| | | |
|---|---|---|
| | **ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 285** | **Fecha: 20-10-2022** |
| | | **Página 07 de 10** |

| | | | |
|---|---|---|---|
| Componente que reporta | **DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ** | | |
| Nombre de la alerta | Campaña de phishing que tiene como objetivo robar credenciales de acceso de cuentas de Yahoo! | | |
| 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 actores de amenazas vienen llevando a cabo una campaña de phishing "tipo de robo de identidad en línea", que utilizando correos electrónicos falsos afirma ser enviado por la empresa "Yahoo!" para atraer la atención de la víctima, en el texto del mensaje se advierte que se ha detectado una actividad de acceso inusual, por lo que será cancelada a menos que se ingrese en el enlace que se adjunta, con el objetivo robar los datos personales (la contraseña de la cuenta).

2. Proceso del ataque phishing:

**Imagen 1:** Mensaje de correo electrónico enviado supuestamente de "Yahoo!" incita a la víctima, hacer << Click para continuar>>.

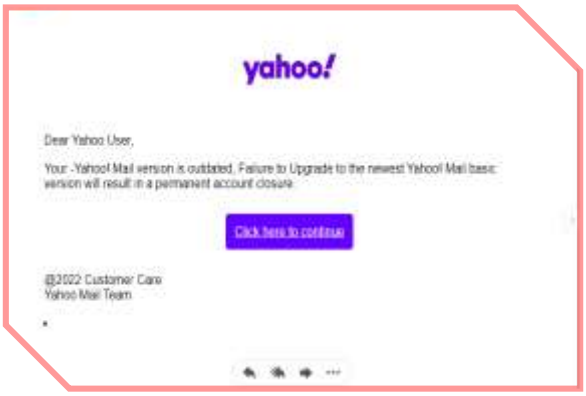
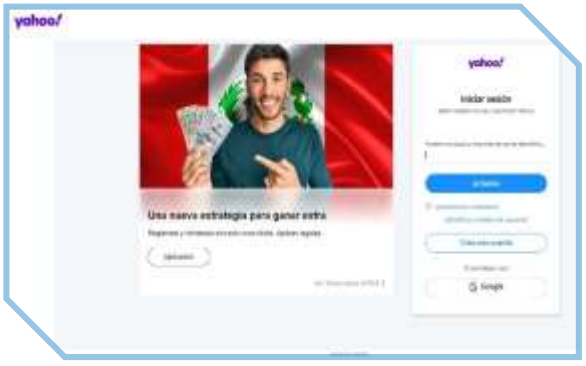



**Imagen 2:** Engaño, solicitud para ingresar nombre de usuario, correo electrónico o móvil.


**Imagen 3:** Solicitud para ingresar la contraseña.


**Imagen 4:** Que, al ingresar la contraseña, es redirigido al sitio oficial de Yahoo! aludiendo un aparente error; sin embargo, los datos fueron capturados por los ciberdelincuentes.



**3.** Comparación de sitio oficial y sitio falso:

**SITIO OFICIAL**
**URL:** https://login.yahoo.com/

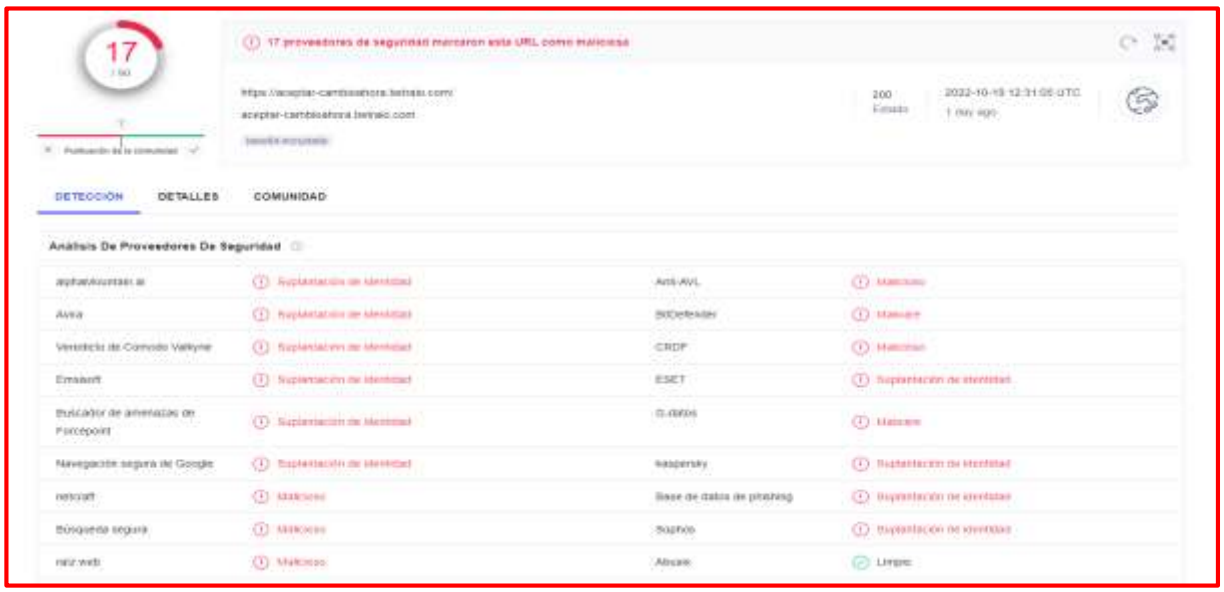
**SITIO FRAUDULENTO**
**URL:** hxxps://accept-changenow[.]betraio[.]com/



- Existe similitud en imagen de fondo, color y escritura.
- Tiene certificado de seguridad de protocolo HTTPS.
- El dominio se hace pasar por el sitio oficial, pero no coincide.

**4.** La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo la siguiente información:

- **URL:** hxxps[:]//accept-changenow[.]betraio[.]com/
- **Dominio:** accept-changenow[.]betraio[.]com
- **Direcciones IP:** 162[.]241[.]60[.]218
- **Código De Estado:** 200
- **Tamaño:** 16.69 KB
- **SHA-256:** eb59f0ad0830031efaf3a107548de6cbd9ed5f226c3a895555389ceacf7e463d



5. **Otras detecciones del análisis**:



6. **Recomendaciones:**

- Acceder al sitio web a través de fuentes oficiales
- Evitar responder a mensajes enviados desde (correo electrónico, Whatsapp, SMS y otros), que contengan enlaces de dudosa procedencia.
- Verificar detenidamente la redacción y ortografía de la dirección URL, que coincidan con el sitio web oficial.
- Evitar proporcionar información personal y/o financiera a través de sitios webs de dudosa procedencia.
- Utilizar una firma de antivirus actualizado, ya que es la primera barrera ante posibles ataques cibernéticos.

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