

| | | | |
|---|--|-----------------------|--------------------------|
|  | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°206 | | Fecha: 01-09-2023 |
| | | | |
| Componente que reporta | DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ | | |
| Nombre de la alerta | Nueva campaña de Phishing que suplanta la identidad de Outlook | | |
| 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 se encuentran desarrollando una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad del sitio oficial de "Outlook"; con el objetivo de acceder u obtener credenciales de inicio de sesión de las posibles víctimas.

2. DETALLES:



Sitio web fraudulento; donde los atacantes buscan persuadir a sus víctimas, solicitando ingresar las credenciales de acceso, sin embargo, la información otorgada es capturada por los ciberdelincuentes.

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

a) Indicadores de compromisos:

I. URL: `hxtps[:]//13llunessitges[.]com/W/uni-frankfurt[.]de/`



| | |
|----------------------------|--|
| Nombre del envío: | hxtps://13llunessitges.com/W/uni-frankfurt.de/ |
| Tamaño: | 70B |
| Tipo: | URL ⓘ |
| Mímica: | Texto sin formato |
| Sistema operativo: | ventanas  |
| Último análisis antivirus: | 01/09/2023 20:50:55 (UTC) |
| Último informe de Sandbox: | 01/09/2023 20:50:53 (UTC) |

II. SHA-256: `954fee63bacdaca5edcffd2c321a26d27909666c184ace72dd8fc55c64041fcf`



| | |
|--|--|
| <code>_CD4CEBE6-4BF8-11EE-986F-080027218644_dat</code> <small>320e85ca3e8d2cf55a5b0e78f68c5ce2ca891dde8e91f6071ce7086d936512d</small> | sospechoso |
| <code>RecoveryStore__88B090CO-D917-11E7-B67B-080027A49DD6_dat</code> <small>18289d33e03bc3c594f1fb8367b3b1dc9649167908382d036369fe20cc68613</small> | sospechoso |
| <code>_C2FD529B-4BF8-11EE-986F-080027218644_dat</code> <small>dd6e7d3d64a0a98aa27b73f57b47d8aef12cc7cb016914565d14353915078cf</small> | sospechoso |
| <code>RecoveryStore__C2FD5299-4BF8-11EE-986F-080027218644_dat</code> <small>0ba08dd527d8af3d587ca9c4c7155bfela0216d79434757b3ef6fe2c791b80c</small> | sospechoso |

III. IP: 192[.]185[.]94[.]57



| Connection | | Detection | |
|-----------------------|--------------------------------|---------------|--------|
| Representative Domain | N/A | Proxy IP | False |
| SSL Certificate | ! True (*.websitewelcome.com) | VPN IP | False |
| IP Address Owner | NETWORK-SOLUTIONS-HOSTI... | Tor IP | False |
| Hostname | 192-185-94-57.unifiedlayer.com | Hosting IP | ! True |
| Connected Domains | ! 73 | Mobile IP | False |
| Country | 🇺🇸 United States | CDN IP | False |
| | | Scanner IP | False |
| | | Special Issue | 0 |

IV. TIPOLOGÍA:



Se puede apreciar como la URL, esta alojada en un servidor ubicado en EE. UU.

B. Se hallaron **14 proveedores** de seguridad que marcaron este dominio como malicioso.

| | | | |
|-----------|-------------|---------------------|-------------|
| Avira | ! Phishing | BitDefender | ! Phishing |
| Emsisoft | ! Phishing | ESET | ! Phishing |
| Fortinet | ! Phishing | Google Safebrowsing | ! Phishing |
| Kaspersky | ! Phishing | Lionic | ! Phishing |
| Netcraft | ! Malicious | Seclookup | ! Malicious |
| Segasec | ! Phishing | Sophos | ! Phishing |
| Trustwave | ! Phishing | Webroot | ! Malicious |

C. Otras detecciones:

MALICIOSO

<https://13lunessitges.com/W/u...>

Analizado en: 01/09/2023 20:50:53 (...)

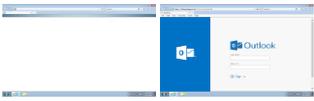
Ambiente: Windows 7 de 32 bits

Puntuación de amenaza: 100/100

Detección AV: 15% sitio de phishing

Indicadores: 2 4 10

Red: 🇩🇪 🇺🇸





malicioso

Puntuación de amenaza: 100/100

#suplantación de identidad

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 legítima (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 lleguen 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 sospechosos o de dudosa procedencia.
- Verificar la fuente de información de tus correos entrantes.
- Introducir 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.