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, 02 de agosto de 2022

N° 208-2022-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° 208	Fecha: 02-08-2022
		Página 04 de 17

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Atención, malware Qbot utiliza nuevas técnicas de evasión		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	Red, Internet		
Código de familia	C	Código de subfamilia	C09
Clasificación temática familia	Código Malicioso		

Descripción

En una publicación realizada en agosto por “Segu-info”, se menciona que el equipo de investigación de amenazas de Uptycs observó recientemente algunos cambios en el flujo de infección de Qbot.

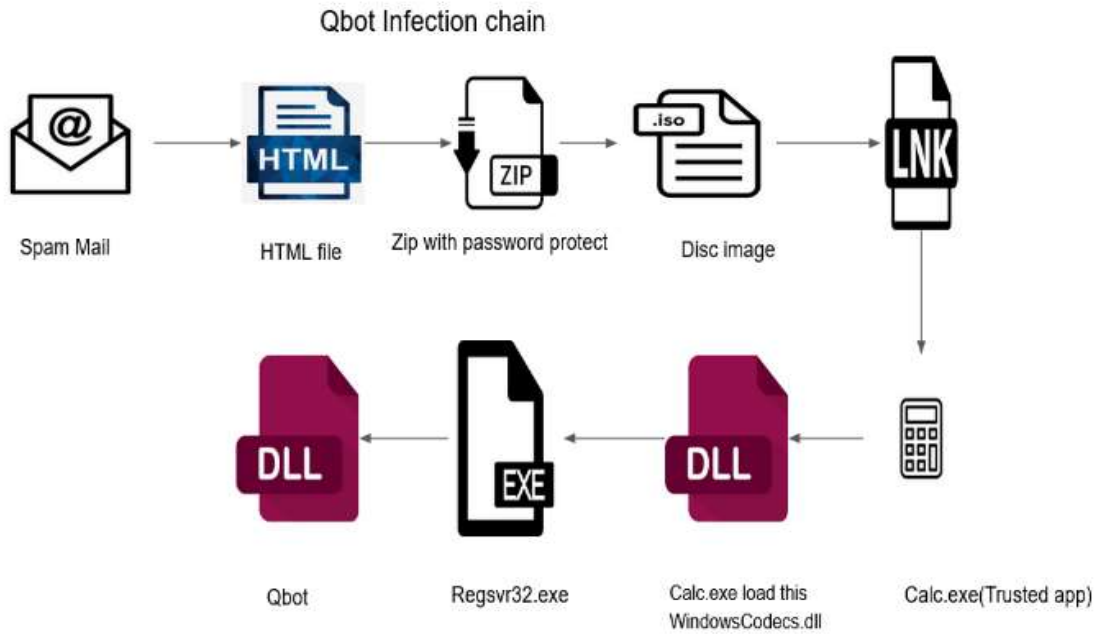
ANTECEDENTES:

- Qbot (también conocido como Qakbot o Pinkslipbot) es un troyano bancario que roba información confidencial de los equipos de las víctimas y la envía a un servidor de comando y control (C2). Esta amenaza fue identificada en 2007 y sigue activa con diferentes variantes.

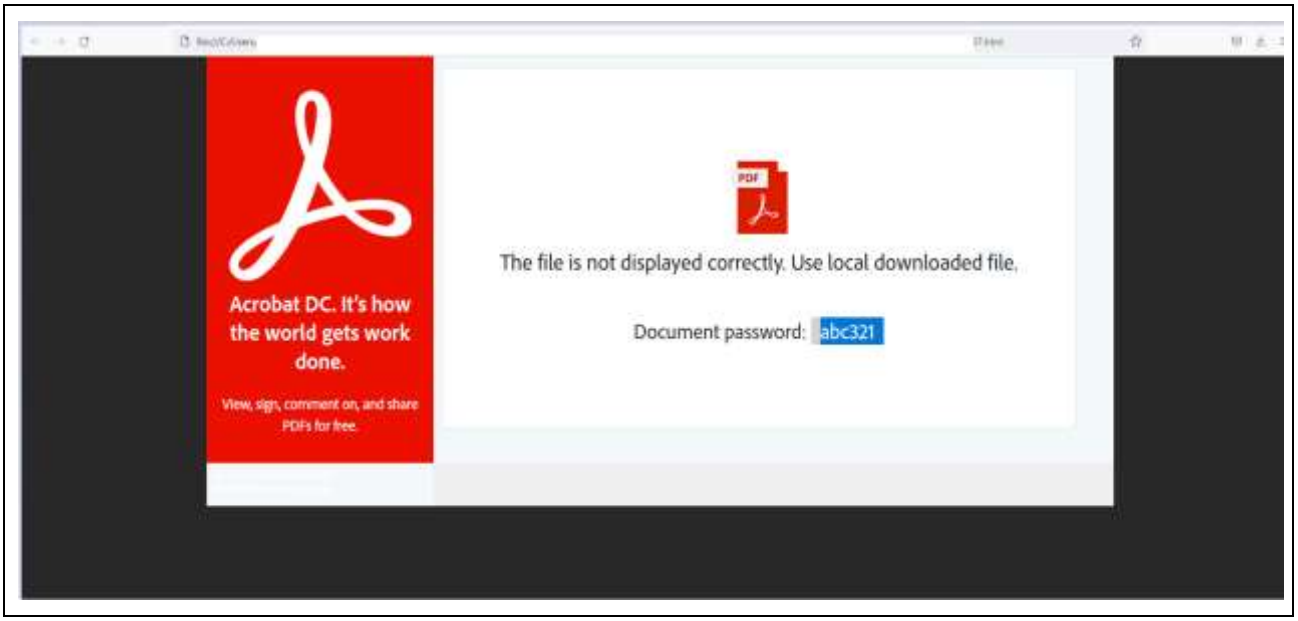
DETALLES:

- La manera de funcionamiento es un método de carga lateral de DLL para ejecutar código malicioso, el cual ayuda al malware a eludir los mecanismos de detección. Otra técnica que se ha en el binario de Qbot es la autodepuración (utilizando variables de entorno) que utiliza para comprobar si observado el sistema ya está infectado. Además, algunas versiones nuevas del binario Qbot apuntan al proceso wermgr[.]exe para inyectar el código malicioso.

  A continuación, se muestra la cadena de infección de las versiones más nuevas del binario Qbot.



- Se puede observar en el diagrama, la cadena de infección para los binarios más nuevos, que incluye aplicaciones confiables como calc[.]exe para carga lateral de DLL. Al abrir el archivo HTML que llega a través del correo electrónico no deseado, se descarga un archivo ZIP protegido con contraseña llamado "TXRTN_2636021[.]zip" en el sistema local. En la siguiente imagen de captura de pantalla se muestra la página HTML del correo electrónico no deseado.



- Al extraer el archivo ZIP usando la contraseña mencionada en la página HTML, se puede obtener un archivo ISO. El archivo ISO contiene lo siguiente:
  - Archivo LNK: TXRTN_8468190: este archivo LNK es el punto de activación de la ejecución.
  - WindowsCodecs[.]dll: nombre de archivo de Windows (nombre enmascarado) para ejecutar cargas maliciosas.
  - Calc[.]exe: Archivo de Windows legítimo con atributo oculto.
  - 102755[.]dll - Qbot DLL con atributo oculto.
- En la siguiente imagen de captura de pantalla se muestran los archivos dentro del archivo ISO.

Name	Date modified	Type	Size
102755.dll	7/11/2022 8:48 PM	Application exten...	687 KB
calc.exe	11/21/2010 8:55 AM	Application	758 KB
TXRTN_8468190	7/8/2022 6:15 PM	Shortcut	2 KB
WindowsCodecs.dll	7/11/2022 7:45 PM	Application exten...	5 KB

- Cuando se ejecuta el archivo LNK, se inicia el "Calc[.]exe" y se carga el archivo llamado "WindowsCodecs[.]dll", el cual contiene el código malicioso. Esto crea un nuevo proceso con la carga de malware "102755[.]dll" (archivo desarrollado en Delphi) y la siguiente línea de comando:

```
C[:]\Windows\Syswow64\regsvr32[.]exe 102755[.]dll
```

- Obteniendo la cadena de ejecución final, donde se muestra la cadena de procesos de Qbot:

```
cmd.exe (10504)                 Window... C:...  M... DESKTOP-KKQJ6... "C:\Windows\System32\cmd.exe" /q /c calc.exe
  Conhost.exe (9548)            Console... C:...  M... DESKTOP-KKQJ6... \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
  calc.exe (4364)               Window... E:...  M... DESKTOP-KKQJ6... calc.exe
    regsvr32.exe (8332)         Microso... C:...  M... DESKTOP-KKQJ6... C:\Windows\SysWOW64\regsvr32.exe 102755.dll
```

- De esta manera, el malware utiliza la técnica de carga lateral de DLL para ejecutar cargas maliciosas sin ser detectado, a menos que sepa lo que está buscando.

- Anteriormente, el malware Qbot intentaba inyectar contenido malicioso en cualquiera de los procesos de la siguiente lista:

%SystemRoot%\SysWOW64\Explorer[.]exe
%Raíz del sistema%\SysWOW64\OneDriveSetup[.]exe
%Raíz del sistema%\System32\OneDriveSetup[.]exe
%SystemRoot%\Explorer[.]exe
%SystemRoot%\SysWOW64\mobsync[.]exe
%SystemRoot%\System32\mobsync[.]exe
%Archivos de programa%\Internet Explorer\iexplorer[.]exe
%Archivos de programa(x86)%\Internet Explorer\iexplorer[.]exe
%SystemRoot%\SysWOW64\msra[.]exe
%SystemRoot%\System32\msra[.]exe

- Ahora, Qbot cambia la lista de procesos de destino a la siguiente:

C:\Windows\SysWOW64\wermgr[.]exe
C:\Windows\SysWOW64\msra[.]exe
C:\Archivos de programa (x86)\Internet Explorer\iexplore[.]exe

RECOMENDACIONES:

- Se debe contar con estrictos controles de seguridad.
- Se debe contar con estrictas soluciones de seguridad y visibilidad de varias capas para la identificación y detección de malware como Qbot.
- Se sugiere realizar un análisis de procesos utilizando reglas YARA, para detecciones avanzadas y la capacidad de correlacionar eventos de registro, eventos de archivos de procesos y eventos de API.

Fuentes de información	▪ hxxps://blog.segu-info.com.ar/2022/08/tecnicas-de-evasion-usadas-por-qbot[.]html ▪ hxxps://www.uptycs.com/blog/qbot-reappears-now-leveraging-dll-side-loading-technique-to-bypass-detection-mechanisms ▪ Análisis propio de fuentes abiertas.

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 208	Fecha: 02-08-2022
		Página 07 de 17

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Usan el antivirus Windows defender para encriptar computadoras con Lockbit Ransomware		
Tipo de ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros.		
Código de familia	C	Código de Subfamilia	C01
Clasificación temática familia	Código Malicioso		

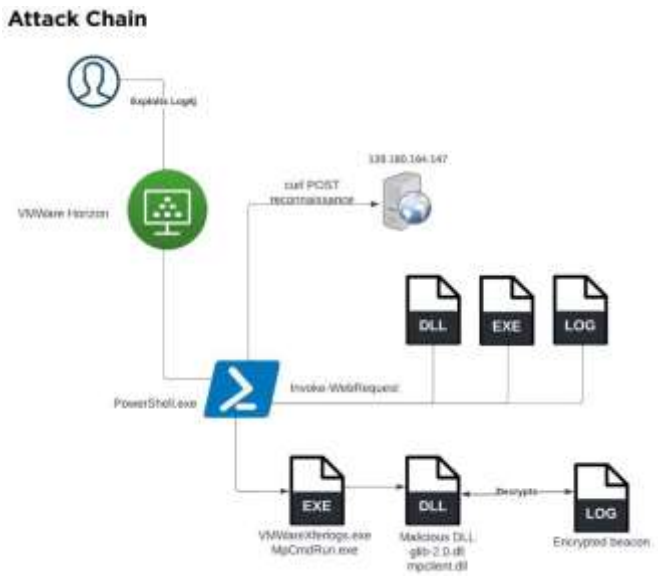
Descripción

FECHA DEL EVENTO:

A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 01 de agosto del 2022, se tomó conocimiento a través de la publicación realizada en la página web de "**SECURITYNEWSPAPER**", que los piratas informáticos han encontrado la forma de evadir la seguridad el programa Windows Defender, el antivirus más utilizado en la actualidad, y hacer que LockBit 3.0 , uno de los ransomware más peligrosos, secuestre todos los datos del ordenador e imposibilite su recuperación.

DETALLES:

- El ransomware es uno de los tipos de malware más peligrosos y difíciles de detectar. Cuando este malware llega al ordenador, por el medio que sea, lo primero que hace es instalarse en el sistema operativo y buscar la manera de evitar que el antivirus lo detecte cuando se ejecuta. Esto se puede hacer de varias formas, pero una de las más interesantes, descubierta recientemente, es aprovechar el uso de Cobalt Strike.



- Cobalt Strike es un conjunto de herramientas utilizadas en la piratería ética para realizar análisis de red sigilosos, así como moverse lateralmente dentro de una red, encontrar datos, cifrarlos y robarlos. Esta herramienta es legítima y los antivirus la reconocen, detectan y bloquean sin ningún problema. Sin embargo, los piratas informáticos detrás de este ransomware han encontrado una debilidad en MpCmdRun.exe Windows Defender. Gracias a él, es posible descargar e inyectar DLL maliciosas que inyectan balizas Cobalt Strike en el sistema.
- El proceso MpCmdRun.exe es responsable de ejecutar análisis programados en el sistema. Y para eso depende de una librería llamada "mpclient.dll". Los piratas informáticos han creado una biblioteca falsa, con el mismo nombre, que, al colocarla en la ruta de la original, logra que Windows Defender la ejecute. Y al hacerlo, permite que el ransomware permanezca oculto en el sistema.
- Los actores de amenazas estaban abusando de la herramienta de línea de comandos de Windows Defender MpCmdRun.exe para descifrar y cargar las cargas útiles de Cobalt Strike .

Signature Info

Signature Verification

Signed file, valid signature

File Version Information

Copyright	© Microsoft Corporation. All rights reserved.
Product	Microsoft® Windows® Operating System
Description	Microsoft Malware Protection Command Line Utility
Original Name	MpCmdRun.exe
Internal Name	MpCmdRun
File Version	4.18.1909.6 (WinBuild.160101.0800)
Date signed	2019-09-25 00:04:00 UTC

Signers

+ Microsoft Windows Publisher
+ Microsoft Windows Production PCA 2011
+ Microsoft Root Certificate Authority 2010

RECOMENDACIONES:

- Evitar descargar archivos de Internet de páginas web peligrosas, o cualquier cosa que nos llegue a través del correo electrónico.
- Utilizar otros antivirus como Kaspersky o McAfee.
- Realizar copias de seguridad de los archivos, de esta forma si nos infectan y roba nuestros datos, tendremos una vía de escape.
- Mantener actualizado el sistema operativo y máquinas virtuales

Fuentes de información	▪ https://www.securitynewspaper.com/2022/08/01/this-is-how-they-use-windows-defender-antivirus-to-encrypt-your-computer-with-lockbit-ransomware/ ▪ https://www.sentinelone.com/blog/living-off-windows-defender-lockbit-ransomware-sideloads-cobalt-strike-through-microsoft-security-tool/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 208	Fecha: 02-08-2022
		Página 09 de 17

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 02 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	abf3730a946a52f42f77ba736543e0bdc930ebf13b71fa30c52c9ffde890904f	zip	Bank_Slip.zip
2	55073d4f472762435d6b73d7ce4e5cd2bb2dd36edaac6fc4cf34bf73e90db29e	png	sxNWciS3
3	9e8ba78ecb96aa4c55d6ed670ded46ba0e6ca4442c844fcc760b856bb34254c2	zip	bT1t85w3hAsiVBo.rar
4	ee9d99a09e56c71072f7ea7e53d36d02e53d2e9dabd029fe0820fada596178b6	exe	百度一下.exe
5	01582bad45f7bb1d0f24be06cbb2c3d1beaba05f9f24c5b40de301fc2c690ba6	gzip	PO_NGOC_2022-08.img.gz
6	09d3b260c029280b24948447d47137bf75ff7a663bf7d9dc778976ab6e357d53	gzip	nuevo pedido 093301_1.gz
7	d7d406243f8a0316c45a6260a29aa4249c01ec282b1573d44273ef7557249735	rar	Company profile.arj
8	043e939409939a043f7afd1fb1e2a0ad88e19b7c7130f9f7e60f671a3f05b545	xlsx	Smart-Classroom-based-Training-Calendar-2022-Arabic.xlsx
9	d0f1632553759a56ff962ed91579589307521a023cfa82bbb8f917fb47a790e3	xlsx	Classroom-Based-Training-Calendar-2022-English-5.xlsx
10	c1d9cd1a9b253c9b556cbaa5e3ebe46fa4dffacaa1f18a67e44dcf2a4f61c628	docx	0
11	a09b48d84c87fe8fb0f3e4a85710073c83c488753a3f5d48023a626684f3b5bc	zip	PO # EOIM001054.zip
12	4404554216e02c6e89530b68d3ee93531c068aa0a9fee567247458f850d7f7f1	zip	Offer for sale.zip
13	667f1f255eb4638751cdb750fe26bd605c2140f9a774aea8da1949386ab0ed45	zip	667f1f255eb4638751cdb750fe26bd605c2140f9a774aea8da1949386ab0ed45
14	cd83ade470d06595302066a5fe404dfd43616dc627825fc7ea974eb98f4bec65	rtf	cd83ade470d06595302066a5fe404dfd43616dc627825fc7ea974eb98f4bec65.rtf
15	4551709351e9a10fc21e94cb18080936fe27bed584dffa9247cd6aaa967dc8ba	zip	UPDATED SOA.zip
16	796678f7a5d0ab9d2c1ee532149e79c384094e7c74a51076d6039b4e5d913664	zip	SHIPMENT DOCUMENT.zip
17	1bc84011fe99457d87d69b9817ec099e3f20cbf9e883dca9f4e7c1f9cf849024	zip	spinsworld.doc.07.13.zip
18	f9619c9398a8d36d4cb7a3ba6fd71965f7d8da448332b8f04af41a61939d9a3f	exe	WINSFX32
19	51a15b0ff200e0ea05f39d2d50f4248335dfe0c5eed15075be7dac96e5993bf5	xlsx	No Determinado
20	286d2d37851f998bcf50ac243efee0ce06570b68019a5040b54ef579a455f15f	doc	content.4337.13339.25102.32360.23038

21	24b5a6f61cb70702962d5a2f4971e55df7ae8292d29d2eb3844c5a335251f1cf	zip	PRE ALERT FINAL DOCS HBL & MBL.zip
22	c1e94377d54fca9b640937492d708006529ff97e74bd9305c9330c8612e00a82	android	No Determinado
23	f25e41bd84b2bf2e7db6cff8de4b4930cc1f11a156066c19fa8bb3e5c5d4d46d	exe	employee.exe
24	b993e78099aba6751bda3990691cc107dc6a424ded689f1d819e86f0569c47b9	exe	employee.pdf.exe
25	c5682f04ceb5fdbc3aaeaa3723f240afcd17236922a5e18e35ce9303de2c529e	dll	ETW.dll
26	666bcf13fc63a1a0ddbaca7b465adc7c3d36c232c0e96b31d4621662d7a1cbc0	rar	Valorant Hack.rar
27	4481199d948c453e962259c61e71293a0918080063e5282ce95e0a464eccaee1	zip	Setup.zip
28	81ae89d9796270678a807eb8a473439224a742ccae22dccc66c3d3464b05995a	exe	sys.exe
29	74b310e5d0a6fb3331a8827cc2423cf5282a25481bd7280f1f7a9393849a4915	lnk	8b4802cf257943e1184c5cc979f5bae0.lnk.vir
30	f5ee032e35a51ef924b9f09623887e09f59e9fa55b10eaf2901f81a9ae4b3781	exe	f5ee032e35a51ef924b9f09623887e09f59e9fa55b10eaf2901f81a9ae4b3781.exe
31	62f1cf982376342714020cc8b013b0cc3aa4e7c746e3a747e9e3071e751f8e2a	exe	62f1cf982376342714020cc8b013b0cc3aa4e7c746e3a747e9e3071e751f8e2a.exe
32	9bece7f8d5feaba8ae050d5126ac81600a1767809382263b7e1c370d1a448195	dll	kon4an.dll
33	73142c245e43c79909df91cc6713f019b62e0d626f995af47d5dbe2f52c22ebc	exe	73142c245e43c79909df91cc6713f019b62e0d626f995af47d5dbe2f52c22ebc.exe
34	b272e8e8ffe0f39e02eb7dcbda676eb53dc20697d0811b1abbfb7bd04895cec7	exe	08-01-203902.exe
35	033d94dec0a57e5c3fbd940a059199d3e555996f2d7fcd6f3713b9a3b05a5d6e	exe	08-01-022710.exe

- 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

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 208	Fecha: 02-08-2022
		Página 11 de 17

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
Vietnam	2022-08-02	125.212.224.192	xxxxs://www.reactivate-page-76845980.click
Vietnam	2022-08-02	210.245.90.209	xxxxs://confirm-page-12345678956.click
Vietnam	2022-08-02	125.212.224.192	xxxxs://www.reactivate-page-76845980.click/
Vietnam	2022-08-02	210.245.90.209	xxxxs://confirm-page-12345678956.click/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.tw
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.sk
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.si
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.se
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.rs
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.no
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.mx
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.md
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.li
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.kr
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.is
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.hk
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.gr
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.fr
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.fi
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.cz
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.com.uy
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.com.es
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.com.eg
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.com.ee
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.com.br
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.com.au
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.co.ke
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.co.il
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.cl
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.ch
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.ca

United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.am
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.al
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.tw/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.sn/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.sk/
United States	2022-08-02	2607:f8b0:4006:81c::2001	xxxxs://freeuse2022.blogspot.si/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.se/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.rs/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.my/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.md/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.lu/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.li/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.in/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.hu/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.hk/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.gr/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.fr/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.fi/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.dk/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.de/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.co.uk/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.co.nz/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.com.ng/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.com.es/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.com.ee/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.com.co/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.com.br/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.com.au/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.com.ar/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.co.il/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.ca/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.be/
United States	2022-08-02	142.250.176.193	xxxxs://freeuse2022.blogspot.am/

2. **Google**

PAIS DE PROCEDENCIA	FECHA	IP	URL
Desconocido	2022-08-02	91.240.118.57	xxxx://karmdal.com/index/?47UONs2jQS
Norway	2022-08-02	138.124.183.254	xxxxs://trusting-hofstadter.138-124-183-254.plesk.page/sfr/Espace%20Client%20SFR%20-%20Gestion%20de%20mon%20compte%20SFR.php
United States	2022-08-02	67.207.93.131	xxxxs://api.perucpe.com/sfr/Espace%20Client%20SFR%20-%20Gestion%20de%20mon%20compte%20SFR.php

3. **Icloud**

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-08-02	108.171.195.135	xxxx://www.apple.com-is.cloud/find/
United States	2022-08-02	108.171.195.135	xxxx://www.apple.com-is.cloud/
United States	2022-08-02	108.171.195.135	xxxxs://www.apple.com-is.cloud/index.asp

4. **Outlook**

PAIS DE PROCEDENCIA	FECHA	IP	URL
Germany	2022-08-02	185.110.188.62	xxxxs://learnmma.net/wp-admin/js/ow/ow/auth/logon.aspx?replaceCurrent=1&reason=2&url=brad.guillot@bedbath.com
United States	2022-08-02	2606:4700::6812:ae07	xxxxs://bf92f294.sibforms.com/serve/MUIEAHStgSAatRl_S5DuF1N_kIM7Uw-A8vwoTEU34f3OaanIyyoReiAMeDx-qERAExnkEqGT_mcFcfivClHt5ksp66ayywNiuoxhBEJTIf1wtMpRw2c6czxsYSy_KDpaOISyYpOv7O9sRoB6HzwooJcovJssvbcXpB6FhPZtmTae09QPDLfOJlYgOZGRT_WseqDSDVCQ3YyDyoVf
United States	2022-08-02	2606:4700::6812:9207	xxxxs://5b15fe32.sibforms.com/serve/MUIEADECzYKdVtlFO-If4-55cBmb-dp7kRCNGY9I1-fZXv-oWV_YXEkYw4yVofossVZF-OPMP86dseJYABurNDIf4CZA9jRa81NkMLgHtr_UpIIFHdpp8uXge3IYv47GKpESGV24eWR5sNxUVJFImeHcim3OvopDu3x3c3RJunY4iKpYDPPjTdPjD2Tvhvm3NPy49JUxWMB5jFzC
United States	2022-08-02	2606:4700::6812:9207	xxxx://6353c80e.sibforms.com/serve/MUIEACUu3YgBQRv1zNcmC6-poQM9YLVQcToEi8rChIUelzI4kyUsJDgqAoNW585uO2pmfjxwQuwSe8xj3ag5wZ1kUllx69DndCZEyrBJBLisjP93T81j2AmqLg6pFIxlAQnDPv06nKBvYy1p9J9DC6jEOZilig8rEb21rwlsHEr8TQYZzdCsBl6mnqkq7KLl-Q9t5NNhBp8ZwSdH
Germany	2022-08-02	194.163.171.127	xxxx://worldbethub.com/arsmtp
Germany	2022-08-02	194.163.171.127	xxxxs://vibrantlivenews.com/arsmtp
United States	2022-08-02	2602:fea2:2::1	xxxxs://bafybeic4vnkmumdevxc7fniiq4hl4trbw64wwsnx2ir4yw4mnnkul6syzm.ipfs.dweb.link/v5.htm
United States	2022-08-02	209.94.90.1	xxxxs://bafybeibcf35wpfiunhrfs2rbcv4ys2soooib2hdxa67y64sm7qsmcq4at4.ipfs.dweb.link/20.html
United States	2022-08-02	2606:4700::6812:ae07	xxxx://6353c80e.sibforms.com/serve/MUIEACUu3YgBQRv1zNcmC6-poQM9YLVQcToEi8rChIUelzI4kyUsJDgqAoNW585uO2pmfjxwQuwSe8xj3ag5wZ1kUllx69DndCZEyrBJBLisjP93T81j2AmqLg6pFIxlAQnDPv06nKBvYy1p9J9DC6jEOZilig8rEb21rwlsHEr8TQYZzdCsBl6mnqkq7KLl-Q9t5NNhBp8ZwSdH/
United States	2022-08-02	2606:4700::6812:ae07	xxxxs://6353c80e.sibforms.com/serve/M

			UIEACUu3YgBQRv1zNcmC6-poQM9YLVQcToEi8rChIUelzI4kyUsJDgqAoNW585uO2pmfjxwQuwSe8xj3ag5wZ1kUlIx69DndCZEyrBJBLisjP93T81j2AmqLg6pFIxlAQnDPv06nKBvYy1p9J9DC6jEOZilig8rEb21rwlsHEr8TQYZzdCsBl6mnqkq7KLl-Q9t5NNhBp8ZwSdH
United States	2022-08-02	209.94.90.1	xxxxs://bafybeibcf35wpfiunhrfs2rbcv4ys2soooib2hdxa67y64sm7qsmcq4at4.ipfs.dweb.link/20.html#xx@xx.com
United States	2022-08-02	104.18.146.7	xxxxs://fc3ff5c1.sibforms.com/serve/MUIEAELmbPL-C_bpcOPz88dZ5juHj8Ij2ICdKIKfioZ9nbLzhrCkxtFbOv4mvobGzQf-vuNB4H5g2SJlpMHcmwlgEtWN8-Wj1dlU7193riOqn8hJr3qwBm18IK9ymZn5uD0h1WZ7lqRFNgVpO4zRt9tpcnHmQNZQK7F_r1zxjg3e8EP8x5IQhhSZAnwIWYyVW74yb-wOwMV3BV1h

5. **WhatsApp Group Invite**

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-08-02	20.25.137.39	xxxx://kvq.jmyg.tk/FZxhmcjssKedelvaUFWl6s0
United States	2022-08-02	20.25.137.39	xxxx://kvq.jmyg.tk/FZxhmcjssKedelvaUFWl6s0/

6. **Microsoft Login**

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-08-02	2606:4700::6812:691	xxxxs://storageapi.fleek.co/e53b2d0a-594e-4aa4-b1c9-05895fa66700-bucket/Newest.html
United States	2022-08-02	142.4.10.233	xxxxs://ospasjx3.tk/office/msft
United States	2022-08-02	131.153.37.18	xxxx://erralkullamn.icu/ny
United States	2022-08-02	72.47.208.90	xxxxs://lisarobertson.com/wp-includes/certificates/schlesingergroup/Noo-Reply/?email=
United States	2022-08-02	131.153.37.18	xxxx://erralkullamn.icu/ny/
United States	2022-08-02	2606:4700::6812:691	xxxxs://storageapi.fleek.co/2f4a1f94-b687-4425-bef5-f267994e37cb-bucket/mach/Personal.html

7. **Office 365**

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-08-02	162.214.69.46	xxxxs://autovidrosemcampinas.com.br/invv2022/purchaseorder57477/office.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

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 208**	**Fecha: 02-08-2022**
		Página 15 de 17

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad de omisión de autenticación en Cisco		
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:

Cisco ha reportado una vulnerabilidad de severidad CRÍTICA de tipo autenticación incorrecta en la funcionalidad de autenticación externa de Cisco Email Security Appliance (ESA) y Cisco Secure Email and Web Manager. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado omitir la autenticación e iniciar sesión en la interfaz de administración basada en la web del dispositivo afectado.

2. Detalles:

- La vulnerabilidad de severidad **crítica** identificada como CVE-2022-20798 de autenticación incorrecta en la funcionalidad de autenticación externa de Cisco Secure Email y Web Manager, anteriormente conocido como Cisco Security Management Appliance (SMA), y Cisco Email Security Appliance (ESA) podría permitir a un atacante remoto no autenticado omitir la autenticación e iniciar sesión en la interfaz web de gestión de un dispositivo afectado.
- Esta vulnerabilidad se debe a la comprobación de autenticación incorrecta cuando un dispositivo afectado utiliza el protocolo ligero de acceso a directorios (LDAP) para la autenticación externa. Un atacante podría aprovechar esta vulnerabilidad al ingresar una entrada específica en la página de inicio de sesión del dispositivo afectado. Una explotación exitosa podría permitir a un atacante obtener acceso no autorizado a la interfaz de administración basada en la web del dispositivo afectado.

3. Productos afectados:

Esta vulnerabilidad afecta a Cisco ESA y Cisco Secure Email y Web Manager, tanto en dispositivos virtuales como de hardware, si ejecutan una versión vulnerable del software Cisco AsyncOS (versión 11 y anteriores, 12, 12.8, 13, 13.6, 13.8, 14 y 14.1) y se cumple las siguientes condiciones:

- Los dispositivos están configurados para usar autenticación externa (La autenticación externa está deshabilitada de forma predeterminada);
- Los dispositivos utilizan LDAP como protocolo de autenticación.

4. Solución:

- CISCO recomienda actualizar los productos afectados con la última versión fija disponible que corrige esta vulnerabilidad. Cabe indicar, que las versiones del software Cisco AsyncOS anteriores a la versión 11 han llegado al final del mantenimiento del software. Por ello, se recomienda migrar a una versión compatible que incluya la solución para esta vulnerabilidad;
- Asimismo, existe una solución alternativa que aborda esta vulnerabilidad. Los administradores pueden deshabilitar los enlaces anónimos en el servidor de autenticación externa. Esta acción debe realizarse en el servidor que maneja la autenticación externa. Los administradores deben trabajar con sus equipos de red para implementar esta solución alternativa. Cisco indicó que, la función de autenticación externa proporcionada por los dispositivos Cisco Secure no debería verse obstaculizada por esta solución alternativa.

Fuentes de información	▪ hxxps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-esa-auth-bypass-66kEcxQD ▪ hxxps://cve.report/CVE-2022-20798

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 208**	**Fecha: 02-08-2022**
		Página 16 de 17

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades críticas en varios producto VMware		
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:

VMware ha reportado múltiples vulnerabilidades de severidad CRÍTICA de tipo omisión de autenticación, ejecución remota de código de inyección JDBC, escalada de privilegios locales, ejecución remota de código de inyección SQL, inyección de URL, cruce de ruta y secuencias de comandos entre sitios (XSS) que afecta a varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante u actor de amenaza con acceso de red a la interfaz de usuario obtener acceso administrativo sin necesidad de autenticarse, escalar privilegios a nivel de usuario "root", redirigir a un usuario autenticado a un dominio arbitrario, acceder a archivos arbitrarios, inyectar código javascript en la ventana del usuario de destino y desencadenar una ejecución remota de código.

2. Detalles:

- La vulnerabilidad de severidad **crítica** identificada como CVE-2022-31656 de omisión de autenticación en VMware Workspace ONE Access, Identity Manager y vRealize Automation que afecta a los usuarios del dominio local, podría permitir a un atacante con acceso de red a la interfaz de usuario obtener acceso administrativo sin necesidad de autenticarse.
- Las vulnerabilidades de severidad **alta** identificadas como CVE-2022-31660, CVE-2022-31661 y CVE-2022-31664 de escalada de privilegios locales en VMware Workspace ONE Access, Identity Manager y vRealize Automation podrían permitir a un atacante con acceso local escalar privilegios a nivel 'root'.
- La vulnerabilidad de severidad **alta** identificada como CVE-2022-31659 de ejecución remota de código de inyección SQL en VMware Workspace ONE Access e Identity Manager podría permitir a un atacante con acceso de administrador y de red puede desencadenar una ejecución remota de código.
- Las vulnerabilidades de severidad **alta** identificadas como CVE-2022-31658 y CVE-2022-31665 de ejecución remota de código de inyección JDBC en VMware Workspace ONE Access, Identity Manager y vRealize Automation podría permitir a un atacante con acceso de administrador y de red desencadenar una ejecución remota de código.
- Las vulnerabilidades de severidad media han sido identificadas como: CVE-2022-31657, CVE-2022-31662 y CVE-2022-31663.

3. Productos afectados:

- VMware Workspace ONE Access (Access)
- VMware Workspace ONE Access Connector (Access Connector)
- VMware Identity Manager (vIDM)
- VMware Identity Manager Connector (vIDM Connector)
- VMware vRealize Automation (vRA)
- VMware Cloud Foundation
- vRealize Suite Lifecycle Manager

4. Solución:

- VMware recomienda actualizar los productos afectados con la última versión fija disponible que corrige estas vulnerabilidades.

Fuentes de información	▪ hxxps://www.vmware.com/security/advisories/VMSA-2022-0021.html ▪ hxxps://kb.vmware.com/s/article/89096 ▪ hxxps://kb.vmware.com/s/article/89084

Índice alfabético