| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°185 | Fecha: 08-08-2023 |
|---|---|---|
| | | Página: 6 de 9 |

| | | | |
|---|---|---|---|
| Componente que reporta | **DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ** | | |
| Nombre de la alerta | Phishing, suplantando la identidad del Banco Scotiabank | | |
| 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 vienen llevando a cabo una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad del Banco Scotiabank (entidad bancaria), con la finalidad de robar información sensible, como datos personales (nombre, fecha de nacimiento, e-mail, claves, números de cuentas de tarjetas de crédito o débito) fingiendo y/o aparentando ser de la entidad bancaria.

## 2. DETALLES:


**Imagen 1:**
Sitio web fraudulento; donde se solicita **CONTINUAR.**


**Imagen 2:**
Solicita validar datos (DNI, contraseña).

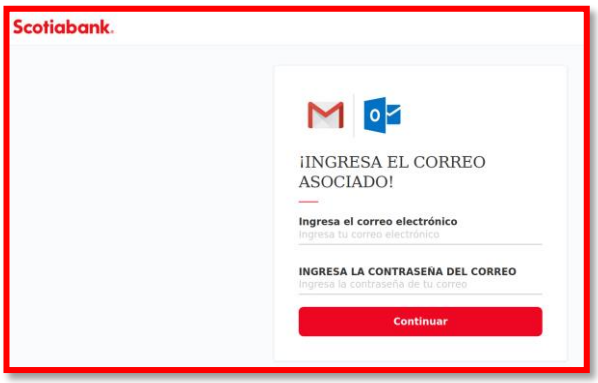



**Imagen 3:**
Solicita ingresar datos del correo asociado.

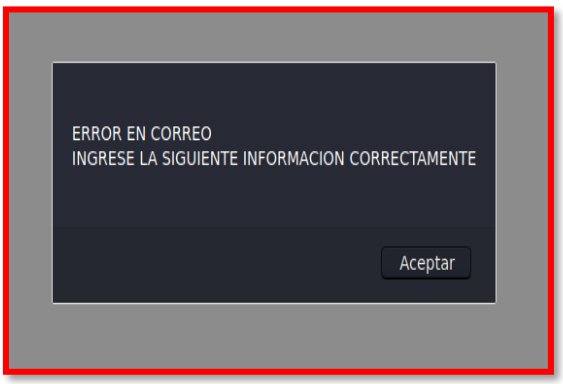



**Imagen 4:**
Redirecciona un mensaje indicando "un error en el correo"; dando así por concluida la estafa.

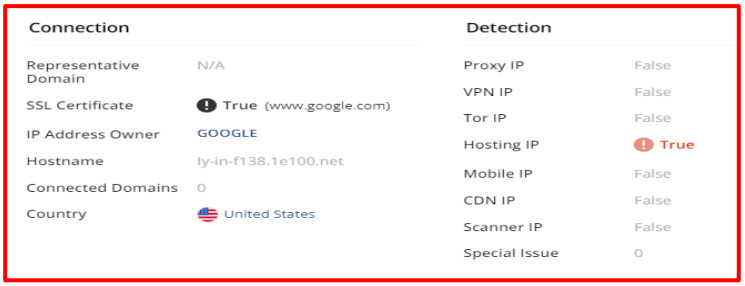
**A.** La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

**Indicadores de compromisos:**

**I. URL:** hxxps[:]//sites[.]google[.]com/view/enlinea294032/p%C3%A1gina-principal/


**II. SHA-256:** d9837967450c001f0b6eae007faacbd3faa07af8cd16c37904204864a35d2af0

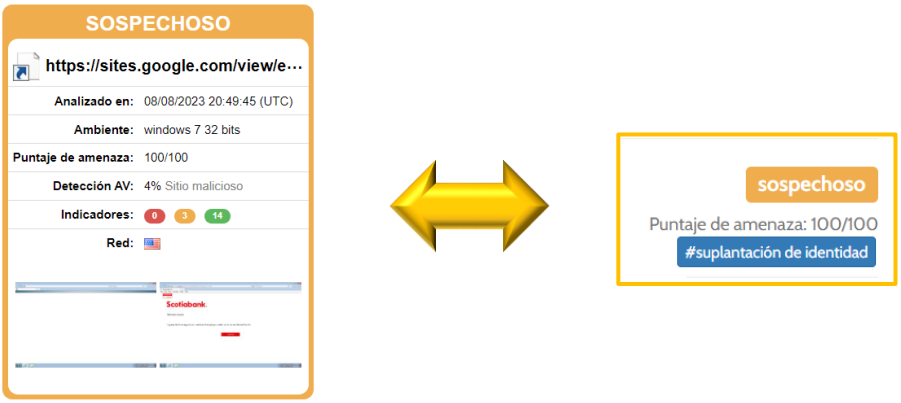

**III. IP:** 173[.]194[.]197[.]138




**B.** Se hallaron **04 proveedores** de seguridad que marcaron este dominio como malicioso.

| | | | |
|---|---|---|---|
| CyRadar | Malicious | ESET | Phishing |
| Quttera | Malicious | VIPRE | 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 legitima (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.

**3. RECOMENDACIONES:**

- Evitar acceder a enlaces que llegan inesperadamente por correo electrónico u otros medios.
- No proporcionar datos personales (contraseñas, tarjetas, cuentas bancarias, etc.) por correo, teléfono o SMS.
- No introducir datos confidenciales en sitios web sospechosas o de dudosa procedencia.
- Verificar la fuente de información de tus correos entrantes.
- Introduce tus datos únicamente en webs seguras.
- Tener siempre actualizado el sistema operativo y el antivirus. En el caso del antivirus, comprobar que está activo.

| | |
|---|---|
| Fuente de Información: | Análisis propio de redes sociales y fuente abierta. |