	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 145	Fecha: 30-05-2022
		Página 9 de 11

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 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***

Solicita el correo electrónico de la víctima, para acceder al servicio en la web de la compañía Microsoft (Outlook, Hotmail, etc.)

Requieren la contraseña de acceso para el servicio web de Microsoft, para luego dar clic en <Registrarse>; sin embargo, después de unos segundos redirige al sitio web oficial de Microsoft.

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

SITIO WEB OFICIAL

https://login.live.com/login.srf

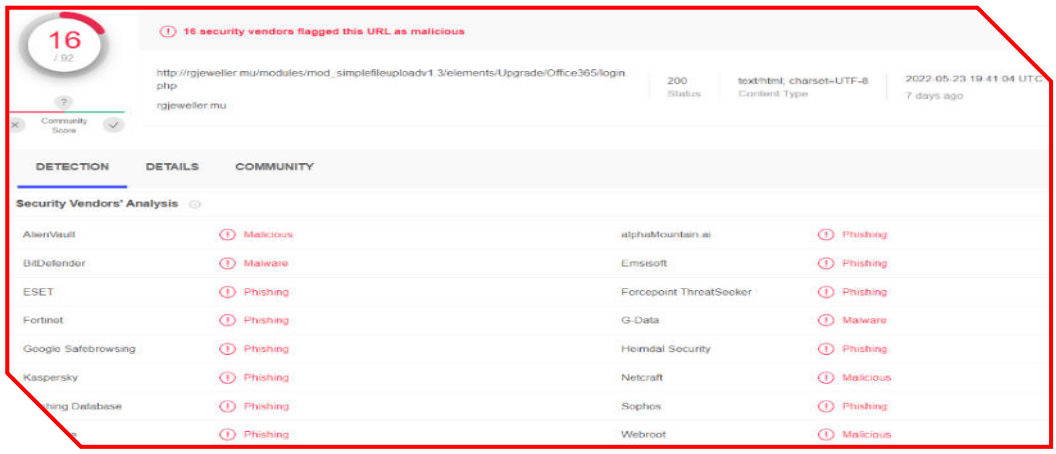
SITIO WEB SOSPECHOSA

hxxp://rgjeweller[.]mu/modules/mod_simplefileuploadv1[.]3/elements/Upgrade/Office365/login[.]php

- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento ***NO POSEE PROTOCOLO DE SEGURIDAD DE RED (HTTP)***

hxxp://rgjeweller[.]mu/modules/mod_simplefileuploadv1[.]3/elements/Upgrade/Office365/login[.]php/

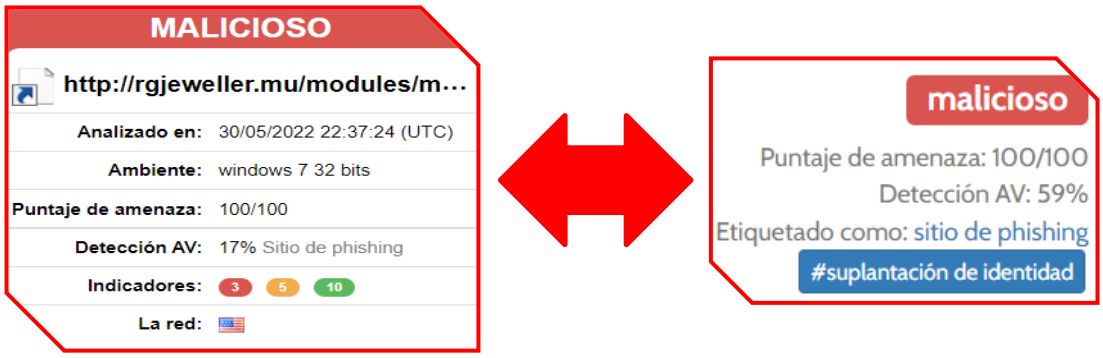
4. ***Proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD - PHISHING.***



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

- ✓ URL : hxxp://rgjeweller[.]mu/modules/mod_simplefileuploadv1[.]3/elements/Upgrade/Office365/login[.]php/
- ✓ Dominio : rgjeweller[.]mu
- ✓ SHA-256 : 1d4638ca4049f377b955c200ae3dd7c7abf17f16bcdec330ebaaf5630679cafc
- ✓ IP : 23[.]235[.]193[.]45

6. ***Otras detecciones:***



7. ***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.).
- El medio de propagación del sitio web fraudulento es a través de los correos electrónicos, donde ciberdelincuentes adjuntan enlaces de sitios web preparados con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram, Messenger y mensajes de textos SMS.

8. ***Algunas Recomendaciones***:

- Verificar detalladamente las URL de los sitios web
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.
- Descargar aplicaciones de fuentes confiables.
- Realizar las actualizaciones correspondientes desde fuentes originales.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta