PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 25 de marzo de 2024

073-2024-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°073	Fecha: 25-03-2024
		Página: 4 de 15

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	El nuevo kit de phishing que omite MFA apunta a cuentas de Microsoft 365 y Gmail		
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:

Un nuevo kit de phishing denominado Tycoon 2FA ha generado importantes preocupaciones en la comunidad de ciberseguridad.

Descubierto por el equipo de Investigación y Detección de Amenazas de Sekoia (TDR) en octubre de 2023 y discutido en un aviso publicado hoy, el kit está asociado con la técnica Adversary-in-The-Middle (AiTM) y supuestamente utilizado por múltiples actores de amenazas para orquestar ataques generalizados. y ataques efectivos.

Según la investigación de Sekoia, la plataforma Tycoon 2FA (autenticación de dos factores) ha estado activa desde al menos agosto de 2023. Desde su descubrimiento, la empresa ha estado monitoreando activamente la infraestructura asociada con Tycoon 2FA.

2. DETALLES:

El análisis reveló que el kit se ha convertido en uno de los kits de phishing AiTM más frecuentes, con más de 1100 nombres de dominio detectados entre octubre de 2023 y febrero de 2024.

Los ciberdelincuentes han estado utilizando cada vez más esta nueva plataforma de phishing como servicio (PhaaS) para apuntar a cuentas de Microsoft 365 y Gmail y eludir la protección de autenticación de dos factores (2FA).

El kit PhaaS comparte similitudes con otras plataformas de adversario en el medio (AitM), como Dadsec OTT, lo que sugiere una posible reutilización de código o una colaboración entre desarrolladores.

El kit de phishing Tycoon 2FA opera a través de varias etapas para ejecutar sus actividades maliciosas de manera efectiva, en las que roba cookies de sesión mediante el uso de un servidor proxy inverso que aloja la página web de phishing, que intercepta la entrada de la víctima y la retransmite al servicio legítimo.

El informe de Sekoia describe los ataques en siete etapas distintas, como se describe a continuación:

- Etapa 0: los atacantes distribuyen enlaces maliciosos a través de correos electrónicos con URL o códigos QR incrustados, engañando a las víctimas para que accedan a páginas de phishing.
- Etapa 1: un desafío de seguridad (Cloudflare Turnstile) filtra los bots, permitiendo que solo las interacciones humanas accedan al sitio de phishing engañoso.
- Etapa 2: los scripts en segundo plano extraen el correo electrónico de la víctima de la URL para personalizar el ataque de phishing.
- Etapa 3: los usuarios son redirigidos silenciosamente a otra parte del sitio de phishing, acercándolos a la página de inicio de sesión falsa.
- Etapa 4: esta etapa presenta una página de inicio de sesión falsa de Microsoft para robar credenciales, utilizando WebSockets para la filtración de datos.
- Etapa 5: el kit imita un desafío 2FA, interceptando el token 2FA o la respuesta para eludir las medidas de seguridad.
- Etapa 6: finalmente, las víctimas son dirigidas a una página que parece legítima, lo que oscurece el éxito del ataque de phishing.

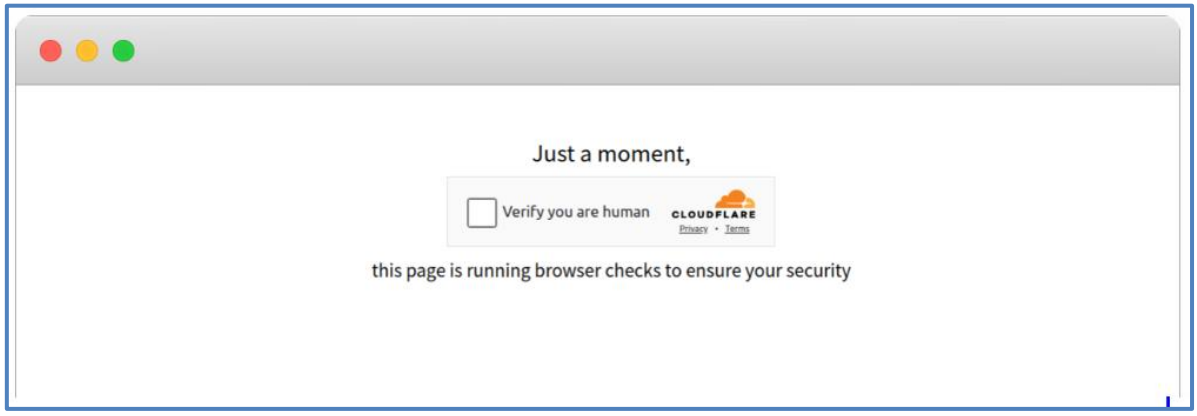


Figura: Página personalizada que incorpora un desafío Cloudflare Turnstile utilizado por el kit de phishing Tycoon 2FA

En el aviso de hoy, Sekoia dijo que identificó una nueva versión de Tycoon 2FA en febrero de 2024 que presenta cambios significativos en sus códigos JavaScript y HTML, mejorando sus capacidades de phishing. En particular, reorganiza la recuperación de recursos y amplía el filtrado de tráfico para frustrar la actividad de los bots y los intentos de análisis.

En comparación con la versión anterior, las modificaciones notables incluyen:

- La página HTML inicial, similar a la etapa 1, conserva su función, pero excluye el desafío Cloudflare Turnstile.
- La carga útil posterior, nombrada en un patrón reconocible, incorpora elementos tanto de la etapa 4 (página de inicio de sesión falsa) como de la etapa 1 de la nueva versión (desafío Cloudflare Turnstile). Se omiten las operaciones matemáticas innecesarias en la desofuscación.
- Las descargas de JavaScript que anteriormente estaban separadas se consolidan en las etapas 4 y 5. Estas etapas ahora manejan la implementación de 2FA y la transmisión de datos.
- Se refinan las tácticas de sigilo, lo que retrasa la provisión de recursos maliciosos hasta después de la resolución del desafío de Cloudflare. Las URL ahora reciben nombres aleatorios.
- Además, el kit se adapta para evadir el análisis identificando y evitando varios patrones de tráfico, incluidos los de centros de datos, Tor y agentes de usuario de bots específicos.

Los investigadores agregaron que ya se han obtenido más de $ 394,000 en criptomonedas mediante la billetera de criptomonedas aprovechada en los ataques Tycoon 2FA.

IOCs

- 0q5e0.nemen9[.]com
- 25rw2.canweal[.]com
- 35fu2.ouchar[.]ru
- 4343w.jgu0[.]com
- 43rw98nop8.m1p8z[.]com
- 4m2swl.7e2r[.]com
- 5me78.methw[.]ru
- 6j312 .rchan0[.]com
- 77p3e.rimesh3[.]com
- 8000n.uqin[.]ru
- 8uecv.gnornamb[.]com
- 98q5e.ructin[.]com
- 9c43r.theq0[.]com
- 9oc0y2isa27.demur3[.]com
- baliza. diremsto[.]com

- bloggcenter[.]com
- buneji.fiernmar[.]com
- e85t8.nechsha[.]com
- ex1uo.rhknt[.]ru
- explore.atlester[.]ru
- fiq75d.rexj[.]ru
- fisaca.trodeckh[.]com
- galume.aricente[.]com
- gz238.uatimin[.]com
- horizonte.sologerg[.]com
- jp1y36.it2ua[.]com
- k348d.venti71[.]com
- kjlvo.ningeona[.]com
- kjsdflwe.nitertym[.] ru
- l846d.ferver8[.]com
- libudi.oreversa[.]com
- n29k4.ilert[.]ru
- n9zph.lw8opi[.]com
- o6t94g.3tdx2r[.]com
- oo99v.coqqwx[.]ru
- p1v12.17nor[.]com
- pmd8ot6xhw.3qjpc[.]com
- q908q.refec7[.]com
- r298y.sem01[.]com
- rlpq.tk9u[.]com
- roriku.orankfix[.]com
- tlger-surveillance[.]com
- tnyr.moporins[.]com
- wasogo .shantowd[.]com
- x12y.restrice[.]ru
- xrs.chenebystie[.]com
- xva.tjlpkcia[.]com
- zaqaxu.dthiterp[.]ru
- zekal6.tnjxb[.]com
- zemj4f.ymarir[.]ru

3. RECOMENDACIONES:

- No hacer clic en enlaces sospechosos ni descargar archivos adjuntos de fuentes desconocidas.
- Verificar la fuente de información de tus correos entrantes.
- Mantener el software actualizado. Actualizar periódicamente los sistemas operativos, las aplicaciones y el software de seguridad para corregir las vulnerabilidades.
- Implementar soluciones de seguridad integrales que puedan detectar y bloquear malware.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• hxxps://www.infosecurity-magazine.com/news/new-tycoon-2fa-phishing-kit/ • hxxps://www.bleepingcomputer.com/news/security/new-mfa-bypassing-phishing-kit-targets-microsoft-365-gmail-accounts/ • hxxps://blog.sekoia.io/tycoon-2fa-an-in-depth-analysis-of-the-latest-version-of-the-aitm-phishing-kit/

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°073**	**Fecha: 25-03-2024**
		Página: 7 de 15

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en LG LED Assistant		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo autenticación incorrecta que afecta a LG LED Assistant. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto restablecer la contraseña de usuarios anónimos sin autorización en el equipo afectado.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-2862 de tipo autenticación incorrecta, podría permitir a un atacante remoto restablecer la contraseña de usuarios anónimos sin autorización en el LG LED Assistant afectado.

Un ataque exitoso de abuso de autenticación podría permitir a un atacante remoto obtener acceso no autorizado a una aplicación, servicio o dispositivo, ya sea a través del conocimiento de las debilidades inherentes de un mecanismo de autenticación o explotando una falla en la implementación del esquema de autenticación. En tal ataque, funciona un mecanismo de autenticación, pero una secuencia de eventos cuidadosamente controlada hace que el mecanismo otorgue acceso al atacante.

A. Productos afectados:

- LG LED Assistant, versión 2.1.65.

3. RECOMENDACIÓN:

- Actualizar los productos afectados con la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxps://www.cve.org/CVERecord?id=CVE-2024-2862 • hxxps://lgsecurity.lge.com/bulletins/idproducts#updateDetails

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°073	Fecha: 25-03-2024
		Página: 8 de 15

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en Microsoft Edge		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado múltiples vulnerabilidades de severidad **ALTA** y **MEDIA** de tipo control de seguridad implementado incorrectamente para el estándar, control inadecuado de un recurso a lo largo de su vida útil, secuencias de comandos universales entre sitios, uso después de la liberación, lectura fuera de límites y ataque de suplantación de identidad en Microsoft Edge. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto obtener acceso a información confidencial, realizar ataques de secuencias de comandos entre sitios (XSS) y de suplantación de identidad.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-2628 de tipo control de seguridad implementado incorrectamente para el estándar, existe debido a una implementación incorrecta en Descargas en Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite y obtener acceso a información confidencial.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-2630 de tipo control de seguridad implementado incorrectamente para el estándar, existe debido a una implementación incorrecta en iOS en Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite y obtener acceso a información confidencial.

Se han asignado los siguientes identificadores para las vulnerabilidades de severidad **media**: CVE-2024-2625, CVE-2024-26247, CVE-2024-2627, CVE-2024-2626 y CVE-2024-2629

A. Productos afectados:

- Microsoft Edge: 79.0.309.71 - 122.0.2365.106.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-2625 • hxxp://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26247 • hxxp://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-2627 • hxxp://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-2626 • hxxp://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-2628 • hxxp://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-2629 • hxxp://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-2630

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°073**	**Fecha: 25-03-2024**
		Página: 9 de 15

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en el cliente RabbitMQ C		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **ALTA** de tipo desbordamiento de búfer basada en la pila en el cliente RabbitMQ C. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

RabbitMQ es un popular software de mensajería de código abierto que implementa el protocolo de Advanced Message Queuing Protocol (AMQP) para sistemas de mensajería.

La vulnerabilidad de severidad **alta** de tipo desbordamiento de búfer basada en la pila, existe debido a un error de límite en la decodificación de la tabla y la matriz. Un atacante remoto no autenticado puede provocar un desbordamiento de búfer basado en pila y ejecutar código arbitrario en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso total del sistema vulnerable.

A. Productos afectados:

- Cliente RabbitMQ C: 0.1 - 0.13.0.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxp://github.com/alanxz/rabbitmq-c/releases/tag/v0.14.0 • hxxps://github.com/alanxz/rabbitmq-c

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°073	Fecha: 25-03-2024
		Página: 10 de 15

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Actualización de Red Hat Enterprise Linux 9 para Thunderbird		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado la actualización de múltiples vulnerabilidades de severidad **ALTA** de tipo valor de retorno no verificado, desbordamiento de enteros, uso después de la liberación y desbordamiento de búfer de Red Hat Enterprise Linux 9 para Thunderbird. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino y comprometer el sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-0743 de tipo valor de retorno no verificado, existe debido a un valor de retorno no verificado en el código de protocolo de enlace TLS en el método NSS TLS. Un atacante remoto puede engañar a la víctima para que visite un sitio web especialmente diseñado y ejecute código arbitrario en el sistema.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-2608 de tipo desbordamiento de enteros, existe debido al desbordamiento de enteros dentro de las funciones: AppendEncodedAttributeValue(), ExtraSpaceNeededForAttrEncoding() y AppendEncodedCharacters(). Un atacante remoto puede engañar a la víctima para que visite un sitio web especialmente diseñado, provocar un desbordamiento de enteros y ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-2612 de tipo uso después de la liberación, existe debido a un error de uso después de la liberación al procesar contenido HTML. Un atacante remoto puede engañar a la víctima para que visite un sitio web especialmente diseñado para activar una ruta de código particular en SafeRefPtr y ejecutar código arbitrario en el sistema.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-2614 de tipo desbordamiento de búfer, existe debido a un error de límite al procesar contenido HTML. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la abra, provocar daños en la memoria y ejecutar código arbitrario en el sistema objetivo.

A. Productos afectados:

- Red Hat Enterprise Linux para ARM 64:9.
- Red Hat Enterprise Linux para potencia, little endian: 9.
- Red Hat Enterprise Linux para sistemas IBM z: 9.
- Red Hat Enterprise Linux para x86_64: 9.
- Thunderbird (paquete Red Hat): anterior a 115.9.0-1.el9_3.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades

Fuente de Información:	• hxxp://access.redhat.com/errata/RHSA-2024:1493

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°073**	**Fecha: 25-03-2024**
		Página: 11 de 15

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en Web Proxy		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **ALTA** de tipo inyección de comandos del sistema operativo en Web Proxy. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar comandos de Shell arbitrarios en el sistema de destino.

2. DETALLES:

Un web proxy es un intermediario que actúa entre un usuario y un servidor web. Funciona como un puente que permite al usuario realizar solicitudes a través del proxy en lugar de comunicarse directamente con el servidor. Esto puede tener varios propósitos, como ocultar la dirección IP del usuario, eludir restricciones de acceso geográfico o de red, mejorar la velocidad de acceso a los sitios web al almacenar en caché contenido previamente descargado, entre otros. Los webs proxies pueden ser útiles para mantener la privacidad en línea o para acceder a contenido bloqueado, pero también pueden tener limitaciones en cuanto a seguridad y confiabilidad, ya que algunos pueden registrar las actividades del usuario o introducir riesgos de seguridad si no están correctamente configurados.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-28033 de tipo inyección de comandos del sistema operativo, existe debido a una validación de entrada incorrecta. Un atacante remoto no autenticado puede pasar datos especialmente diseñados a la aplicación y ejecutar comandos arbitrarios del sistema operativo en el sistema de destino.

A. Productos afectados:

- Proxy web: 1.7.8.

3. RECOMENDACIÓN:

- Actualizar el paquete afectado cuando el proveedor lance la última versión para abordar esta vulnerabilidad. Actualmente aún no hay ninguna solución oficial.

Fuente de Información:	• hxxp://jvn.jp/en/jp/JVN22376992/index.html.

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°073	Fecha: 25-03-2024
		Página: 12 de 15

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 Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

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 (correo y contraseña) de los usuarios de la compañía tecnológica.

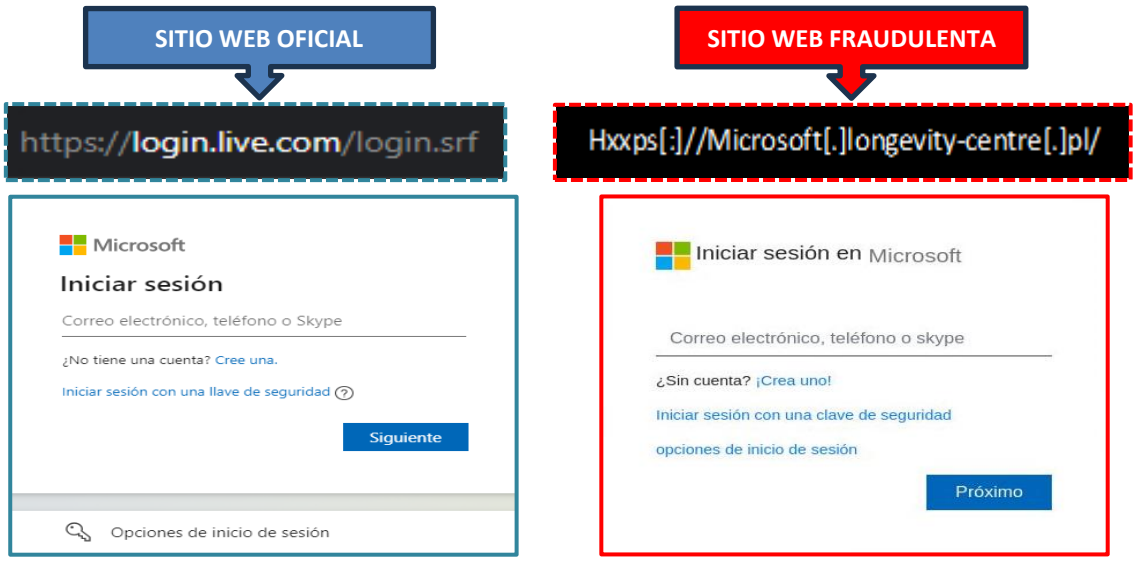
2. DETALLES:

El proceso del Phishing es el siguiente:

Sitio web falso de la compañía de "Microsoft", solicita a la víctima que registre el correo electrónico de la víctima, para acceder al servicio en la web de la compañía Microsoft (Outlook, Hotmail, etc.)

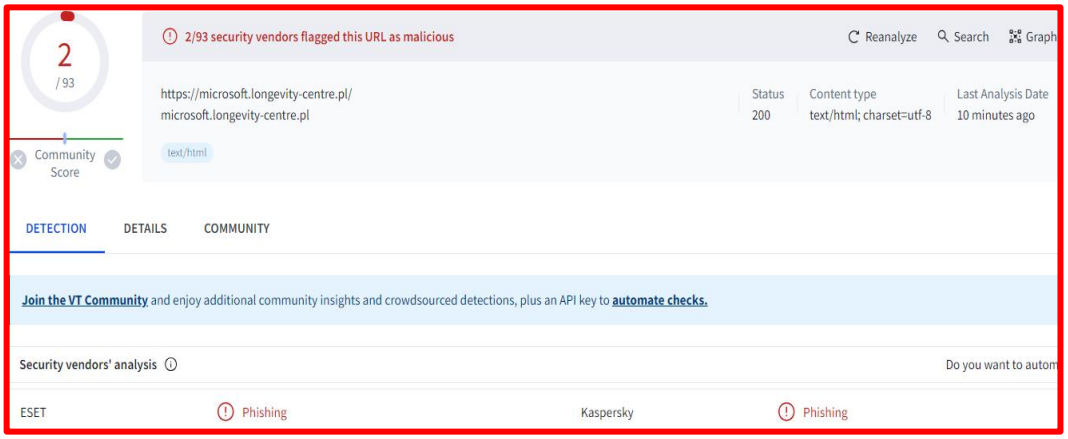
Luego, el atacante requiere la contraseña de acceso para el servicio web de Microsoft, para luego dar clic en <**Iniciar sesión**>; sin embargo, después de unos segundos redirige al servicio del correo electrónico de la compañía Microsoft.

A. Comparación del sitio web oficial y fraudulento.



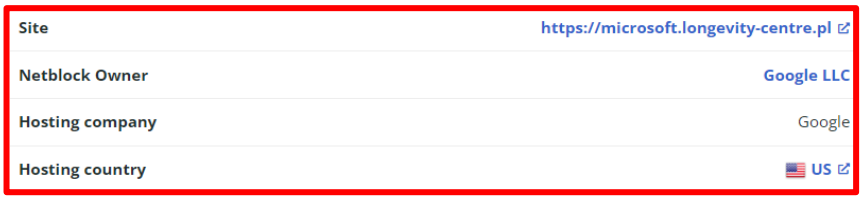
- Existe diferencias entre la URL original y la fraudulenta.
- La URL del sitio web fraudulento posee protocolo de seguridad de red (https)
- Existe una similitud entre ambas páginas en imagen, fondo y colores de ambos sitios web.

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

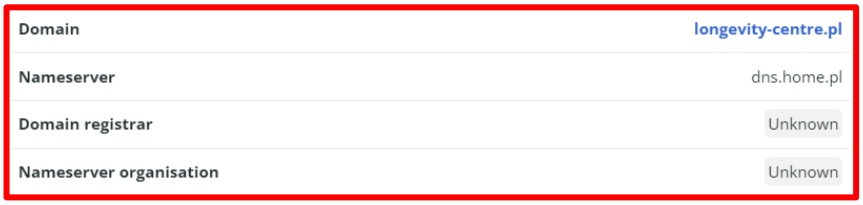


C. Indicadores de compromiso (IoC)

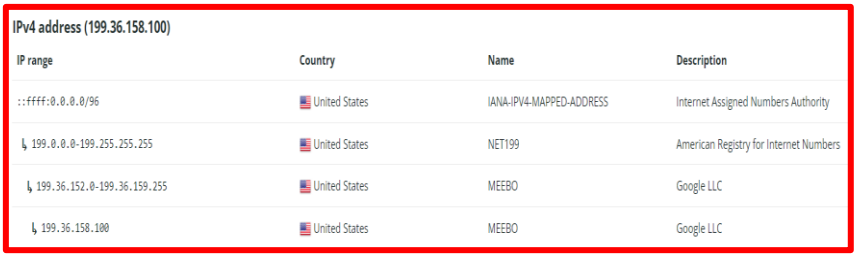
- Url : hxxps[:]//Microsoft[.]longevity-centre[.]pl/



- Dominio : longevity-centre[.]pl



- IP : 199[.]36[.]158[.]100



- SHA-256 : 37e7a7ad7b9ec41782991721a37e53867be791b2f7873094909aaf78b4131f00
- Contenido : Text/Html

D. 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.).
- La propagación del sitio web fraudulento se realiza mediante envió masivos de email, adjuntando enlaces de sitios web fraudulentos con la finalidad de obtener información sensible de las víctimas; asimismo, dicho enlace malicioso, es enviado a través de las plataformas digitales como el WhatsApp, Telegram, Messenger y mensajes de textos SMS.

3. 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.

Fuente de Información:	Análisis propio de redes sociales y fuente abierta

Índice alfabético