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, 03 de agosto de 2022

N° 209-2022-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

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 209	Fecha: 03-08-2022
		Página 04 de 15

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Piratas informáticos chinos utilizan el nuevo marco de piratería de Manjusaka similar a Cobalt Strike		
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

A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 02 de Agosto del 2022, se tomó conocimiento sobre un nuevo marco ofensivo llamado Manjusaka al que llaman "hermano chino de Sliver y Cobalt Strike".

MARCO DE ATAQUE:

El implante de malware es una familia RAT llamada "Manjusaka". El C2 es un binario ELF escrito en GoLang, mientras que los implantes están escritos en el lenguaje de programación Rust, que consta de una variedad de capacidades que se pueden usar para controlar el punto final infectado, incluida la ejecución de comandos arbitrarios. Descubrimos las versiones EXE y ELF del implante. Ambos conjuntos de muestras que atienden a estas plataformas consisten en casi el mismo conjunto de funcionalidades RAT y mecanismos de comunicación.

CAPACIDADES DEL IMPLANTE:

El implante consiste en una multitud de capacidades de troyanos de acceso remoto (RAT) que incluyen algunas funciones estándar y un módulo de administración de archivos dedicado.

- Ejecutar comandos arbitrarios: el implante puede ejecutar comandos arbitrarios en el sistema usando " cmd.exe /c ".
- Obtener información de archivo para un archivo específico: hora de creación y última escritura, tamaño, número de serie del volumen e índice de archivo.
- Obtener información sobre las conexiones de red actuales (TCP y UDP) establecidas en el sistema, incluidas las direcciones de red local, las direcciones remotas y los ID de proceso (PID) propietarios.
- Recopilar las credenciales del navegador: Específicamente para navegadores basados en Chromium usando la consulta: SELECT signon_realm, username_value, password_value FROM logins ; Navegadores objetivo: Google Chrome, Chrome Beta, Microsoft Edge, 360 (Qihoo), QQ Browser (Tencent), Opera, Brave y Vivaldi.
- Recopilar información de SSID de Wi-Fi, incluidas las contraseñas, mediante el comando: netsh wlan show profile <WIFI_NAME> key=clear
- Tomar capturas de pantalla del escritorio actual.
- Obtener información completa del sistema desde el punto final, que incluye:
  - Información global de la memoria del sistema.
  - Información de potencia del procesador.
  - Lecturas de temperatura actual y crítica de WMI usando " SELECT * FROM MSAcpi_ThermalZoneTemperature "
  - Información sobre las interfaces de red conectadas al sistema: Nombres
  - Tiempos de proceso y sistema: tiempo de usuario, tiempo de salida, tiempo de creación, tiempo de kernel.
  - Nombres de los módulos de proceso.
  - Información del disco y la unidad: número de serie del volumen, nombre, nombre de la ruta raíz y espacio libre en el disco.
  - Nombres de cuentas de red, grupos locales.
  - Números de compilación y versión principal de Windows.

CADENA DE CONTAGIOS:

También descubrimos una campaña relacionada que consistía en la distribución de un maldoc a objetivos que conducían al despliegue de balizas Cobalt Strike en los sistemas infectados.

La cadena de infección implica el uso de un maldoc disfrazado de informe y aviso sobre la pandemia de COVID-19 en la ciudad de Golmud, una de las ciudades más grandes de la prefectura autónoma mongola y tibetana de Haixi, provincia de Qinghai, citando específicamente un caso de COVID-19. y el seguimiento posterior de los contactos de las personas.

格尔木市新型冠状病毒感染的肺炎疫情防控处置工作指挥部通告

（第 32 号）

2022 年 3 月 17 日，格尔木市排查出一名昔口市确诊病例的密切接触者在我市活动。目前，该密接及已追踪到在格尔木市次密接人员均已落实集中隔离管控措施，首次核酸检测结果均为阴性。经流行病学调查，现将此密切接触者抵格后活动轨迹公布如下：

3 月 14 日，董某某 21：50 乘坐西宁至格尔木的 Z6811 次列车（座位号：加 1 车 01 下铺）。

3 月 15 日，凌晨 4：38 到达格尔木，出火车站后步行至黄河宾馆，登记入住 3330 房间。08：30 从黄河宾馆步行至市第二人民医院体检，11：30 体检结束后返回黄河宾馆。12：00 在黄河宾馆后院的平房食堂内就餐，12：30 返回房间。18：00 在宾馆后院的平房食堂内就餐，19：00 至 22：00，在宾馆二楼会议室开会，会后返回房间未外出。

3 月 16 日，早上 08：00 在宾馆后院的平房食堂内就餐，餐后乘坐公司皮卡车前往雪水河附近工地（南山口附近）工作，11：30 返回黄河宾馆，12：00 在宾馆后院的平房食堂内就餐。13：30 自宾馆步行至铁东社区报备（报备时"双码"正常不带星号），14：10 自铁东社区步行至市第二人民医院采集核酸，15：40 步行至中山路源峰综合批发市场，自东门进入市场，在源峰市场长平百货购买推子，后在源峰市场艳阳霞行购买物品，随后步行返回黄河宾馆，18：00 在宾馆后院的平房食堂内就餐。18：40 自黄河宾馆步行前往铁路市场中段马建精品水果超市购买水果，19：30 返回黄河宾馆，19：40 至 23：00 期间在黄河宾馆 3303 房间洗衣服，后返回 3330 房间未外出。

RECOMENDACIONES:

- La disponibilidad del marco ofensivo de Manjusaka es una indicación de la popularidad de las tecnologías ofensivas, sin embargo, está escrito en los lenguajes de programación más modernos y portátiles. El desarrollador del marco puede integrar fácilmente nuevas plataformas de destino o versiones más exóticas de Linux como las que se ejecutan en dispositivos integrados.
- Debemos ser diligentes frente a herramientas y marcos tan fácilmente disponibles que pueden ser mal utilizados por una variedad de actores de amenazas. Las estrategias de defensa en profundidad basadas en un enfoque de análisis de riesgos pueden ofrecer los mejores resultados en la prevención. Sin embargo, esto siempre debe complementarse con un buen plan de respuesta a incidentes que no solo haya sido probado con ejercicios de simulación y revisado, sino mejorado cada vez que se ponga a prueba en compromisos reales.

Fuentes de información	▪ https://thehackernews.com/2022/08/chinese-hackers-using-new-manjusaka.html ▪ https://blog.talosintelligence.com/2022/08/manjusaka-offensive-framework.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 209	Fecha: 03-08-2022
		Página 06 de 15

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 03 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	df50e9ae62a46bda93ff03d76b707d574a3803754a782e21e4b9ef547f7ca32e	exe	516.dll
2	517b37b47dc15abc5ae733109d178dde2e34a6f0cc3d9f93b1869c3c576b3d76	exe	No Determinado
3	7ec1d0796cb4163cec686ae4f9c0b0b8e8ae5572cebcea472616e99552042d20	exe	No Determinado
4	ac64e343753c2912dedf804bcb0202cf2aee410b77e52dfb6fae9c0ea610ccbc	exe	3a0e88b8460abe668ad29c2ca29bfedc.virus
5	464cc5b5b281c2e7fbf8a4b5b944243605c71cbbeb97faff10bdd6d89951dc3f	exe	No Determinado
6	9aaa46606f36b7f4b26420e95a75090d1a933356e994ca69d3af6bb4c3774430	exe	超导体.exe
7	49c51e75d38997d19b9873f86b832631dbe4f5e48260240bbd89530bd8f7b439	exe	vibran_drv.sys
8	999e537d3fe2789a074121cee8f83d6858ca7d0baf7b54e6e24ed5f91a231444	dll	ServerDll.dll
9	a6e439d10a521e60b7e18f6a43e59049399ce3421009910c30ae7076384b3c29	xls	update.xls
10	f44f6fbfc891bec5aaece28be3e010289e8c067389863110a9ea493c175a342e	7zip	f44f6fbfc891bec5aaece28be3e010289e8c067389863110a9ea493c175a342e.7z
11	f72b6eb053f427e2793bd12ab6bae781f2eb868561cc547dc0a17aa9fb32b5a4	rar	Glxfra.z
12	905dcd26038c83f0df03e9e2db563cdeec5a4cdf4aad7c5b507bf3c84371e225	zip	QNLNSAHMD2202897.zip
13	82881470b86dcb38d12ad34c10d5e1339aad98ef7e3bcc1537d78819eaf25229	exe	Silent.exe
14	ff4600c517b34b5d9c2cfa695122f5a9d1f78c84e8f9c3bb77d46d4b6691dd4b	pdf	1.pdf
15	2b2ffb9a2fbf1673da80d3fee086132999593b681c2dda9c666722d627551c33	powershell	163286975
16	8d376c08a62e613b59f43b9be243b71b352d74bb22467be6581a3483d936cc9a	zip	8d376c08a62e613b59f43b9be243b71b352d74bb22467be6581a3483d936cc9a
17	841e619a0e57780663987feaaac1e623160cd534aa263c563423edcb91cafcc6	exe	quietmoth (3).exe
18	8ffa991a360615cf36fcc297769617e36c8665308808419362830e49ab028155	exe	8ffa991a360615cf36fcc297769617e36c8665308808419362830e49ab028155.exe
19	82a01540546ff4201dd98d45d0b7cfa5a56a00485add894e6b493afc23132e9a	exe	unknown
20	eae0ae4e59805b02e90bddcdb364e3efc2472b2527ee34508552ec3e0a65445c	dll	unknown

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

Fuentes de información	▪ Comandancia de Ciberdefensa de la Marina, Osint

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 209	Fecha: 03-08-2022
		Página 07 de 15

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	G
Clasificación temática familia	Fraude		

Descripción

1. 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:

a. Facebook

PAIS DE PROCEDENCIA	FECHA	IP	URL
Russia	2022-08-03	178.159.36.31	xxxxs://2021-deutschland-de-zdf.xyz
Russia	2022-08-03	178.159.36.31	xxxxs://2021-deutschland-de-zdf.xyz/
United States	2022-08-03	149.102.154.128	xxxxs://one.praneshprayaag.com/login.php
United States	2022-08-03	149.102.154.128	xxxxs://one.praneshprayaag.com/incorrect_password.php
United States	2022-08-03	149.102.154.128	xxxxs://one.praneshprayaag.com/?check=

b. Instagram

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-08-03	2600:1f18:2489:8200:32de:9a3c:e401:d649	xxxxs://instagramfourm.netlify.app
United States	2022-08-03	2600:1f18:2489:8200:a007:6646:1f31:908c	xxxxs://instagramfourm.netlify.app/

c. Google

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-08-03	2600:1f18:43d1:2a02:b6ee:327b:545e:e578	xxxxs://0rq8e.bemobtrcks.com/go/17619c9d-d2ec-4a2e-aedf-d99ba442e8a7
Desconocido	2022-08-03	91.240.118.107	xxxx://life-in-the-stix.com/index/?TuWKFctxls

d. Netflix

PAIS DE PROCEDENCIA	FECHA	IP	URL
France	2022-08-03	62.210.219.95	xxxxs://securis-pass-sd.on-the-web.tv/de/de
France	2022-08-03	62.210.219.95	xxxxs://securis-pass-sd.on-the-web.tv/de/de/

e. Interbank

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-08-03	199.36.158.100	xxxxs://interbank--pe.web.app/#/
United States	2022-08-03	2620:0:890::100	xxxxs://cuenta-millonaria-interbank.web.app/#/
United States	2022-08-03	2620:0:890::100	xxxxs://cuenta-millonaria-

			interbank.firebaseapp.com/#/

f. Outlook

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-08-03	5.254.40.27	xxxx://8g025045jtanengve63jb8eq7puo5o95090gv07tru4l4ps9en49298.siasky.net
United States	2022-08-03	216.52.183.170	xxxx://8g0d30icpdk895onci0aesi9k9l4t2jn2r1epqpuulldd9g99ks3378.siasky.net/
United States	2022-08-03	162.244.80.49	xxxx://8g09adk7aoc3ia9i9pvcrfdsc3nnba5uo35cectv6dgim85677739c8.siasky.net/
United States	2022-08-03	5.254.40.27	xxxx://8g025045jtanengve63jb8eq7puo5o95090gv07tru4l4ps9en49298.siasky.net/
United States	2022-08-03	2606:4700::6812:9207	xxxx://103168d8.sibforms.com/serve/MUIEAA4C_io2OJp_p1_ccTO7fSyQsqLtXztfT1f0JTpEdNdNObQ05rEtdoTeaPflsMBBwmuDQeyuoSDJMqDsgFV5-586YdvQB-jbkjdH7iyugEE71DdybozJo5GnY5xqqwPc4FnaLjaXTyK7BdApP7Du1ITnolZj7kiNjI8Li2nICLDSqFZ46uA6WxrOv9rTRVDMwERXDozehOEo
United States	2022-08-03	104.21.26.147	xxxx://theprestigecitysarjapur.info/indeex.html
United States	2022-08-03	54.205.81.162	xxxxs://infura-ipfs.io/ipfs/QmbeUpfiHjBmHm9g8FhNg2Qos33tZRNcqnk1S5SuPKkqXo?filename=maco.html
United States	2022-08-03	54.80.64.45	xxxxs://bafybeigfxe2jvxckg45pbatmccaswrc5fyjjblp3kurm6urytgt5f7xk2i.ipfs.infura-ipfs.io/?filename=maco.html
United States	2022-08-03	104.18.174.7	xxxxs://4205d37a.sibforms.com/serve/MUIEAIBmGuV16wZb2huYGEYk2h3-cH_ZYXLrSAMgT-uBH6CT8J5R3BdRu25X2C1XuFjCqQt6DAZOapyhjnbEm8QF40olWLQt4WTG9EM_q7i4DfBTDjpPucT7OKe3vAOOlk9ElVp1Hnlo6V7sNuw8DpJcQXeqkDphHGMDU6tnt7YZan5LHpc2HzSctP8B8rVHkBkqGKT7t9abtOWj
United States	2022-08-03	104.18.174.7	xxxx://103168d8.sibforms.com/serve/MUIEAA4C_io2OJp_p1_ccTO7fSyQsqLtXztfT1f0JTpEdNdNObQ05rEtdoTeaPflsMBBwmuDQeyuoSDJMqDsgFV5-586YdvQB-jbkjdH7iyugEE71DdybozJo5GnY5xqqwPc4FnaLjaXTyK7BdApP7Du1ITnolZj7kiNjI8Li2nICLDSqFZ46uA6WxrOv9rTRVDMwERXDozehOEo/
United States	2022-08-03	104.18.174.7	xxxxs://103168d8.sibforms.com/serve/MUIEAA4C_io2OJp_p1_ccTO7fSyQsqLtXztfT1f0JTpEdNdNObQ05rEtdoTeaPflsMBBwmuDQeyuoSDJMqDsgFV5-586YdvQB-jbkjdH7iyugEE71DdybozJo5GnY5xqqwPc4FnaLjaXTyK7BdApP7Du1ITnolZj7kiNjI8Li2nICLDSqFZ46uA6WxrOv9rTRVDMwERXDozehOEo
Japan	2022-08-03	118.27.122.26	xxxxs://igacorp.conohawing.com/south-saki-Qwa/New/Login.php
United States	2022-08-03	2606:4700::6812:ae07	xxxxs://bf92f294.sibforms.com/serve/MUIEAHStgSAatRl_S5DuF1N_kIM7Uw-A8vwoTEU34f3OaanIyyoReiAMeDx-qERAExnkEqGT_mcFcfivClHt5ksp66ayywNiuoxhBEJTIf1wtMpRw2c6czxsYSy_KDpaOISyYpOv7O9sRoB6HzwooJcovJssvbcXpB6FhPZtmTae09QPDLfOJlYgOZGRT_WseqDSDVCQ3YyDyoVf
United States	2022-08-03	2606:4700::6812:92	xxxxs://5b15fe32.sibforms.com/serve/MUIEADEC

		07	zYKdVtlFO-lf4-55cBmb-dp7kRCNGY9I1-fZXv-oWV_YXEkYw4yVofossVZF-OPMP86dseJYABurNDIf4CZA9jRa81NkMLgHtr_UpIIFHdpp8uXge3IYv47GKpESGV24eWR5sNxUVJFImeHcim3OvopDu3x3c3RJunY4iKpYDPPjTdPjD2Tvhvm3NPy49JUxWMB5jFzC
United States	2022-08-03	2606:4700::6812:9207	xxxx://6353c80e.sibforms.com/serve/MUIEACUu3YgBQRv1zNcmC6-poQM9YLVQcToEi8rChIUeIzI4kyUsJDgqAoNW585uO2pmfjxwQuwSe8xj3ag5wZ1kUlIx69DndCZEyrBJBLisjP93T81j2AmqLg6pFIxlAQnDPv06nKBvYy1p9J9DC6jEOZilig8rEb21rwlsHEr8TQYZzdCsBl6mnqkq7KLl-Q9t5NNhBp8ZwSdH
United States	2022-08-03	2602:fea2:2::1	xxxxs://bafybeic4vnkmumdevxc7fniiq4hl4trbw64wwsnx2ir4yw4mnnkul6syzm.ipfs.dweb.link/v5.htm
United States	2022-08-03	2606:4700::6812:ae07	xxxx://6353c80e.sibforms.com/serve/MUIEACUu3YgBQRv1zNcmC6-poQM9YLVQcToEi8rChIUeIzI4kyUsJDgqAoNW585uO2pmfjxwQuwSe8xj3ag5wZ1kUlIx69DndCZEyrBJBLisjP93T81j2AmqLg6pFIxlAQnDPv06nKBvYy1p9J9DC6jEOZilig8rEb21rwlsHEr8TQYZzdCsBl6mnqkq7KLl-Q9t5NNhBp8ZwSdH/

g. WhatsApp Group Invite

PAIS DE PROCEDENCIA	FECHA	IP	URL
Desconocido	2022-08-03	103.157.27.220	xxxxs://link-grup-18-whatsaap0.cf
Desconocido	2022-08-03	103.157.27.220	xxxxs://link-grup-18-whatsaap0.cf/

h. Microsoft Login

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-08-03	104.18.7.107	xxxxs://bafybeianakfmxfwygx57t7vcczptoirqkfz4ukkcs63jajzricwmsivzna.ipfs.nftstorage.link
United States	2022-08-03	162.244.80.49	xxxx://7g075duvtv7ub7qtnd8iqa7bnib2hp5s3hfdr5k9jp2e63f7j0guu3o.siasky.net
United States	2022-08-03	162.244.81.253	xxxx://7g05qj96lh9ofcpp1g80rf8l5r0tcg48jlk2ei37pci1t89mvo3v4k8.siasky.net
United States	2022-08-03	162.244.80.231	xxxx://7g05i0qp3mnoisbhlc2ac2vrt2iltqmmpm59bc4gtk5cl1lfnbi742g.siasky.net
United States	2022-08-03	2606:4700::6812:66b	xxxxs://bafybeianakfmxfwygx57t7vcczptoirqkfz4ukkcs63jajzricwmsivzna.ipfs.nftstorage.link/
United States	2022-08-03	162.244.80.231	xxxx://7g075duvtv7ub7qtnd8iqa7bnib2hp5s3hfdr5k9jp2e63f7j0guu3o.siasky.net/
United States	2022-08-03	162.244.80.49	xxxx://7g05qj96lh9ofcpp1g80rf8l5r0tcg48jlk2ei37pci1t89mvo3v4k8.siasky.net/
United States	2022-08-03	162.244.81.253	xxxx://7g05i0qp3mnoisbhlc2ac2vrt2iltqmmpm59bc4gtk5cl1lfnbi742g.siasky.net/
India	2022-08-03	182.18.157.233	xxxx://srenterpriseslko.in/xpc/office
Netherlands	2022-08-03	5.101.110.225	xxxxs://ams3.digitaloceanspaces.com/living2343/zom.htm
United States	2022-08-03	69.49.234.98	xxxx://enlightenuplife.com/inv/cccccc
United States	2022-08-03	72.47.208.90	xxxxs://lisarobertson.com/wp-includes/certificates/schlesingergroup/Noo-Reply/

i. Office 365

PAIS DE PROCEDENCIA	FECHA	IP	URL
United States	2022-08-03	69.49.234.252	xxxxs://envznary.com/auto/updation/

2. Recomendaciones:

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

Fuentes de información	▪ Comandancia de Ciberdefensa de la Marina, Osint

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 209	Fecha: 03-08-2022
		Página 11 de 15

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades críticas en varios productos de Cisco		
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:**
   Cisco ha reportado múltiples vulnerabilidades de severidad CRÍTICA de tipo desbordamiento de búfer clásico, inyección de comando de sistema operativo, restricción incorrecta de marcos, Cross-site Scripting, falta el enmascaramiento del campo de contraseña y cruce de ruta (Path Traversal) que afecta a varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar código arbitrario como usuario root y/o generar una condición de denegación de servicio (DoS), realizar ataques de secuencias de comandos entre sitios (XSS) y de Frame Hijacking, ejecutar código de secuencia de comandos arbitrario en el contexto de la interfaz afectada, acceder a información confidencial basada en el navegador y eliminar archivos arbitrarios de un sistema afectado.

2. **Detalles:**
   - La vulnerabilidad de severidad **crítica** identificada como CVE-2022-20842 en la interfaz de administración basada en web de los enrutadores Cisco de la serie RV340, RV340W, RV345 y RV345P Dual WAN Gigabit VPN podría permitir a un atacante remoto no autenticado ejecutar código arbitrario como usuario raíz en el sistema operativo subyacente o hacer que el dispositivo se vuelva a cargar, lo que resultaría en una condición DoS. Esta vulnerabilidad se debe a una validación insuficiente de la entrada proporcionada por el usuario a la interfaz de administración basada en web.
   - La vulnerabilidad de severidad **crítica** identificada como CVE-2022-20827 en la función de actualización de la base de datos del filtro web de los enrutadores de la serie RV160, RV260, RV340 y RV345 de Cisco Small Business podría permitir a un atacante remoto no autenticado enviar información manipulada a la función de actualización de la base de datos del filtro web y realizar una inyección de comando y ejecutar comandos en el sistema operativo subyacente con privilegios de root.
   - La vulnerabilidad de severidad **alta** identificada como CVE-2022-20841 en el módulo Open Plug and Play (PnP) de los enrutadores de la serie RV160, RV260, RV340 y RV345 de Cisco Small Business podría permitir a un atacante remoto no autenticado enviar información maliciosa a un dispositivo afectado e inyectar y ejecutar comandos arbitrarios en el sistema operativo subyacente. Para aprovechar esta vulnerabilidad, un atacante debe aprovechar una posición intermedia o tener un punto de apoyo establecido en un dispositivo de red específico que esté conectado al enrutador afectado.
   - Cisco indicó que, las vulnerabilidades dependen unas de otras. La explotación de una de las vulnerabilidades puede ser necesaria para explotar otra vulnerabilidad. Además, es posible que una versión de software que se vea afectada por una de las vulnerabilidades no se vea afectada por las otras vulnerabilidades.
   - Las vulnerabilidades de severidad **media** han sido identificadas como: CVE-2022-20820, CVE-2022-2085, CVE-2022-20914; CVE-2022-20816 y CVE-2022-20869.

3. **Productos afectados:**
   - Routers Cisco Small Business de la serie: RV160, RV260, RV340 y RV345;
   - Cisco Webex Meetings (basado en la nube);
   - Cisco Identity Service Engine (ISE): versión 2.3 y anteriores, 2.4, 2.6, 2.7, 3.0 y 3.1;
   - Cisco Unified CM y Cisco Unified CM SME: versión 11.5, 12.5 y 14;
   - Cisco BroadWorks Application Delivery Platform: version 22.0, 23.0 y 24.0.

4. **Solución:**
   - CISCO recomienda actualizar los productos afectados con la última versión fija disponible que corrige estas vulnerabilidades.

Fuentes de información	▪ hxxps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 209**	**Fecha: 03-08-2022**
		Página 12 de 15

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades críticas en routers Arris		
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:

El investigador Derek Abdine, ha reportado múltiples vulnerabilidades de severidad CRÍTICA de tipo limitación incorrecta de la ruta a un directorio restringido, desreferencia a puntero nulo y desbordamiento de búfer que afectan a varios modelos de routers Arris. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autentificado o a cualquier usuario local, recorrer las rutas de directorios desde la raíz del sistema de archivos y obtener acceso a la configuración del equipo vulnerable.

2. Detalles:

- El investigador indicó que existen tres vulnerabilidades en el servidor web muhttpd con licencia del MIT. Señalo que este servidor web es ampliamente utilizado en equipos de las instalaciones del cliente (CPE) del ISP, sobre todo en el firmware de Arris utilizado en modelos de enrutador de la serie NVG443, NVG599, NVG589, NVG510, así como variantes personalizadas por ISP como BGW210 y BGW320. Estos enrutadores generalmente se prestan a los suscriptores de ISP para telefonía y acceso a Internet.
- La vulnerabilidad de severidad **crítica** identificada como CVE-2022-31793 de path traversal podría permitir a un atacante remoto, no autentificado, o a cualquier usuario local, recorrer las rutas de directorios desde la raíz del sistema de archivos.
- La vulnerabilidad de falta de referencia de puntero NULL (aun no registrada con CVE), se debe a que el servidor muhttpd recibe solicitudes HTTP en un socket sin bloqueo.
- La vulnerabilidad de sobrelectura de búfer cuando se eliminan URL (aun no registrada con CVE), se debe a que el servidor muhttpd contiene una sobrelectura de búfer cuando se trata de valores codificados en porcentaje.
- El investigador indico además que hay aproximadamente 19,000 enrutadores vulnerables expuestos directamente a Internet en los ISP de EE. UU., Europa y APAC, lo que afecta tanto a clientes residenciales como comerciales.

3. Productos afectados:

- Servidor web muhttpd, empleado en equipos de cliente (CPE) de ISP, principalmente en el firmware de Arris utilizado en los modelos de Router: NVG443, NVG599, NVG589, NVG510, BGW210 y BGW320.

4. Solución:

- Arris indicó que para la vulnerabilidad CVE-2022-31793 de path traversal, se debe detener el servidor web, o utilizar un firewall para evitar el acceso a redes no confiables (Internet, LAN). En el caso de los Gateways basados en Arris afectados, desactivar la gestión remota, o utilizar un cortafuego para los puertos de acceso remoto desde Internet. Para los usuarios habituales de muhttpd, actualizar a la versión 1.1.7;
- Respecto a las otras 2 vulnerabilidades sin CVE asignado: se debe desactivar el acceso remoto o emplear un firewall para los puertos de acceso remoto desde Internet.

Fuentes de información	▪ hxxps://derekabdine.com/blog/2022-arris-advisory

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 209	Fecha: 03-08-2022
		Página 13 de 15

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantado la identidad de la compañía multinacional Amazon		
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, los ciberdelincuentes se vienen llevando a cabo una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad de la compañía multinacional de comercio electrónico Amazon, con el objetivo de acceder u obtener credenciales de acceso, datos personales y bancarios de las posibles víctimas.

2. **Imagen**: Proceso del ataque Phishing:

Imagen 1: Solicita dirección de correo electrónico y contraseña.

Imagen 2: Solicita datos bancarios como el número de tarjeta, fecha de caducidad y el CVC de la tarjeta.

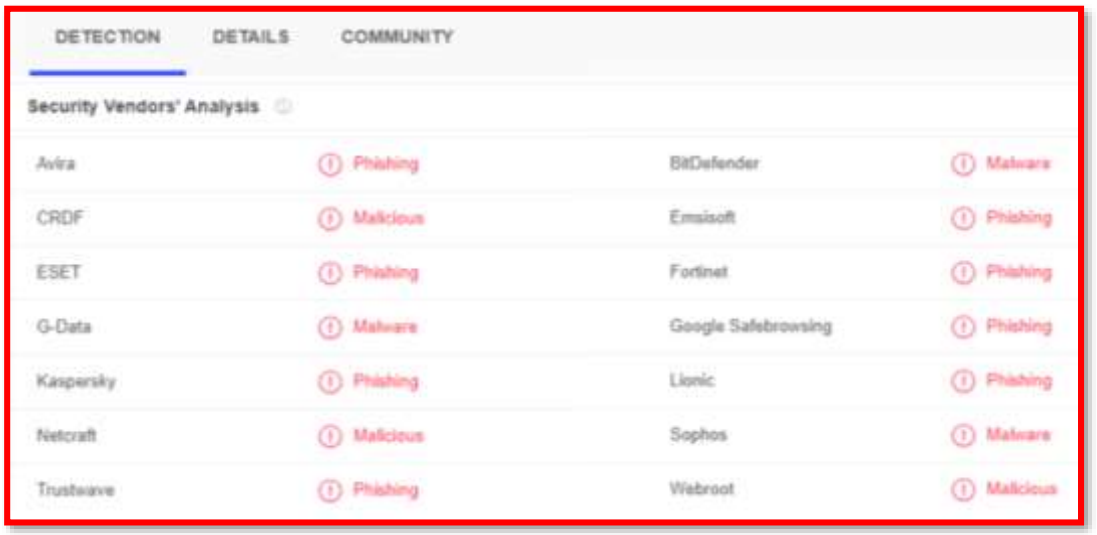
Imagen 3: Solicita datos personales fecha de nacimiento, número telefónico, ciudad y más.

Imagen 4: Solicita ingresar las credenciales de acceso de la página (usuario y contraseña).

Imagen 5: Por último, es redirigido automáticamente a un supuesto sitio web de Amazon, donde la víctima puede verificar una serie de consultas como se aprecia en la imagen.

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[:]//deinetike[.]com/amazon[-]RD292[-]user[-]card[-]detail[-]em[-]thank/
  - ✓ **Dominio:** deinetike[.]com
  - ✓ **IP:** 192[.]185[.]114[.]52
  - ✓ **Código:** 200
  - ✓ **Longitud:** 8.68 KB
  - ✓ **SHA-256**: d676ed256c90735592555b7fa0d814cbd5348a219548dd3bfc36760bdf6bc45a



- **OTRAS DETECCIONES:**

4. **ALGUNAS RECOMENDACIONES:**
   - Verificar la información en la entidad correspondiente.
   - Acceder al sitio web a través de fuentes oficiales.
   - No abrir enlaces de dudosa procedencia.
   - No seguir indicaciones de sitios web fraudulentos.
   - No compartir la información con terceras personas, amigos o familiares.
   - Mantener instalado un servicio de antivirus en el dispositivo.

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

Índice alfabético