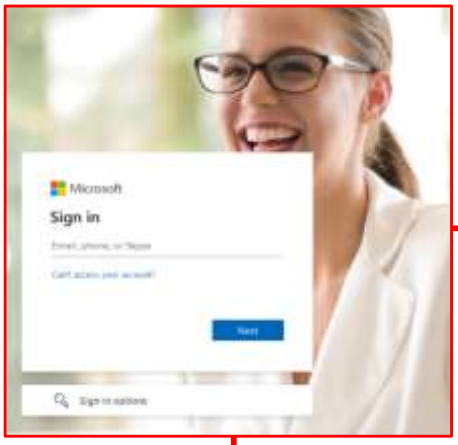
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 138	**Fecha: 13-06-2023**
		Página 28 de 32

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección Fraudulententa del servicio de correo electrónico Microsoft		
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

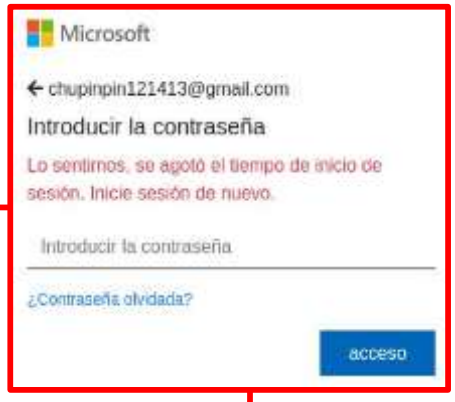
1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que actores de amenazas vienen realizando una campaña de Phishing, activando un falso servicio del correo electrónico de la compañía Microsoft (Outlook, Hotmail, etc.), con la finalidad de obtener las credenciales de acceso (correos y contraseñas) de los usuarios de la compañía tecnológica.

2. **Detalles del proceso de Phishing:**



Paso N.º 01

En sitio web fraudulento de Microsoft, el atacante solicita a la víctima que registre el correo electrónico, el número de teléfono o de Skype, para acceder al servicio en la web de la compañía Microsoft (Outlook, Hotmail, etc.)



Paso N.º 02

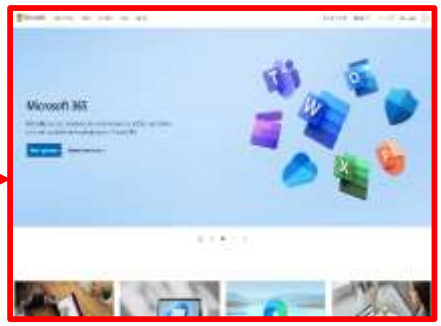
Una vez registrado el usuario y contraseña hecho clic en <Iniciar sesión>, requiere ingresar la contraseña para continuar con el acceso.

Paso N.º 03

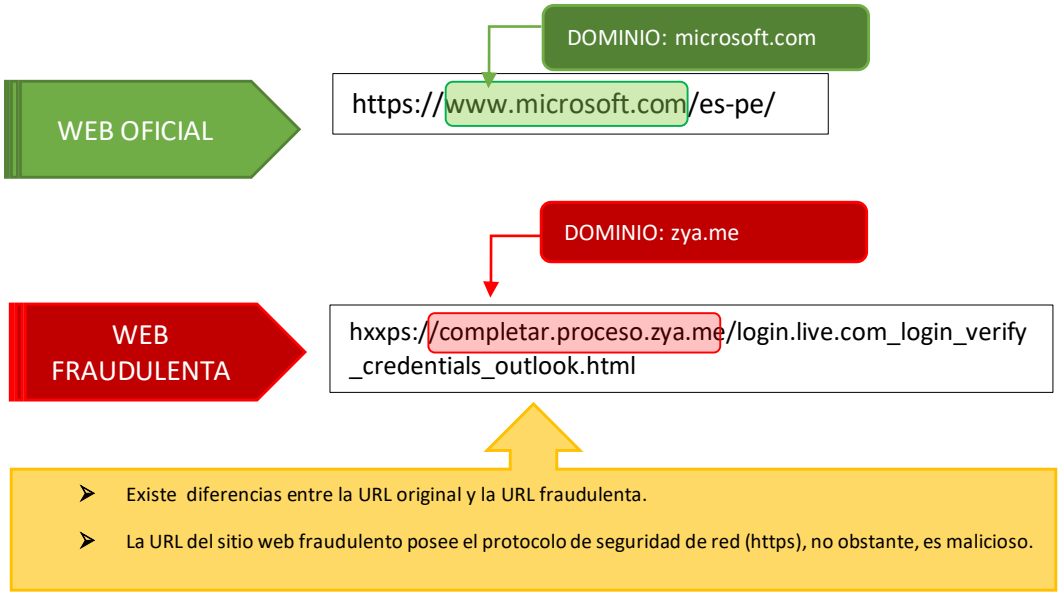
Luego de completar las credenciales de acceso y darle clic en <Acceso> se muestra un aviso que la cuenta ha sido verificada y actualizada.

Paso N.º 04

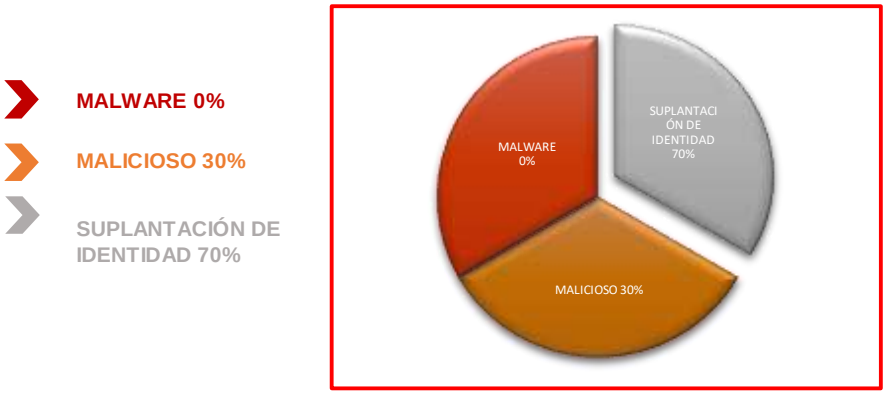
Al esperar unos 3 segundos, automáticamente es redirigido al sitio oficial de Microsoft, sin embargo, los datos ya fueron capturados.



3. **Comparación del sitio web oficial y fraudulento.**



4. **Proveedores de seguridad informática alertan como VULNERACIONES. - PHISHING.**



alphaMountain.ai	Suplantación de identidad	Anti-AVL	Malicioso
Avira	Suplantación de identidad	CRDF	Malicioso
CyRadar	Malicioso	Emsisoft	Suplantación de identidad
kaspersky	Suplantación de identidad	Leonico	Suplantación de identidad
netcraft	Malicioso	Búsqueda segura	Malicioso
Sophos	Suplantación de identidad	Inteligencia de amenazas de Viettel	Suplantación de identidad
raíz web	Malicioso	Navegación segura de Yandex	Suplantación de identidad

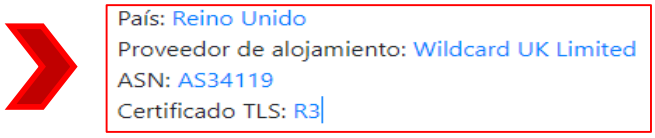
5. **Indicadores de compromiso (IoC)**

a) URL: hxxp://completar[.]proceso[.]zya[.]me/login[.]live[.]com_login_verify_credentials_outlook.html

b) Dominio : zya[.]me

c) IP : 82[.]163[.]176[.]104

d) Proveedor de alojamiento : Wildcard UK Limited



6. **Otras detecciones:**

7. **Apreciación de la información:**

   a) La presente campaña de Phishing permite a los actores de amenazas obtener las credenciales de acceso del servicio del correo electrónico en la web de la compañía Microsoft (Outlook, Hotmail, etc.).

   b) La propagación del sitio web fraudulento se realiza mediante envió masivos de email, adjuntando enlaces de sitios web fraudulentos con la finalidad de obtener información sensible de las víctimas; asimismo, dicho enlace malicioso, es enviado a través de las plataformas digitales como el WhatsApp, Telegram, Messenger y mensajes de textos SMS.

8. **Concepto de MICROSOFT:**

   a) Es una compañía que ofrece programas y soluciones ofimáticas, que favorecen las áreas profesionales, estudiantiles y domésticas. Por lo que una cuenta de Microsoft es una dirección de correo electrónico y una contraseña que usa con Outlook.com, Hotmail, Office, OneDrive, Skype, Xbox y Windows. Si crea una cuenta de Microsoft, puede usar cualquier dirección de correo como el nombre de usuario, incluidas las direcciones de Outlook.com, Yahoo! o Gmail.

9. **Algunas Recomendaciones:**

   a) Verificar detalladamente las URL de los sitios web

   b) No abrir o descargar archivos sospechosos.

   c) No seguir las instrucciones de sitio web sospechoso.

   d) Mantener el antivirus actualizado.

   e) Descargar aplicaciones de fuentes confiables.

   f) Realizar las actualizaciones correspondientes desde fuentes originales.

Fuentes de información	Análisis propio de redes sociales y fuente abierta