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, 01 de agosto de 2022

N° 207-2022-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

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 207	Fecha: 01-08-2022
		Página 04 de 13

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Vulnerabilidades, error crítico de Samba		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

En una publicación realizada a fines de julio por "Sophos", se menciona que un error crítico de Samba podría permitir que cualquiera se convierta en administrador de dominio.

ANTECEDENTES:

- Samba es un conjunto de herramientas de código abierto, que es ampliamente utilizado, no solo porque facilita que las computadoras Linux y Unix se comuniquen con las redes de Windows, sino que también permite alojar un dominio de Active Directory al estilo de Windows sin ningún servidor de Windows.
- Samba nació a principios de la década de 1990 gracias al arduo trabajo del pionero australiano de código abierto Andrew Tridgell, quien descubrió a partir de principios básicos cómo funcionaba SMB para poder implementar una versión compatible para Unix mientras estaba ocupado con su doctorado en el Australian National Universidad.

DETALLES:

- A continuación, se detallan los errores numerados CVE de samba.

CVE-2022-2031	Los usuarios de Samba AD pueden omitir ciertas restricciones asociadas con el cambio de contraseñas.
CVE-2022-32745	Los usuarios de Samba AD pueden bloquear el proceso del servidor con una solicitud de modificación o adición de LDAP.
CVE-2022-32746	Los usuarios de Samba AD pueden inducir un uso después de la liberación en los procesos del servidor con una solicitud de modificación o adición de LDAP.
CVE-2022-32742	Fuga de información de la memoria del servidor a través de SMB1.
CVE-2022-32744	Los usuarios de Samba Active Directory pueden falsificar solicitudes de cambio de contraseña para cualquier usuario

El último error **CVE-2022-32744** se considera grave, ya que los ciberdelincuentes podrían disputar el servicio de cambio de contraseña de Samba, conocido como ***kpasswd***, a través de una serie de intentos fallidos de cambio de contraseña, hasta que finalmente se acepte una solicitud de cambio de contraseña que fue autorizada por los propios ciberdelincuentes.

RECOMENDACIONES:

- Si usa la versión 4.16, actualice a la versión 4.16.4
- Si usa la versión 4.15, actualice a la versión 4.15.9
- Si usa la versión 4.14, actualice a la versión 4.14.14
- Si no puede actualizar, algunos de los errores enumerados anteriormente se pueden mitigar con cambios de configuración, cabe mencionar que algunos de esos cambios desactivan la funcionalidad en la que podría confiar su red, lo que le impediría utilizar esas soluciones alternativas particulares.

Fuentes de información	▪ hxxps://nakedsecurity.sophos.com/2022/07/27/critical-samba-bug-could-let-anyone-become-domain-admin-patch-now/ ▪ hxxps://www.samba.org/samba/history/samba-4.16.4.html ▪ Análisis propio de fuentes abiertas.

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 207	Fecha: 01-08-2022
		Página 05 de 13

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Error crítico de Confluence explotado en ataques		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	Software infectado, Enlaces de internet.		
Código de familia	C	Código de Subfamilia	C01
Clasificación temática familia	Código Malicioso		

Descripción

FECHA DEL EVENTO:

A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 31 de julio del 2022, se tomó conocimiento a través de la publicación realizada en la página web de **"BleepingComputer"**, que CISA ha agregado una vulnerabilidad crítica de Confluence rastreada como CVE-2022-26138 a su lista de errores abusados en la naturaleza, una falla que puede proporcionar a los atacantes remotos credenciales codificadas después de una explotación exitosa.

ANTECEDENTES:

Como reveló la firma de software australiana Atlassian la semana pasada, las versiones sin parches de la aplicación Questions for Confluence (instalada en más de 8,000 servidores) crean una cuenta con credenciales codificadas.

DETALLES:

Un día después de parchear la vulnerabilidad, la compañía notificó a los administradores que arreglaran sus servidores de inmediato, al ver que la contraseña codificada había sido encontrada y compartida en línea.

CISA agregó el CVE-2022-26138 a su catálogo de vulnerabilidades explotadas conocidas (KEV) basadas en evidencia de explotación activa.

La firma de ciberseguridad Rapid7 también publicó un informe el miércoles advirtiendo que la falla de seguridad ahora se explota activamente en la naturaleza, pero no compartió ninguna información sobre los ataques o indicadores de compromiso recopilados mientras los investigaba**.**

Como dice una directiva operativa vinculante (BOD 22-01) emitida en noviembre, todas las agencias de la Rama Ejecutiva Civil Federal (FCEB) tienen que proteger sus sistemas contra errores agregados al catálogo de vulnerabilidades explotadas conocidas (KEV) de CISA.

A pesar de que la directiva BOD 22-01 solo se aplica a las agencias federales de los Estados Unidos, CISA también insta encarecidamente a las demás organizaciones a corregir esta falla para frustrar los ataques contra los servidores vulnerables de Confluence.

Desde que se emitió esta directiva, CISA ha agregado cientos de errores de seguridad a su catálogo de errores explotados en ataques, ordenando a parchear sistemas vulnerables lo antes posible para evitar infracciones.

Asegurar los servidores de Confluence es particularmente importante dado que son objetivos atractivos, como lo demuestran los ataques anteriores con el ransomware AvosLocker y Cerber2021, el malware de botnet Linux y los criptomineros.

Fuentes de información	▪ https://www.bleepingcomputer.com/news/security/cisa-warns-of-critical-confluence-bug-exploited-in-attacks/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 207	Fecha: 01-08-2022
		Página 06 de 13

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:

1. **Facebook**

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.tw/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.sn/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.sk/
United States	2022-08-01	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.si/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.se/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.rs/
United States	2022-08-01	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.pt/
United States	2022-08-01	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.pe/
United States	2022-08-01	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.no/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.my/
United States	2022-08-01	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.mx/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.md/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.lu/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.li/
United States	2022-08-01	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.kr/
United States	2022-08-01	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.jp/
United States	2022-08-01	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.is/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.in/
United States	2022-08-01	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.ie/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.hu/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.hk/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.gr/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.fr/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.fi/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.dk/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.de/
United States	2022-08-01	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.cz/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.co.uk/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.co.nz/
United States	2022-08-01	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.com.uy/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.com.ng/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.com.es/
United States	2022-08-01	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.com.eg/

United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.com.ee/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.com.co/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.com.br/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.com.au/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.com.ar/
United States	2022-08-01	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.com/
United States	2022-08-01	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.co.ke/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.co.il/
United States	2022-08-01	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.co.id/
United States	2022-08-01	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.cl/
United States	2022-08-01	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.ch/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.ca/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.be/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.am/
United States	2022-08-01	142.250.176.193	xxxxs://freeuse2022.blogspot.al/
United States	2022-08-01	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.ae/
United States	2022-08-01	199.36.158.100	xxxxs://support-helpcenter785136190.web.app
United States	2022-08-01	199.36.158.100	xxxxs://support-helpcenter2168917101.web.app
United States	2022-08-01	199.36.158.100	xxxxs://support-helpcenter16893327.web.app

2. **Netflix**

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-08-01	172.67.206.16	xxxx://jacsonsveneers.com/inc/16c222aa19898e5058938167c8ab6c57
United States	2022-08-01	2606:4700:3036::6815:34f9	xxxxs://jacsonsveneers.com/inc/91299a41773c667d2ee8cddc3f6eeb64
United States	2022-08-01	2606:4700:3035::ac43:ce10	xxxx://jacsonsveneers.com/inc/e61eaa38aed621dd776d0e67cfeee366
United States	2022-08-01	2606:4700:3036::6815:34f9	xxxx://jacsonsveneers.com/inc/93ac0c50dd620dc7b88e5fe05c70e15b
United States	2022-08-01	104.21.52.249	xxxx://jacsonsveneers.com/inc/008bd5ad93b754d500338c253d9c1770

3. **Outlook**

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-08-01	2602:fea2:2::1	xxxxs://bafybeie6yngibwqd7doniyhqugst5nklcmmzo22mz6w25ranc5te6ak64y.ipfs.dweb.link/mb0012.html

4. **Microsoft Login**

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-08-01	2606:4700::6812:691	xxxxs://storageapi.fleek.co/2f4a1f94-b687-4425-bef5-f267994e37cb-bucket/mach/Personal.html
Desconocido	2022-08-01	103.153.183.146	xxxx://fraudb.info/ythtfdefefe/

5. **Interbank**

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-08-01	199.36.158.100	xxxxs://interbank-puntaje-crediticio.web.app/#/
United States	2022-08-01	199.36.158.100	xxxxs://interbank-puntaje-crediticio.firebaseapp.com/#/

- 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° 207	Fecha: 01-08-2022
		Página 09 de 13

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

Descripción

- El día 01 de agosto 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	c6cc559981229a1a4c06dbd94bc1fd1b31f405800515be464f3dfce7e64d766f	dll	nw_elf.dll
2	6944b970a39557b2982243eb0fe377841417ef7631fb53693f66629c01c6d3ea	exe	IMG-20022891.exe
3	4bfdb22134bc73b6b428c51e899f36da6ad72c54340cc4809c0f952cfd84cd22	xlsx	No Determinado
4	4b008c365160a9da811eb2c72882d4c5324bf81ef9f7656bc77573af00b9d1ea	exe	4b008c365160a9da811eb2c72882d4c5324bf81ef9f7656bc77573af00b9d1ea.exe
5	ca50cf18bdca3de3be48e5229590cf356e5e3f29361733b475fc15719d72d7f0	xlsx	ca50cf18bdca3de3be48e5229590cf356e5e3f29361733b475fc15719d72d7f0
6	b631cdf82500db83e4b298d4a16bac84e227162971f933c0117f4303ca8ae5f3	xlsx	No Determinado
7	20044bc3515379b70e4d42b57ff3ac32d5b590a0d185c8b5da2cea830f3368ed	xlsx	62e9a02d562d879475a0fe3ab0d3922e.xlsx.vir
8	2e72514a05ff383452a3dc1f1a8be040c3a1ebc23a224dc480064322efb85eb7	xlsx	dda7452a7d7110037e081d50b4207bca.xlsx.vir
9	921ed2a30e17fc6d7e9da74d64485ae8a40c95caa40e5108da51ad3c40599978	exe	921ed2a30e17fc6d7e9da74d64485ae8a40c95caa40e5108da51ad3c40599978.exe
10	c2349800849ad7b99ab8b9da1f0b1782c88ee09919a4e0df26e9bb3c20572121	jpeg	c2349800849ad7b99ab8b9da1f0b1782c88ee09919a4e0df26e9bb3c20572121.unknown
11	b3276f35d0b6666f9bb3f9bc1f3464cb979fd095728ceeb079c645e881a6725b	jpeg	b3276f35d0b6666f9bb3f9bc1f3464cb979fd095728ceeb079c645e881a6725b.unknown
12	05732e84de58a3cc142535431b3aa04efbe034cc96e837f93c360a6387d8faad	exe	05732e84de58a3cc142535431b3aa04efbe034cc96e837f93c360a6387d8faad.exe
13	8e980cd2f4f6fc7f92c7b45d4f0416adf36676d0fb346e8296695848246c4d35	exe	8e980cd2f4f6fc7f92c7b45d4f0416adf36676d0fb346e8296695848246c4d35.exe
14	010e32be0f86545e116a8bc3381a8428933eb8789f32c261c81fd5e7857d4a77	exe	010e32be0f86545e116a8bc3381a8428933eb8789f32c261c81fd5e7857d4a77.exe
15	98ac1117b23244bdc2e8132babd8da13ef8bff684db18312be31daa88c27fece	dll	98ac1117b23244bdc2e8132babd8da13ef8bff684db18312be31daa88c27fece.exe
16	5e97ccd8dafcb36b3cb772f6a2fd425abcf221ab9ea1930e8c2618c95332f2c6	dll	Bunifu.UI.dll
17	79a9e416da076f3c744e30c50d55a6b46cc2acdb54cbbab535663ba5b87c441b	dll	ClassLibrary1.dll
18	8f8deeea87c9beee4bb74139e72bc1635c27dfc3721f08564ee4a86f02335394	dll	ClassLibrary1.dll
19	e49c94732ee6f709c455bca51338207443ee0b56cd78bef901bebf27ac3d05b1	exe	unknown

- 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° 207**	**Fecha: 01-08-2022**
		Página 10 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades críticas en productos de IBM		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. Resumen:

Se ha reportado múltiples vulnerabilidades de severidad CRÍTICA de tipo denegación de servicio, validación de entrada incorrecta y exposición de información en varios productos de IBM. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto manipular la configuración del sistema y/o provocar una denegación de servicio (DoS). Asimismo, un usuario remoto autenticado podría obtener acceso a información confidencial.

2. Detalles:

- La vulnerabilidad de severidad **crítica** identificada como CVE-2022-35643 de denegación de servicio que afecta a IBM PowerVM VIOS, podría permitir a un atacante remoto manipular la configuración del sistema y/o provocar una denegación de servicio.
- La vulnerabilidad de severidad **media** identificada como CVE-2021-35561 de validación de entrada incorrecta en IBM DataPower Gateway, podría permitir a un atacante remoto no autenticado interrumpir el servicio. La vulnerabilidad existe debido a una validación de entrada incorrecta dentro del componente Utility en Oracle GraalVM Enterprise Edition. Un atacante remoto no autenticado puede aprovechar esta vulnerabilidad para interrumpir el servicio.
- La vulnerabilidad de severidad **baja** identificada como CVE-2022-22393 de divulgación de información que afecta a PowerVM NovaLink, podría permitir a un usuario remoto obtener acceso a información potencialmente confidencial. IBM PowerVM Novalink es vulnerable porque IBM WebSphere Application Server Liberty 1, con la función adminCenter-1.0 configurada, podría permitir que un usuario autenticado emita una solicitud para obtener el estado de los puertos HTTP/HTTPS a los que puede acceder el servidor de aplicaciones.

3. Productos afectados:

- IBM PowerVM VIOS, versión 3.1;
- IBM DataPower Gateway: versión 10.0.1.0, 10.0.1.1, 10.0.1.2, 10.0.1.3, 10.0.1.4, 10.0.1.5, 10.0.1.6, 10.0.1.7, 10.0.1.8, 10.0.2.0, 10.0.3.0, 10.0. 4.0, 10.5.0.0, 2018.4.1.0, 2018.4.1.1, 2018.4.1.2, 2018.4.1.3, 2018.4.1.4, 2018.4.1.5, 2018.4.1.6, 2018.4.1.7, 2018.4.1.8, 4.1.1.8, 2018.4.1.8, 4.1.1.8, 2018.4.1.8, 2018.4.1.8 2018.4.1.11, 2018.4.1.12, 2018.4.1.13, 2018.4.1.14, 2018.4.1.15, 2018.4.1.16, 2018.4.1.17, 2018.4.1.18, 2018.4.1.20, 2018.4.1.1;
- IBM PowerVM NovaLink, versión 2.0 - 2.0.3.

4. Solución:

- IBM recomienda actualizar los productos afectados con la última versión disponible que corrigen estas vulnerabilidades.

Fuentes de información	▪ hxxps://www.ibm.com/support/pages/node/6607886 ▪ hxxp://www.ibm.com/support/pages/node/6608166 ▪ hxxp://www.ibm.com/support/pages/node/6608546

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 207	Fecha: 01-08-2022
		Página 11 de 13

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de Phishing, que suplanta al aplicativo móvil Yape		
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. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que actores de amenazas vienen llevando a cabo una campaña de Phishing, suplantando al aplicativo móvil Yape, con la finalidad de mostrar al vendedor de haber realizado un supuesto pago con este aplicativo móvil.
2. Proceso del ataque phishing:

Imagen 1:

Ingresando a la URL fraudulenta redirige a esta ventana donde solicita la supuesta clave Yape (123***).

Imagen 2:

Una vez ingresado la contraseña, redirige a esta ventana, para luego escanear la QR de la posible víctima e introducir el monto a pagar.

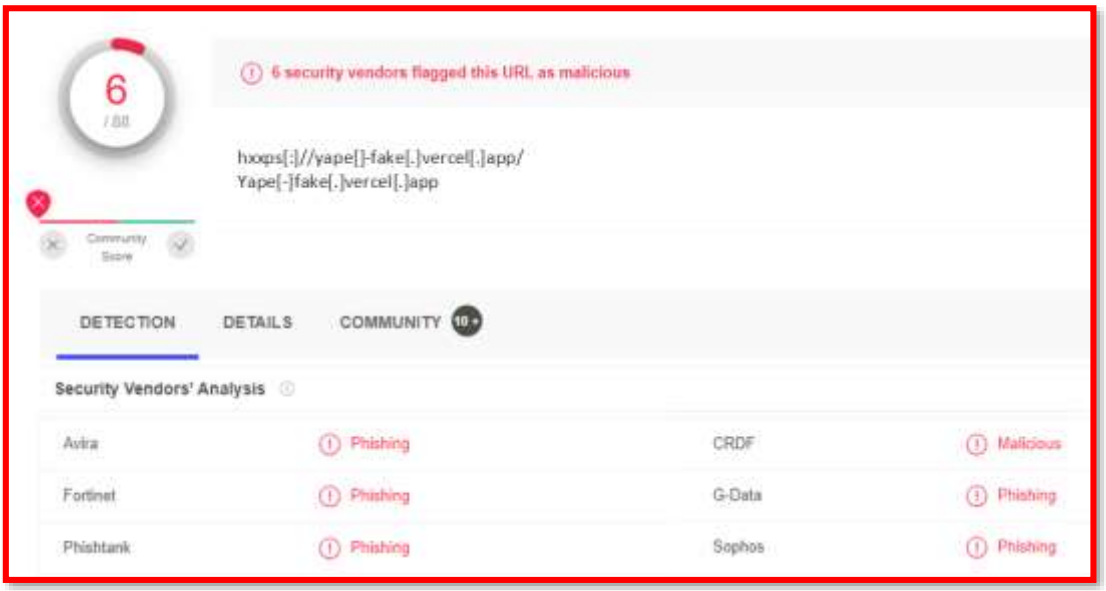
Imagen 3:

Por último, muestra esta ventana del supuesto yape efectuado a la posible víctima.

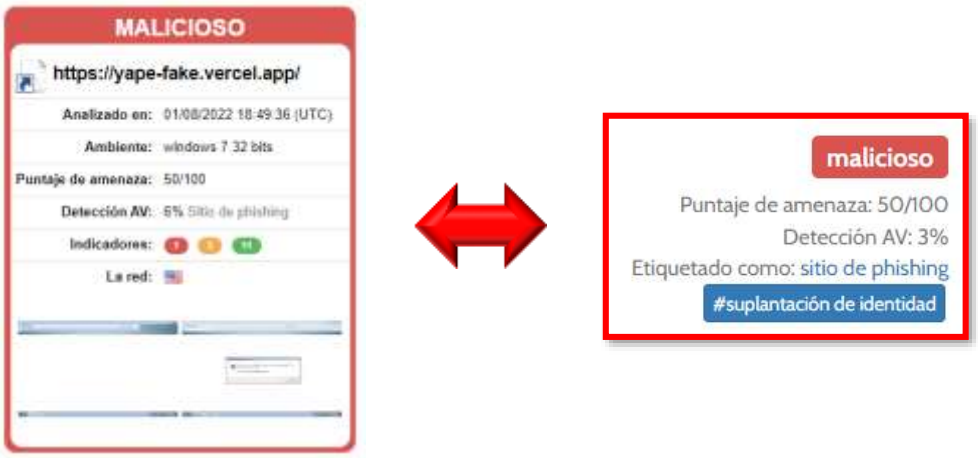
3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

- **INDICADORES DE COMPROMISO:**

  - ✓ **URL:** hxxps[:]//yape-fake[.]vercel[.]app/
  - ✓ **Dominio:** yape[-]fake[.]vercel[.]app
  - ✓ **IP:** 76[.]76[].21[.]241
  - ✓ **Código:** 404
  - ✓ **Longitud:** 1.13 KB
  - ✓ **SHA-256**: 2029bbc480472500c816780fe153581bde5177a49d3a2e2f1670aa7d263704f2



- **OTRAS DETECCIONES:**



4. **Recomendaciones:**
   - Confirmar el sitio web al que se ingresa sean los oficiales.
   - Verificar la redacción y ortografía de la URL.
   - Verificar la operación desde el aplicativo.
   - Evitar proporcionar información personal y/o bancaria en sitios webs fraudulentas.
   - Contar con una solución de seguridad, constantemente actualizada tanto en dispositivos de escritorio como en móviles, ya que sirven como barrera inicial protectora ante sitios web maliciosos.

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

Índice alfabético