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

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc

Lima, 26 de julio de 2022

N° 201-2022-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

SmokeLoader infecta sistemas mediante malware Amadey 4

El hackeo SATAn convierte en un emisor de radio el cable de tu disco duro y permite copiar su contenido sin abrir el PC 6

Suplantación de página web de empresa 7

Nuevos hashes maliciosos 9

Vulnerabilidades en el servidor de dispositivos NPORT 5110 de MOXA 11

Nueva campaña de Phishing que suplanta la identidad de la plataforma de Discord 12

Índice alfabético 14

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	SmokeLoader infecta sistemas mediante malware Amadey		
Tipo de ataque	Malware	Tipo de ataque	Malware
Medios de propagación	Red, internet		
Código de familia	C	Código de familia	C03
Clasificación temática familia	Código Malicioso		

Descripción

En una publicación realizada el 26 de julio de este año por "The Hacker News", se menciona a SmokeLoader infectando sistemas objetivo con malware de robo de información de Amadey.

ANTECEDENTES:

- Amadey, es una botnet que apareció por primera vez en octubre de 2018, dentro de los foros clandestinos rusos.
- En julio pasado, Walmart Global Tech detectó una actualización que incorporó la funcionalidad para recopilar datos de los enrutadores Mikrotik y Microsoft Outlook, el conjunto de herramientas se actualizó para capturar información de FileZilla, Pidgin, Total Commander FTP Client, RealVNC, TightVNC, TigerVNC y WinSCP.

DETALLES:

- El malware de robo de información lleva por nombre Amadey y se distribuye a través de otra puerta trasera llamada SmokeLoader.
- Según investigadores del Centro de Respuesta a Emergencias de Seguridad AhnLab (ASEC), la forma de ataque es engañar a los usuarios para que descarguen SmokeLoader, el cual se hace pasar por cracks de software, facilitando el camino para el despliegue de Amadey.

- Amadey está equipada para desviar credenciales, hacer capturas de pantalla, metadatos del sistema e incluso información sobre motores antivirus y malware adicional instalado en una máquina infectada.
- Su objetivo principal es implementar complementos adicionales y troyanos de acceso remoto como Remcos RAT y RedLine Stealer, lo que permite aún más que el actor de amenazas realice una serie de actividades posteriores a la explotación.

A continuación, se brinda una lista con Indicadores de Compromiso (IoC).

http[:]//azd[.]at/forum/index[.]php	http[:]//45[.]227[.]255[.]49/5Lsq3FR/index[.]php
http[:]//62[.]204[.]41[.]117/nkg3skjvSaq2/index[.]php	http[:]//179[.]43[.]155[.]137/fjgD555c3/index[.]php
http[:]//cloudreactions[.]xyz/g93kdm3SaQ/index[.]php	http[:]//soul-kissed[.]org/fjgD555c3/index[.]php
http[:]//guideanceers[.]com/g93kdm3SaQ/index[.]php	http[:]//rupeika[.]info/fjgD555c3/index[.]php
http[:]//dssclientdownloadsprospect[.]com/nkg3skjvSaq2/index[.]php	http[:]//antispam-screen[.]com/fjgD555c3/index[.]php
http[:]//russk21[.]icu/rest/index[.]php	http[:]//systemupdate22[.]cf/d2VxjasuwS/index[.]php
http[:]//moscow13[.]at/rest/index[.]php	http[:]//185[.]215[.]113[.]15/Lkb2dxj3/index[.]php
http[:]//81[.]19[.]135[.]247/Kn82d22zzU/index[.]php	http[:]//5[.]188[.]118[.]7/ppp3aZfj3nil/index[.]php
http[:]//teamfighttacticstools[.]info/5Lsq3FR/index[.]php	http[:]//62[.]204[.]41[.]174/f8dfksdj3/index[.]php
http[:]//185[.]215[.]113[.]204/Lkb2dxj3/index[.]php	http[:]//185[.]215[.]113[.]92/gg4mn3s/index[.]php
http[:]//pppproyectkz[.]icu/5kv4Pqi/index[.]php	http[:]//marobast[.]ws/b3m2fVVs0/index[.]php
http[:]//kkskksnut[.]icu/5kv4Pqi/index[.]php	http[:]//185[.]215[.]113[.]205/fjgD555c3/index[.]php
http[:]//huteuhksr[.]icu/5kv4Pqi/index[.]php	http[:]//sigint[.]ws/f8dfksdj3/index[.]php
http[:]//nftmatrixed[.]info/5Lsq3FR/index[.]php	http[:]//dhisa8f9ah02hopasiaf[.]com/gg4mn3s/index[.]php
http[:]//authymysexy[.]info/5Lsq3FR/index[.]php	http[:]//xksldjf9sksdjfks[.]com/gg4mn3s/index[.]php

RECOMENDACIONES:

- Actualizar los dispositivos a las últimas versiones del sistema operativo.
- Actualizar los navegadores web.
- Evitar software ilegal.
- Evitar links de dudosa procedencia.
- Descargar software de sitios confiables y verificados.
- Utilizar configuraciones robustas de seguridad.
- Realizar backups de información de carácter sensible y confidencial de manera periódica.
- Reforzar medidas de seguridad ante ataques de malware (herramientas de seguridad robustas).

Fuentes de información	▪ hxxps://thehackernews.com/2022/07/smokeloader-infecting-targeted-systems.html ▪ hxxps://diariopb.com/smokeloader-infecta-sistemas-objetivo-con-malware-de-robo-de-informacion-de-amadey/ ▪ hxxps://threatfox.abuse.ch/browse/tag/Amadey/ ▪ Análisis propio de fuentes abiertas.

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 201	Fecha: 26-07-2022
		Página 06 de 14

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	El hackeo SATAn convierte en un emisor de radio el cable de tu disco duro y permite copiar su contenido sin abrir el PC		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Subfamilia	C02
Clasificación temática familia	Código Malicioso		

Descripción

ANTECEDENTES

1. El 25 de julio del 2022, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tuvo conocimiento que, investigadores de seguridad de Israel han descubierto una nueva técnica de ciberataque que han denominado "SATAn"

2. El nuevo método SATAn es, básicamente, una forma de robar información y datos de sistemas protegidos por el aire utilizando el cable SATA como antena inalámbrica para transmitir datos e información desde un PC a algún dispositivo de un lugar cercano.

MODO DE ATAQUE

3. El cable SATA (Serial Advanced Technology Attachment), es el elemento que une físicamente la placa base con los dispositivos de almacenamiento. Este lo vamos a encontrar muy fácilmente si abrimos nuestra torre PC y sirvieron para mejorar la velocidad y la capacidad de transmisión de datos respecto a los conectores que se utilizaban antes.
4. Este tipo de hackeo surge de la necesidad de robo de datos muy protegidos que pertenecen a sistemas o redes con protección aérea, que están aislados de cualquier conexión con el resto del mundo (ni Internet, ni Bluetooth). Es por eso que se hace necesaria otra forma de violación de los sistemas de seguridad. Hackearlos es muy complicado, pero ya vemos que no imposible y SATAn es la respuesta. Y es que, en este proceso todo se reduce a la manipulación de la interferencia electromagnética gracias a este cable.
5. En una prueba para analizar cómo este sistema realmente funciona y, por lo tanto, hace vulnerable un sistema protegido, el investigador manipuló esta interferencia electromagnética y utilizó el cable SATA como una antena inalámbrica improvisada que opera en la banda de frecuencia de 6 GHz., manifestando que, el receptor monitoriza el espectro de 6 GHz en busca de una posible transmisión, demodula los datos, los descodifica y los envía al atacante.
6. Además, para este ataque se necesita la instalación previa de un software malicioso (Malware) para poder completar todo el proceso. Quizá esta pueda ser la parte más compleja, ya que sin esto es imposible robar datos a través de SATAn.

RECOMENDACIÓN

7. Como contramedidas, se recomienda tomar medidas para evitar que el actor de la amenaza obtenga un punto de apoyo inicial, usar un sistema de monitoreo de radiofrecuencia (RF) externo para detectar anomalías en la banda de frecuencia de 6 GHz del sistema de espacio de aire, o alternativamente, contaminar la transmisión con operaciones aleatorias de lectura y escritura cuando se detecta una actividad sospechosa en un canal encubierto.

Fuentes de información	▪ https://computerhoy.com/noticias/tecnologia/hackeo-satan-convierte-emisor-radio-cable-disco-duro-permite-copiar-contenido-abrir-pc-1099099

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 201	Fecha: 26-07-2022
		Página 07 de 14

Componente que reporta	**COMANDANCIA DE CIBERDEFENSA DE LA MARINA DE GUERRA DEL PERÚ**		
Nombre de la alerta	Suplantación de página web de empresa		
Tipo de ataque	Phishing	Tipo de ataque	Phishing
Medios de propagación	Correo Electrónico		
Código de familia	G	Código de familia	G03
Clasificación temática familia	Fraude		

Descripción

- A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectaron varios sitios webs fraudulentos activos, donde suplantan páginas web de diversas empresas, con la finalidad de obtener las credenciales del usuario y robar información:

- **Facebook**

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-07-26	138.197.235.123	xxxxs://stale-shelf.surge.sh
United States	2022-07-26	138.197.235.123	xxxxs://defeated-nation.surge.sh
United States	2022-07-26	138.197.235.123	xxxxs://abstracted-start.surge.sh
United States	2022-07-26	138.197.235.123	xxxx://mixed-pipe.surge.sh
United States	2022-07-26	138.197.235.123	xxxx://large-cause.surge.sh
Singapore	2022-07-26	52.221.119.58	xxxxs://tribelio.page/recovery-pages
United States	2022-07-26	138.197.235.123	xxxxs://stale-shelf.surge.sh/
United States	2022-07-26	138.197.235.123	xxxxs://defeated-nation.surge.sh/
United States	2022-07-26	138.197.235.123	xxxxs://abstracted-start.surge.sh/
United States	2022-07-26	138.197.235.123	xxxx://mixed-pipe.surge.sh/
United States	2022-07-26	138.197.235.123	xxxx://large-cause.surge.sh/
United States	2022-07-26	138.197.235.123	xxxx://teeny-bread.surge.sh
United States	2022-07-26	138.197.235.123	xxxxs://puffy-trouble.surge.sh
United States	2022-07-26	138.197.235.123	xxxx://teeny-bread.surge.sh/
United States	2022-07-26	138.197.235.123	xxxxs://puffy-trouble.surge.sh/
United States	2022-07-26	199.36.158.100	xxxxs://copyright-helpcenter13165391.firebaseapp.com/

- **Instagram**

PAIS DE PROCEDENCIA	FECHA	IP	URL
Netherlands	2022-07-26	190.2.146.141	xxxx://www.chplaxer.bmsub.icu
Netherlands	2022-07-26	190.2.146.141	xxxx://chplaxer.bmsub.icu
Italy	2022-07-26	45.14.185.135	xxxx://45.14.185.135
Netherlands	2022-07-26	190.2.146.141	xxxx://www.chplaxer.bmsub.icu/
Netherlands	2022-07-26	190.2.146.141	xxxx://chplaxer.bmsub.icu/
Italy	2022-07-26	45.14.185.135	xxxx://45.14.185.135/login.html
Italy	2022-07-26	45.14.185.135	xxxx://45.14.185.135/

- **Office 365**

PAIS DE PROCEDENCIA	FECHA	IP	URL
Hungary	2022-07-26	185.33.53.142	xxxx://www.kkzcoaching.com/CD/docusign%20office
Seychelles	2022-07-26	103.211.218.190	xxxxs://corbettparkindia.com/ufile
Hungary	2022-07-26	185.33.53.142	xxxx://www.kkzcoaching.com/CD/docusign%20office/
Seychelles	2022-07-26	103.211.218.190	xxxxs://corbettparkindia.com/ufile/

- **Netflix**

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-07-26	109.206.241.140	xxxxs://vibrant-kapitsa.109-206-241-140.plesk.page/x3d/main
Russia	2022-07-26	91.189.114.12	xxxx://www.school238.ru/cm.php
United States	2022-07-26	162.241.117.188	xxxxs://www.secur61kverify.duckdns.org/Netflix/Home/login.php
United States	2022-07-26	109.206.241.140	xxxxs://vibrant-kapitsa.109-206-241-140.plesk.page/x3d/main/
United States	2022-07-26	20.14.89.196	xxxxs://nfxserve08.co.vu/
United States	2022-07-26	20.14.89.196	xxxxs://nfxserve06.co.vu/
United States	2022-07-26	20.14.89.196	xxxxs://nfxserve05.co.vu/
United States	2022-07-26	20.14.89.196	xxxxs://nfxserve04.co.vu/
United States	2022-07-26	20.14.89.186	xxxx://nfxserve03.co.vu/
France	2022-07-26	62.4.16.84	xxxxs://verif-id.selfip.info/net/login.php
France	2022-07-26	62.4.16.84	xxxxs://verif-id.selfip.info/net
United States	2022-07-26	162.240.215.15	xxxxs://zcarh.ml
United States	2022-07-26	162.240.215.15	xxxxs://zcarh.ml/

- **Microsoft Login**

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-07-26	18.223.159.119	xxxxs://www.officefiles.duckdns.org/access
United States	2022-07-26	18.223.159.119	xxxxs://www.officefiles.duckdns.org/access/
United States	2022-07-26	2606:4700::6812:691	xxxxs://storageapi.fleek.co/81a83d0e-db36-4bb2-8b30-3f7519860592-bucket/renew.html
United States	2022-07-26	134.70.124.2	xxxxs://objectstorage.us-sanjose-1.oraclecloud.com/n/axywnxryioz2/b/newdocument001/o/newdocument0001index%20(1).html

- Recomendaciones:
  - Evitar ingresar datos personales a enlaces de dudosa procedencia.
  - Mantener los equipos protegidos, con el software actualizado.

Fuentes de información	Comandancia de Ciberdefensa de la Marina, Osint

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 201	Fecha: 26-07-2022
		Página 09 de 14

Componente que reporta	**COMANDANCIA DE CIBERDEFENSA DE LA MARINA DE GUERRA DEL PERÚ**		
Nombre de la alerta	Nuevos hashes maliciosos		
Tipo de ataque	Malware	Tipo de ataque	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de familia	C03
Clasificación temática familia	Código malicioso		

Descripción

1. El día 26 de julio del 2022, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectaron nuevas firmas de hash maliciosas, entre ellas:

ITEM	HASH SHA256	TIPO DE ARCHIVO	NOMBRE DEL ARCHIVO
1	5f47668ceebd2e8b4b78d34a3a4b8fc18e9ad570201855360af01ccbef372b14	rar	MalwareBytes Premium.rar
2	df63c998bbd8f636780ac228fd7ab7c44fe52cd5bdcf785a3944b5721eb7f2b9	exe	server
3	7d85c6c8abf4c9f2fa6c4528991979d5cbedefc73ec3ce83c04a4839b50c9555	exe	Loader.exe
4	1fe926b0f462b5084913adf51373dbe8e4836cb237e849ff4550679173780881	rar	Loader.rar
5	398dda8819020b08d425a49e334a26aeb49b7b3915cc0d704cd9f9307aef9622	crx	onomjaelhagjjojbkcafidnepbfkpnee.crx
6	79438db226f6df69f83940d66147d7caa952047c0b868a21d647d9bd293bd4af	rar	Installer-2022.rar
7	e30f26ea0eabac5feffa76cf35c0cf8848ab0bcbbc6258cb681ce3969300c176	exe	vt-upload-IiArN
8	4c91a0b1473528bcae811fb58a5306617dc04b64ea4961c0dff0c48f1dfc3e62	exe	No Determinado
9	3422e6f79f556b96084cd45206b2cad7c916f4fceb96a0ec245189a6c3d23a40	exe	Farmaceut.exe
10	6a4494f8358270180bf4ae499fbad16e37da1b072c71b5bf762f83b513f6ec78	exe	Shortcut
11	c1e23c7ba8224266734b9d0914e722627423cdfa81e8aa5efb4def7a0c4c4e28	exe	Farmaceut.exe
12	fc78f2aef5905408e5fcee54803950971117b0ddd96115fff34c2a367e76f779	pdf	inv-wp9577.pdf
13	5f3106c4d1ca3e2b65c50034ff4b9fa597df5278265686760a78967b32a5a78c	exe	Farmaceut.exe
14	b74be8f3f26d71fb5739f1b54f7c7d24db27585acdf33d2f79d94ea898514563	pdf	Office-login.pdf
15	bdbbad2880f980eb911a7d9c6f5e8ed735d08cebe96defdad4e3cb273ece6e43	zip	quotation and agreement.zip
16	0cf50f70d7c77e466dd5ce256f5c78800469977b1266e944da1cd06ba63add21	zip	Special_Rate_Proposal_xlsx.zip
17	d4fa9582da4dd30e6b92b94c52a0fe67f01132da8d40bd229e3c4f7403dc302e	docx	about-us.doc
18	21825f7e7893e4db1214b0b36a755fb83f80cf716a3dc906b83ec66cdb7d6216	exe	Microsoft.Tools.ServiceModel.Svcutil.dll
19	25d76d51bbfe6a09392a23e9077e410a89cac0ac6bb9fed74d5131dc6006dda8	zip	content.5042.21324.7505.28102.31875
20	cbd5ce212f302bdc2a81485ee4d2e4081bb32559e97aed9b663de550f6a29c50	zip	content.4070.30268.20289.1690.19587
21	d30948540393f18ecea174d4d02af2946592d964	rar	FEDeX-Tracking

	3e48e704673aa55fe60ddf64		Details_Updated.r00
22	8afaa0c565368bcb0873dc9e037ffaa7e50514b9d4c646f27daac25332e75182	ace	SKM%20Ref%2026072022%20.ace
23	6b80632991c52ad6552c538d9743cb1006fe8db8ce80fbb58567e1a1606f0230	exe	Farmaceut.exe
24	7005e6d9b81a8392bef6e6667f49adf342d4bcfff339d1337b5caf620061959a	exe	Wextract
25	85031fa95e6d833a180b3e2f2e3c265c2c15152f6ce7d686fe3eeccc028db9d8	exe	85031fa95e6d833a180b3e2f2e3c265c2c15152f6ce7d686fe3eeccc028db9d8.exe

2. Recomendaciones:

- Evitar descargar archivos y/o enlaces de dudosa procedencia.
- Mantener los equipos protegidos, con el software actualizado.

Fuentes de información	Comandancia de Ciberdefensa de la Marina, Osint

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 201**	**Fecha: 26-07-2022**
		Página 11 de 14

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades en el servidor de dispositivos NPORT 5110 de MOXA		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Tipo de Ataque	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. Resumen:

El investigador, Jens Nielsen de En Garde Security, ha reportado dos vulnerabilidades de severidad ALTA de tipo escritura fuera de los límites en el servidor de dispositivos NPort 5110 de MOXA. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto cambiar los valores de la memoria, generar una condición de denegación de servicio (DoS) y/o bloquear el dispositivo afectado.

2. Detalles:

- La vulnerabilidad de severidad **alta** identificada como CVE-2022-2043 de escritura fuera de los límites podría hacer que el dispositivo vulnerable deje de responder y genere una condición de denegación de servicio.
- La vulnerabilidad de severidad **alta** identificada como CVE-2022-2044 de escritura fuera de los límites podría permitir a un atacante sobrescribir los valores en la memoria, provocando una condición de denegación de servicio o bloqueando potencialmente el dispositivo.
- La vulnerabilidad de escritura fuera de los límites se debe a que el software escribe datos más allá del final, o antes del comienzo, del búfer previsto. Por lo general, esto puede provocar la corrupción de datos, un bloqueo o la ejecución de código. El software puede modificar un índice o realizar aritmética de punteros que haga referencia a una ubicación de memoria que esté fuera de los límites del búfer. Una operación de escritura posterior produce resultados indefinidos o inesperados.
- Estas vulnerabilidades afectan a los sectores de infraestructura crítica de Manufactura Crítica, Energía y Sistemas de Transporte en todo el mundo.

3. Productos afectados:

- Servidor de dispositivos MOXA NPort 5110: Versiones de firmware 2.10.

4. Solución:

MOXA recomienda actualizar el producto afectado con la última versión de software disponible que corrige estas vulnerabilidades.

Asimismo, CISA recomienda tomar medidas defensivas para minimizar el riesgo de explotación de estas vulnerabilidades:

- Minimizar la exposición de la red para todos los dispositivos y/o sistemas del sistema de control, y asegurarse de que no sean accesibles desde Internet;
- Ubicar las redes de sistemas de control y dispositivos remotos detrás de firewalls y aíslelos de las redes comerciales;
- Cuando se requiera acceso remoto, use métodos seguros, como Redes Privadas Virtuales (VPN), reconociendo que las VPN pueden tener vulnerabilidades y deben actualizarse a la versión más reciente disponible. También reconozca que VPN es tan segura como sus dispositivos conectados.

Fuentes de información	▪ hxxps://www.cisa.gov/uscert/ics/advisories/icsa-22-207-04

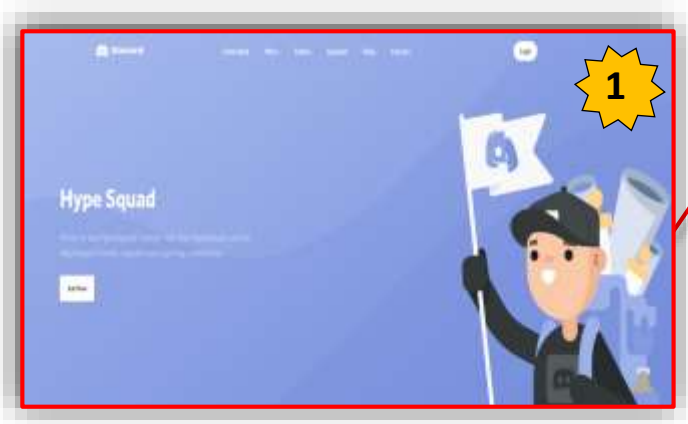
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 201	Fecha: 26-07-2022
		Página 12 de 14

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de Alerta	Nueva campaña de Phishing que suplanta la identidad de la plataforma de Discord		
Tipo de Ataque	Phishing	Tipo de Ataque	Phishing
Medio de Propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de familia	G02
Clasificación temática familia	Fraude		

Descripción

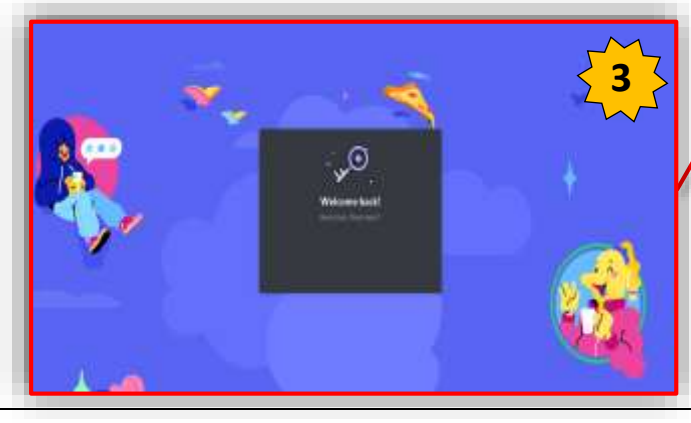
1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad de mensajería instantánea "DISCORD", el supuesto sitio web cuenta con colores y logos característicos idénticos al sitio web oficial, el cual tiene como finalidad robar las credenciales de acceso al servicio.

2. Proceso del ataque Phishing.



Sitio web fraudulento de la plataforma de mensajería instantánea "Discord".

Solicita acceder a la plataforma a través de las credenciales de inicio de sesión (correo electrónico y contraseña).

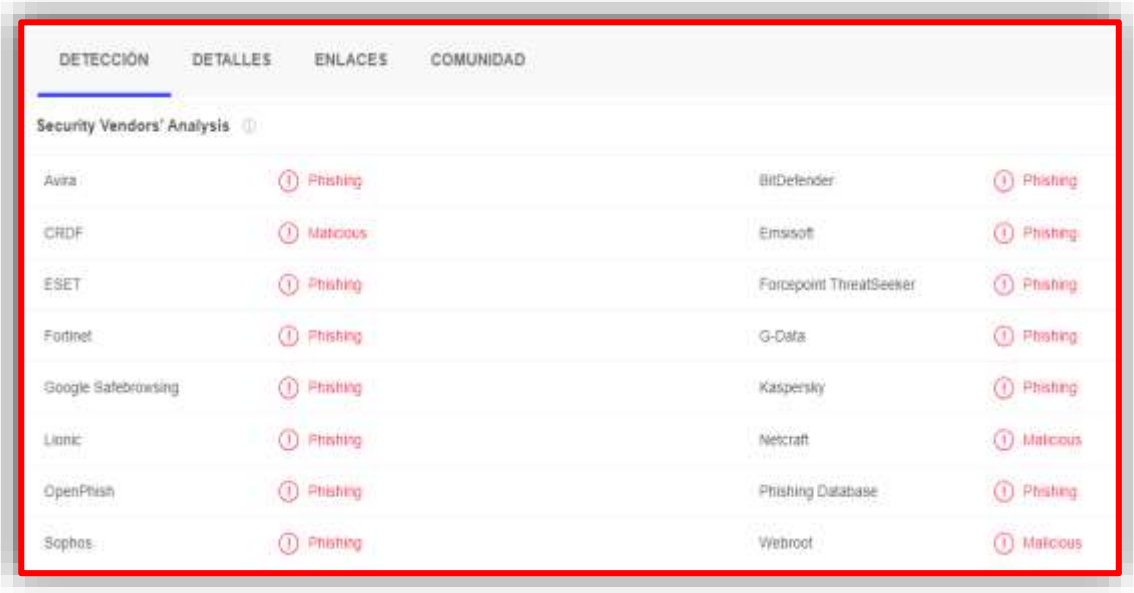


Una vez que se inicie sesión, redirige un mensaje indicando "Bienvenido de nuevo", dando así por concluida la estafa.

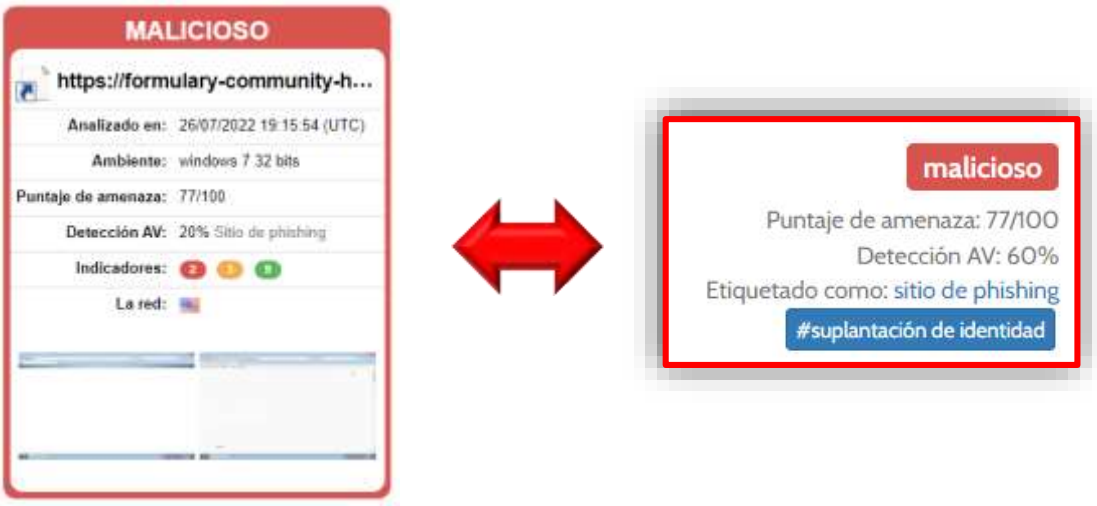
3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

- **INDICADORES DE COMPROMISO:**

  - ✓ **URL** : hxxps[:]//formulary[-]community[-]hypesquad[.]ml/
  - ✓ **Dominio :** formulario[-]comunidad[-]hypesquad[.]ml
  - ✓ **IP.** : 172[.]67[.]169[.]68
  - ✓ **Tamaño** : 45.83 KB
  - ✓ **SHA-256 :** e346288cec71cfe9244c4decea4142654bc291d71ccc08d9e8553434ebe43a52



- **OTROS RESULTADOS DEL ANÁLISIS:**



4. **Algunas Recomendaciones:**

- Verificar detalladamente las URL de los sitios web.
- Introducir datos confidenciales únicamente en webs seguras.
- No introducir nunca las credenciales de inicio de sesión en servicios o aplicaciones de terceros.
- Utilizar una solución de seguridad que filtre los mensajes sospechosos y bloquee las páginas Phishing.
- Ser precavido cuando se recibe mensajes de proveedores o terceros.
- Mantener el antivirus actualizado.

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

Índice alfabético

Ciberespacio 6, 7, 9, 12
Hash 9
Malware 4, 5, 6, 9
Phishing 7, 12, 13
Plataforma 12, 13
Suplantación 7, 13
Vulnerabilidades 11