| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 130 | Fecha: 03-06-2023 |
|---|---|---|
| | | Página 9 de 27 |

| | | | |
|---|---|---|---|
| Componente que reporta | **DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ** | | |
| Nombre de la alerta | Suplantación de la identidad de la empresa de servicios multimedia Spotify | | |
| 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 | | |

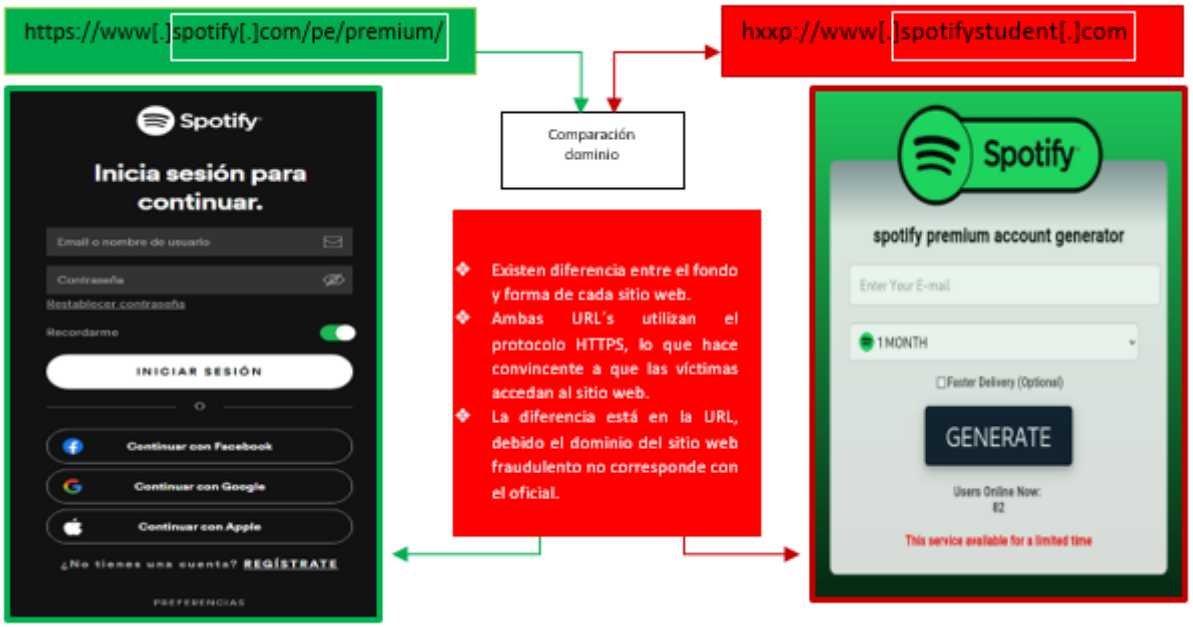
Descripción

1. Mediante el monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, ciberdelincuentes vienen llevando a cabo una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad de la empresa de servicios multimedia Spotify (servicio de música, pódcasts y vídeos digitales que te da acceso a millones de canciones y a otro contenido de creadores de todo el mundo), el cual tiene como finalidad robar información confidencial y bancaria de las posibles víctimas como número de tarjeta, fecha de vencimiento, código de seguridad, entre otros.

   a) Detalles del proceso de Phishing.



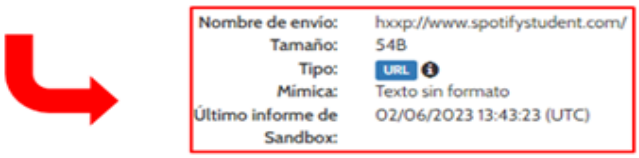

2. La Comparación del sitio web oficial y el sitio web fraudulente.




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

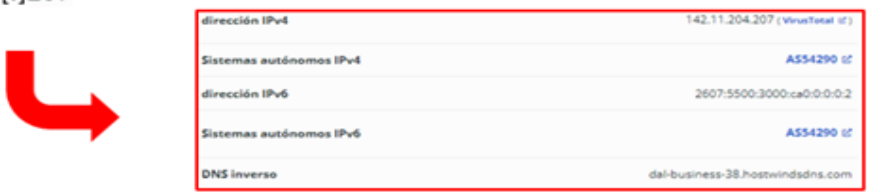
a) Indicadores de compromiso:

I. **URL:** hxxp://www[.]spotifystudent[.]com

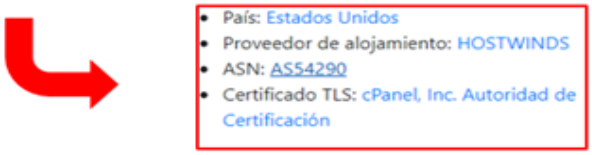



II. **Dominio:** spotify[.]ax

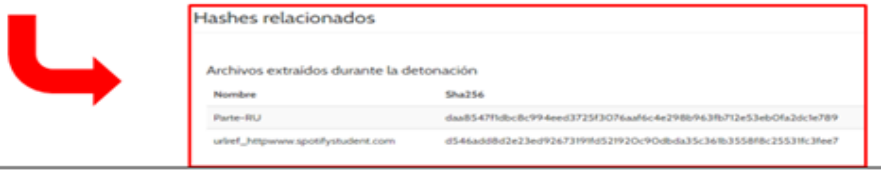

III. **IP:** 142[.]11[.]204[.]207




IV. **Proveedor de alojamiento**: HOSTWINDS



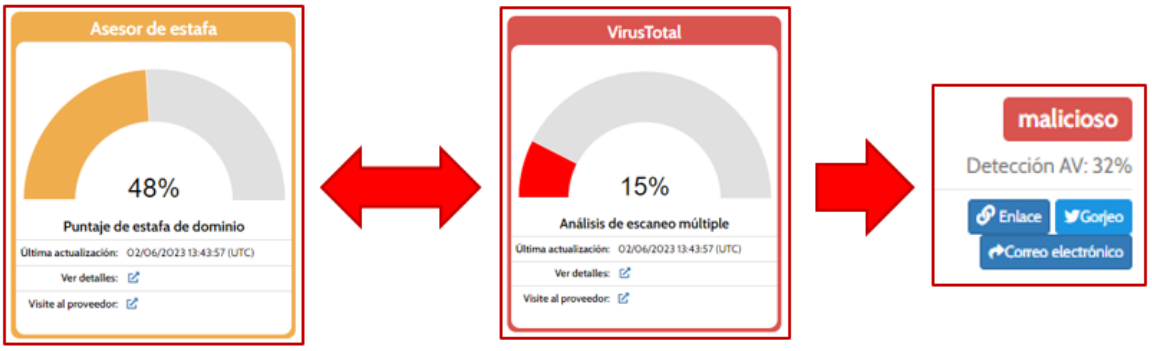

V. **SHA-256:** daa8547f1dbc8c994eed3725f3076aaf6c4e298b963fb712e53eb0fa2dc1e789



VI. Se hallaron diecisiete (17) proveedores de seguridad que marcaron este dominio como malicioso.

| | | | |
|---|---|---|---|
| alphaMountain.ai | Suplantación de identidad | AlphaSOC | Suplantación de identidad |
| Anti-AVL | Malicioso | Avira | Suplantación de identidad |
| BitDefender | Malware | CRDF | Malicioso |
| CyRadar | Malicioso | ESET | Suplantación de identidad |
| Buscador de amenazas de Forcepoint | Suplantación de identidad | Fortinet | Suplantación de identidad |
| G-datos | Malware | Leonico | Suplantación de identidad |
| Búsqueda segura | Malicioso | Sophos | Suplantación de identidad |
| Inteligencia de amenazas de Viettel | Malicioso | VIPRE | Malicioso |
| raíz web | Malicioso | Abusix | Limpio |

4. Otras detecciones:




5. Cómo funciona el Phishing:
   a) Los correos electrónicos incluyen enlaces a sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
   b) Medios de propagación del Phishing: WhatsApp, telegram, redes sociales, SMS entre otros.
   c) Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público o privado, entidad financiera, servicio técnico, etc.)
6. Referencia:
   a) 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.
7. Spotify:
   a) Es un servicio de música, pódcasts y vídeos digitales que te da acceso a millones de canciones y a otro contenido de creadores de todo el mundo. Spotify está disponible en una gran variedad de dispositivos, como ordenadores, teléfonos, tabletas, altavoces, televisores o coches, y puedes pasar fácilmente de uno a otro con Spotify Connect.
8. Recomendaciones:
   a) Utilizar un antivirus actualizado ya que es la primera barrera ante un ataque cibernético.
   b) No compartir la información con terceras personas, amigos o familiares.
   c) Evitar responder a mensajes enviados (correo electrónico, Whatsapp, SMS y otros), que contengan enlaces de dudosa procedencia.
   d) Verificar detenidamente la redacción y ortografía de la dirección URL, que coincidan con el sitio web oficial.
   e) Acceder al sitio web a través de fuentes oficiales.

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