utilizar contraseñas robustas y la autenticación de dos factores para proteger las cuentas de posibles ataques.
- Establecer políticas de seguridad, filtros antispam y antivirus, mantener sistemas actualizados, y realizar auditorías de seguridad periódicas son medidas esenciales para proteger a las empresas de ataques de phishing.

Fuente de Información:	• hxxps://gbhackers.com/outlook-login-panel/ • hxxps://twitter.com/doc_guard/status/1780232141332176984/photo/2