	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°160	Fecha: 07-07-2023
		Página: 24 de 27

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de falso servicio del correo electrónico de 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 Sub familia	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:**

El proceso del Phishing es el siguiente:

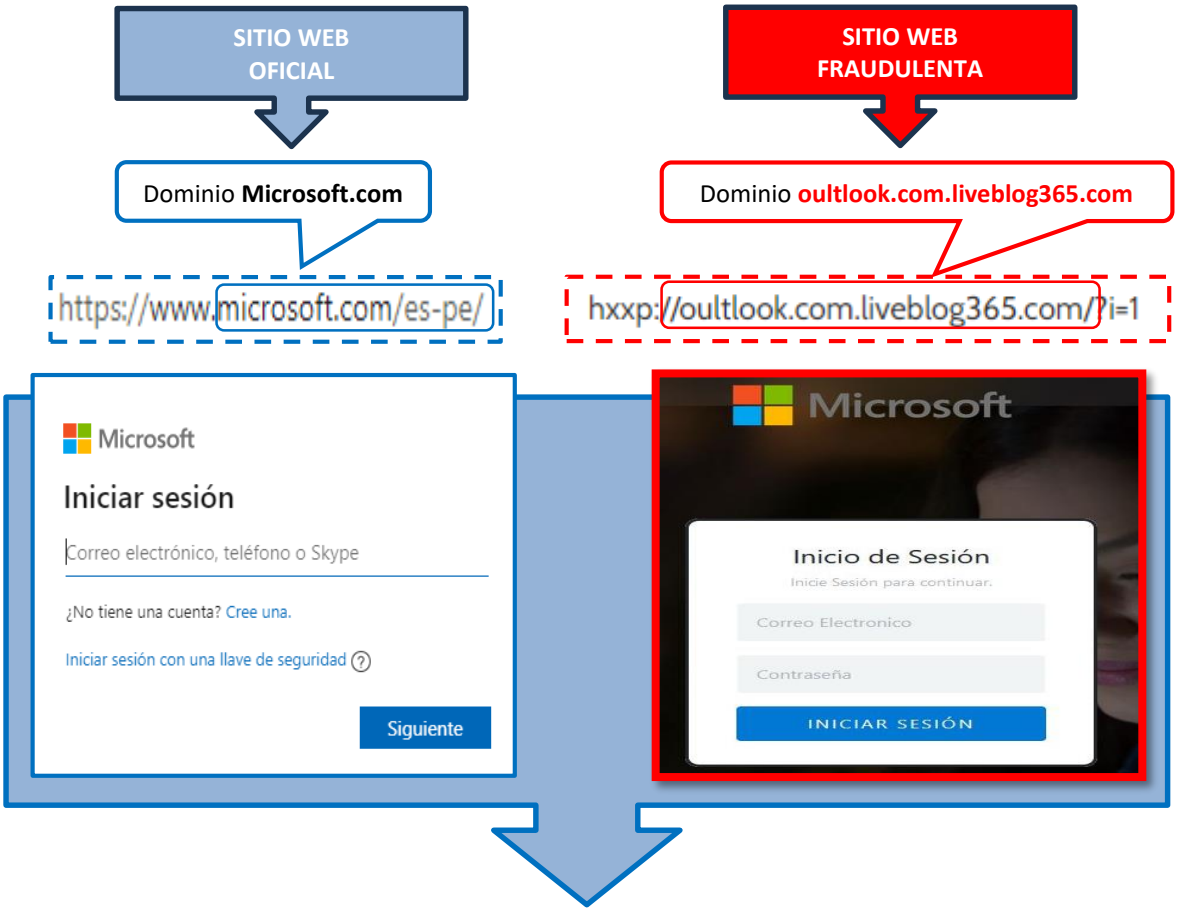
Paso N.º 01

Sitio web fraudulento solicita a la víctima registrar el correo electrónico, teléfono o Skype, para acceder al servicio en la web de la compañía Microsoft (Outlook, Hotmail, etc.)

Paso N.º 03

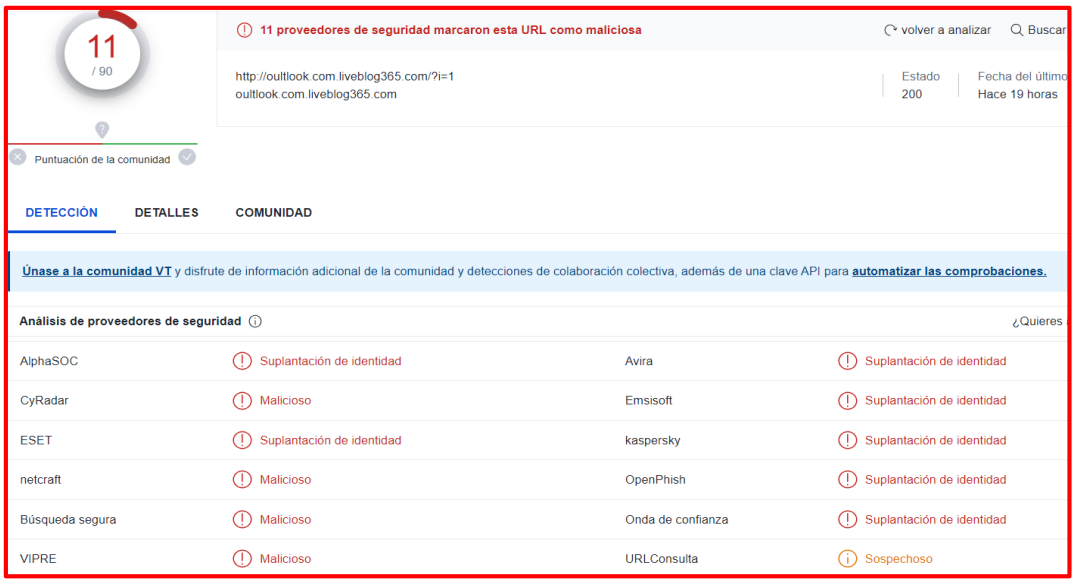
Por último, le pide a la víctima cambiar el PIN, luego de registrar lo requerido por el atacante le redirige al servicio del correo electrónico de la compañía Microsoft oficial aparentando un error de autenticación, sin embargo, los datos fueron capturados por los cibercriminales.

A. Comparación del sitio web oficial y fraudulento.



- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento no posee el protocolo de seguridad de red (https)
- Existe una similitud entre ambas páginas en imagen, fondo y color.

B. Proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD - PHISHING.



C. Indicadores de compromiso (IoC)

- Dominio : liveblog365.com

Dominio	liveblog365.com
Nombre del servidor	ns1.liveblog365.com
registrador de dominio	nombrebarato.com
Organización del servidor de nombres	whois.namecheap.com

- IP : 185[.]27[.]134[.]60

Dirección IPv4 (185.27.134.60)

rango de IP	País	Nombre	Descripción
::ffff:0.0.0.0/96	Estados Unidos	IANA-IPV4-DIRECCIÓN ASIGNADA	Autoridad de asignación de números de Internet
↳ 185.0.0.0-185.255.255.255	Países Bajos	MADURO-185	Centro de Coordinación de la Red RIPE
↳ 185.27.132.0-185.27.135.255	Reino Unido	Reino Unido-IFASTNET-20130530	I FastNet LTD
↳ 185.27.134.60	Reino Unido	Reino Unido-IFASTNET-20130530	I FastNet LTD

- Servidor : nginx
- SHA-256 : ddcdf8fc4af83fe489e0bec719b5847ccf5128f21aea9157280e896778e0d892

D. Otras detecciones:

E. Apreciación de la información:

- 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.).
- 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, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram, Messenger, etc. y mensajes de textos SMS.

3. RECOMENDACIONES:

- Verificar detalladamente las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- No aceptar permisos de instalación de archivos desconocidos o dudosa procedencia.
- Mantener actualizado el sistema operativo y aplicaciones del equipo de cómputo.
- Mantener actualizado el sistema antivirus (el antivirus debe ser licenciado).
- Comunicar a la entidad financiera si ha realizado un registro de acceso en un sitio web sospechoso.

Fuente de Información:	Análisis propio de redes sociales y fuente abierta