	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 063	Fecha: 04-03-2022
		Página 8 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**			
Nombre de la alerta	Nueva campaña de phishing que suplanta las identidades de “Outlook Web App”			
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 subfamilia	G02	
Clasificación temática familia	Fraude			

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de phishing dirigidos a usuarios del correo electrónico “Outlook Web App”, con el objetivo robar credenciales de inicio de sesión y contraseña.

2. Proceso del ataque phishing:

Imagen 01: Sitio web que simula ser el oficial de “Outlook Web App”, solicita a la víctima, ingresar sus credenciales de acceso (usuario y contraseña).

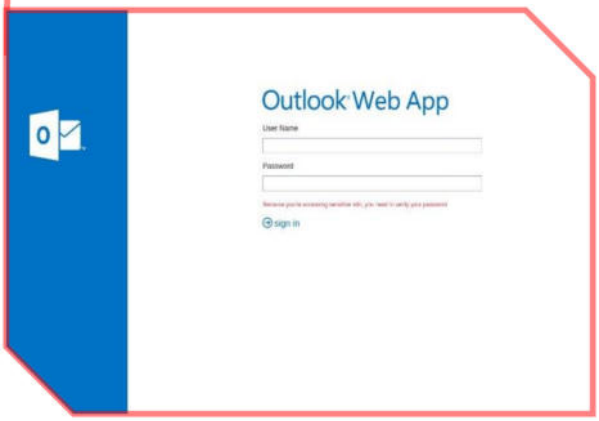


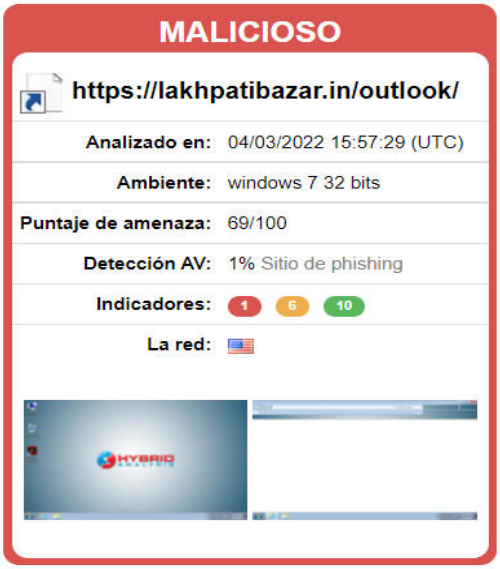
Imagen 02: Una vez hecho clic en <Iniciar sesión>, es redirigido al sitio web oficial de “Outlook”, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados por los ciberdelincuentes.

3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado lo siguiente:
   - Indicadores de compromiso:
     - URL: hXXps[:]//lakhpatibazar[.]in/outlook/
     - Dominio: lakhpatibazar[.]in
     - Dirección IP: 162[.]241[.]123[.]75
     - Código: 200
     - Tamaño: 22.12KB
     - SHA-256: 54d9d4782e3e3118fed8ab938252adeff76b6e6e68c175046caf9fcc7f659e81

- Lista negra / IP: 162[.]241[.]123[.]75

4. Otras detecciones:

- URL: hXXps[:]//lakhpatibazar[.]in/outlook/



5. Cómo funciona el phishing:

- Los ciberdelincuentes a través de los correos electrónicos, adjuntan enlaces que redirige a sitios webs fraudulentos en los que solicitan información personal.
- Los ciberdelincuentes utilizan como medios de propagación del Phishing: WhatsApp, telegram, redes sociales, SMS entre otros.
- Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público, entidad financiera, servicio técnico, etc.).

6. Referencia:

- Phishing o suplantación de identidad: Es una técnica fraudulenta consiste en engañar al usuario solicitando información personal, contraseñas, datos bancarios etc., a través del correo electrónico o redirigiendo a la víctima a una copia falsa de una página web donde se le solicita el ingreso de los datos que se quieren obtener.

7. Recomendaciones:

- Evitar abrir correos de usuarios desconocidos o que no hayas solicitado, elimínalos directamente.
- No brindar información personal a sitios web de dudosa procedencia.
- Escribir directamente la URL de la entidad en el navegador, en lugar de llegar a ella a través de enlaces disponibles desde páginas de terceros o en correos electrónicos.
- Contar con una solución de seguridad, constantemente actualizada tanto en dispositivos de escritorio como en móviles, ya que sirven como barrera inicial protectora ante sitios web maliciosos.

Fuentes de información	Análisis propio de redes sociales y fuente abierta