

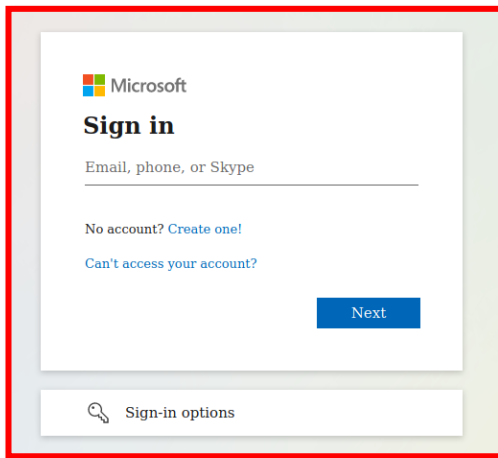
	<b>ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°302</b>		<b>Fecha: 20-12-2023</b>
			<b>Página: 8 de 11</b>
Componente que reporta	<b>DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ</b>		
Nombre de la alerta	Detección de una nueva campaña de Phishing a Microsoft Office 365		
Tipo de Ataque	Phishing	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**

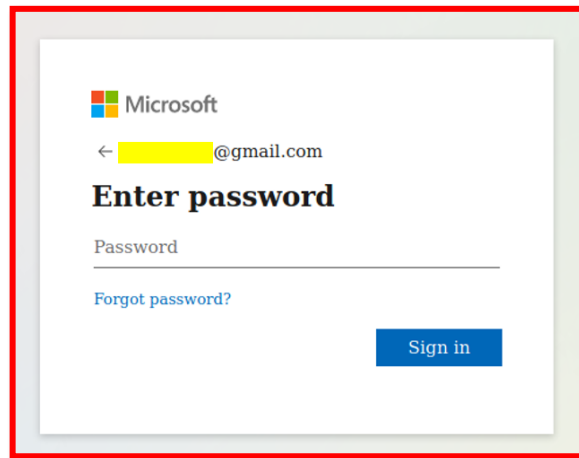
**1. ANTECEDENTES:**

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes se encuentran desarrollando una nueva campaña de Phishing, activando un sitio web fraudulento suplantando la identidad de la compañía Microsoft Office 365, con la finalidad de robar las credenciales de acceso (usuarios y contraseñas) de los clientes de la compañía.

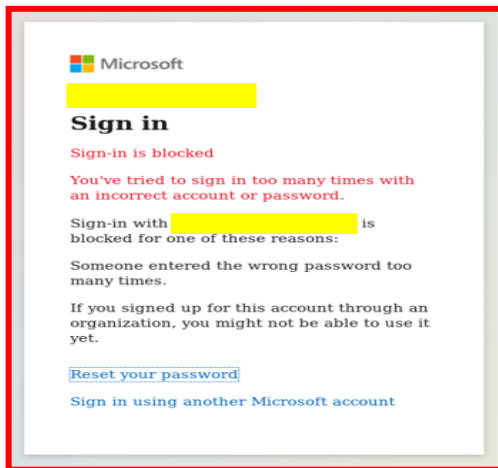
**2. DETALLES:**



**Imagen 1:**  
Solicita ingresar su usuario (e-mail) para su inicio de sesión.



**Imagen 2:**  
Solicita ingresar el password (contraseña) para dar inicio a Microsoft Office 365



**Imagen 3:**  
Una vez ingresada el e-mail y contraseña, redirige a un mensaje en la que indica que la cuenta se encuentra bloqueada; dando por concluida la estafa.

A. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

a) **Indicadores de compromisos:**

I. **URL:** <https://www.sharession.com/gbr/4d30a371-55bc-4888-8f4c-306b4971bd39/209e3e84-5de1-48b6-902f-80233098d5d8/e90cd5b6-7b8d-4a7d-8d28-5f1bf5d88f6d...>



Nombre de envío: <https://www.sharession.com/gbr/4d30a371-55bc-4888-8f4c-306b4971bd39/209e3e84-5de1-48b6-902f-80233098d5d8/e90cd5b6-7b8d-4a7d-8d28-5f1bf5d88f6d.../login?id=MktleVhBZZVbjhRbWxkWCtnWW9vWHU7HFzBEI2Q3AzSujmdWVmRnFpdTZYIZ3NUIWFFrN0UONWVzdZDTVZJMujOVbXMXk3WDBCVGNvQThjSFVjSlivdVMxK1kyNStiTAwZGItb0NmbERINmpBbHFRVFIK2U5YnBidUOwZ3NjOjJSUS9LcnBklFhSnLOS2Vnd2cwKOZzNDg4QWY1MXhvbGVIMDUwK1NHNmUjS0kjScGVONmR5RGpkLlhGdXdDSUpVRC9GSmdNTjJLNWIPVnjFdlWISN3dFSZRLNVY4OUdtUHZUc0IzN2sxaDRVeUJZSEVOD2hwbmcsNI1BdlpLU3UyWlVsOTRLWUpER3FKrmjMMENVOVhobEpKNkpbzRydZlMdlhYWtGROxCMXlRnRlqRFXIVG53NHE1aOR6OTcxWxCd2oxc2pnMk9VNVp5W5Gc3T1dTYlZTBoNldSRUlthjQNVFRkQwVWwS4MOUrOWg4Q3ZadmRDZDF1>

Tamaño: 687B

Tipo: URL

Mimica: Texto sin formato

Sistema operativo: ventanas

Último análisis antivirus: 18/08/2023 19:04:04 (UTC)

Último informe de Sandbox: 18/08/2023 19:03:31 (UTC)

II. **SHA-256:** 338f6cf04e8d26f138151214e8862accea803adf09afb950952abeb6b338b80e



uriref\_ <https://www.sharession.com/gbr/4d30a371-55bc-4888-8f4c-306b4971bd39/209e3e84-5de1-48b6-902f-80233098d5d8/e90cd5b6-7b8d-4a7d-8d28-5f1bf5> 338f6cf04e8d26f138151214e8862accea803adf09afb950952abeb6b338b80e ninguna amenaza específica

III. **IP:** 13[.]107[.]213[.]38

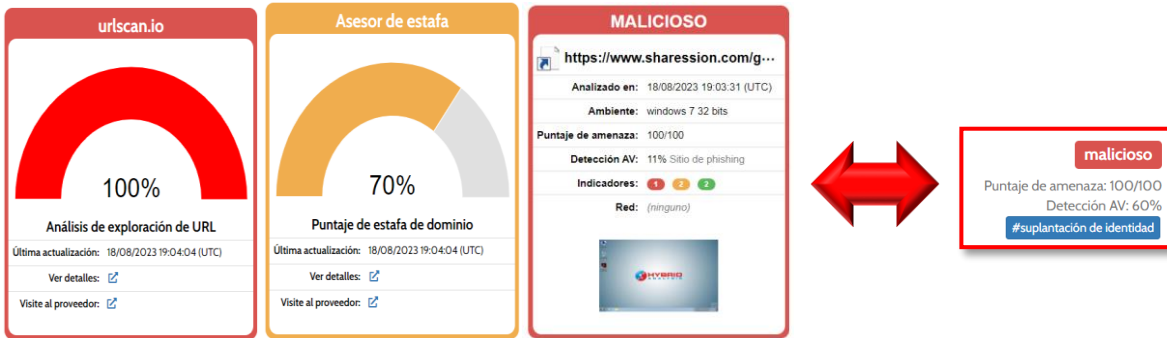


Connection		Detection	
Representative Domain	N/A	Proxy IP	False
SSL Certificate	<span style="color: red;">!</span> True (*.azureedge.net)	VPN IP	False
IP Address Owner	MICROSOFT-CORP-MSN-AS-BL...	Tor IP	False
Hostname	N/A	Hosting IP	<span style="color: red;">!</span> True
Connected Domains	<span style="color: red;">!</span> 129	Mobile IP	False
Country	United States	CDN IP	False
		Scanner IP	False
		Special Issue	0

B. Se hallaron **10 proveedores** de seguridad que marcaron este dominio como malicioso.

Antiy-AVL	<span style="color: red;">!</span> Malicious	Avira	<span style="color: red;">!</span> Phishing
BitDefender	<span style="color: red;">!</span> Phishing	Emsisoft	<span style="color: red;">!</span> Phishing
Kaspersky	<span style="color: red;">!</span> Phishing	Lionic	<span style="color: red;">!</span> Malicious
Seclookup	<span style="color: red;">!</span> Malicious	SOCradar	<span style="color: red;">!</span> Phishing
Trustwave	<span style="color: red;">!</span> Phishing	Webroot	<span style="color: red;">!</span> Malicious

### C. Otras detecciones:



### D. Cómo funciona el Phishing:

- Los correos electrónicos incluyen enlaces a sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
- Medios de propagación del Phishing: WhatsApp, telegram, redes sociales, SMS entre otros.
- Los ciberdelincuentes intentan suplantar a una entidad legítima (organismo público o privado, entidad financiera, servicio técnico, etc.).

### E. Referencia:

- Phishing o suplantación de identidad: Es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.

### F. Microsoft Office 365

- Se trata de una herramienta que permite crear, acceder y compartir documentos de Word, Excel, OneNote y PowerPoint. En este sentido presenta cambios con un paquete Office normal, pero la diferencia está en que puede acceder a todos los programas en tiempo real. Además, puede acceder desde cualquier dispositivo que tenga acceso a Internet y OneDrive.

## 3. RECOMENDACIONES:

- Mantener instalado un servicio de antivirus en el dispositivo.
- Verificar la información del sitio web correspondiente.
- Acceder al sitio web a través de fuentes oficiales.
- No abrir enlaces de dudosa procedencia.
- No seguir indicaciones de sitios web fraudulentos.
- No compartir la información con terceras personas, amigos o familiares.

Fuente de Información:

Análisis propio de redes sociales y fuente abierta.