

24 de agosto, 2023



Boletín Ciberseguridad

CLARO EMPRESAS

BOLETÍN SEMANAL #98

Estrategias clave para enfren- tar la explotación de software remoto

CISA emitió el Plan de Ciberdefensa de Monitoreo y Gestión Remotos (RMM), el primer Plan proactivo desarrollado por socios de la industria y el gobierno a través de la Colaboración Conjunta de Ciberdefensa (JCDC). Este plan aborda los riesgos sistémicos que enfrenta la explotación del software RMM. Los actores de amenazas cibernéticas pueden afianzarse a través del software RMM en proveedores de servicios administrados (MSP) o administrar servidores de proveedores de servicios de seguridad (MSSP) y, por extensión, pueden causar impactos en las organizaciones pequeñas y medianas que son clientes de MSP/MSSP.

Este lanzamiento se basa en la Agenda de Planificación JCDC 2023 y marca un hito importante en la evolución y maduración continuas del desarrollo de la Colaborativa para satisfacer las funciones principales de JCDC, entre ellas se

encuentran:

- Desarrollo y coordinación de planes de ciberdefensa
- Colaboración operativa y fusión de información de ciberseguridad
- Producir y difundir orientación sobre ciberdefensa

A través de este esfuerzo, CISA y sus socios en el gobierno y el sector privado tomarán medidas para reducir considerablemente algunos de los riesgos cibernéticos más importantes que enfrenta la comunidad cibernética mundial.

CISA alienta a las organizaciones a revisar las páginas web del Plan Estratégico de Defensa Cibernética RMM de JCDC y la Agenda de Planificación 2023.

Fuente:

<https://www.cisa.gov/news-events/alerts/2023/08/16/cisa-releases-jcdc-remote-monitoring-and-management-rmm-cyber-defense-plan>

Índice

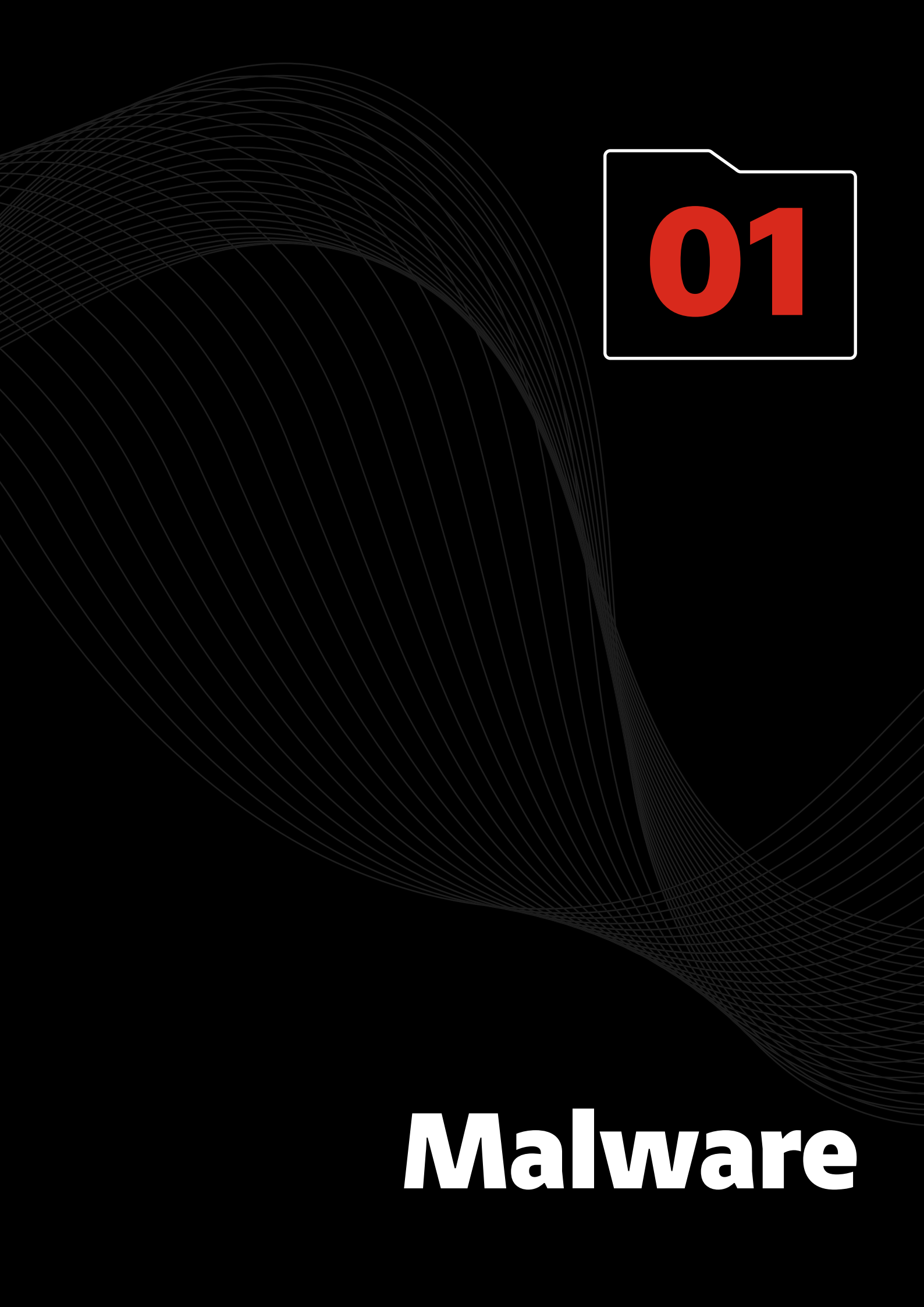
1. Malware	04
1.1 Propagación de malware a través de aplicación PROXY	
1.2 Programas maliciosos para Android utilizan métodos de compresión únicos para evitar la detección	
2. Vulnerabilidades	09
2.1 Vulnerabilidades en el sistema operativo Juniper Junos ponen en riesgo dispositivos frente a ataques remotos	
3. Phishing	12
3.1 Nueva campaña dirigida a usuarios de Zimbra	
4. Adversarios	15
4.1 Nueva campaña de distribución del ransomware HiatusRAT	
5. Indicadores de Compromiso	18
6. Fuentes	25

Prioridad

Crítica 

Alta 

Media 

The background of the slide is black, featuring a series of thin, grey, curved lines that flow from the left side towards the right, creating a sense of motion and depth. In the upper right corner, there is a white-outlined folder icon containing the red text '01'.

01

Malware



1.1 Propagación de malware a través de aplicación PROXY

Los investigadores de AT&T Alien Labs descubrieron recientemente una campaña masiva de amenazas que entregan una aplicación de servidor proxy a máquinas Windows y macOS.

El objetivo de estos ataques tiene es lograr infectar los equipos con malware para entregar una aplicación de servidor proxy y usarlas como nodos de salida para redirigir las solicitudes de proxy.

Según AT&T Alien Labs, la compañía anónima que ofrece el servicio de proxy opera más de 400,000 nodos de salida, sin embargo, aún no está claro de inmediato cuántos han sido comprometidos por el malware instalado en máquinas infectadas sin conocimiento e interacción del usuario.

Finalmente, el malware se encuentra en constante propagación con su nueva versión, 1.6, y revela la continua evolución y sofisticación del troyano, complicando así el proceso de análisis. Además, como la aplicación proxy está firmada, no tiene detección antivirus, pasando por debajo del radar de las empresas de seguridad.

Recomendaciones:

- › Ejecutar el bloqueo de los Indicadores de compromiso detallados en el ítem 5.
- › Implementar controles de seguridad que garanticen el respaldo de la información y deben estar fuera de línea y en redes separadas.
- › Implementar un control de seguridad que realice actualizaciones periódicas en estaciones de trabajo, dispositivos móviles, portátiles y otros activos críticos de la organización.
- › Implementar campañas de concientización asociado a malware & phishing para que los usuarios puedan abstenerse de abrir enlaces y archivos adjuntos de correo electrónico que no sean de confianza sin verificar su autenticidad.
- › Implementar o tercerizar soluciones avanzadas de ciberseguridad tales como EDR/XDR que permitan la identificación de amenazas basado en comportamiento.

1.2 Programas maliciosos para Android utilizan métodos de compresión únicos para evitar la detección

Los investigadores de ciberseguridad de Zimperium zLab identificaron recientemente un archivo de paquete de aplicación (APK) denominado "a.apk" que podría instalarse en el sistema operativo Android anterior a Android 9, el APK no se puede escanear desde la mayoría de las herramientas anti descompilación.

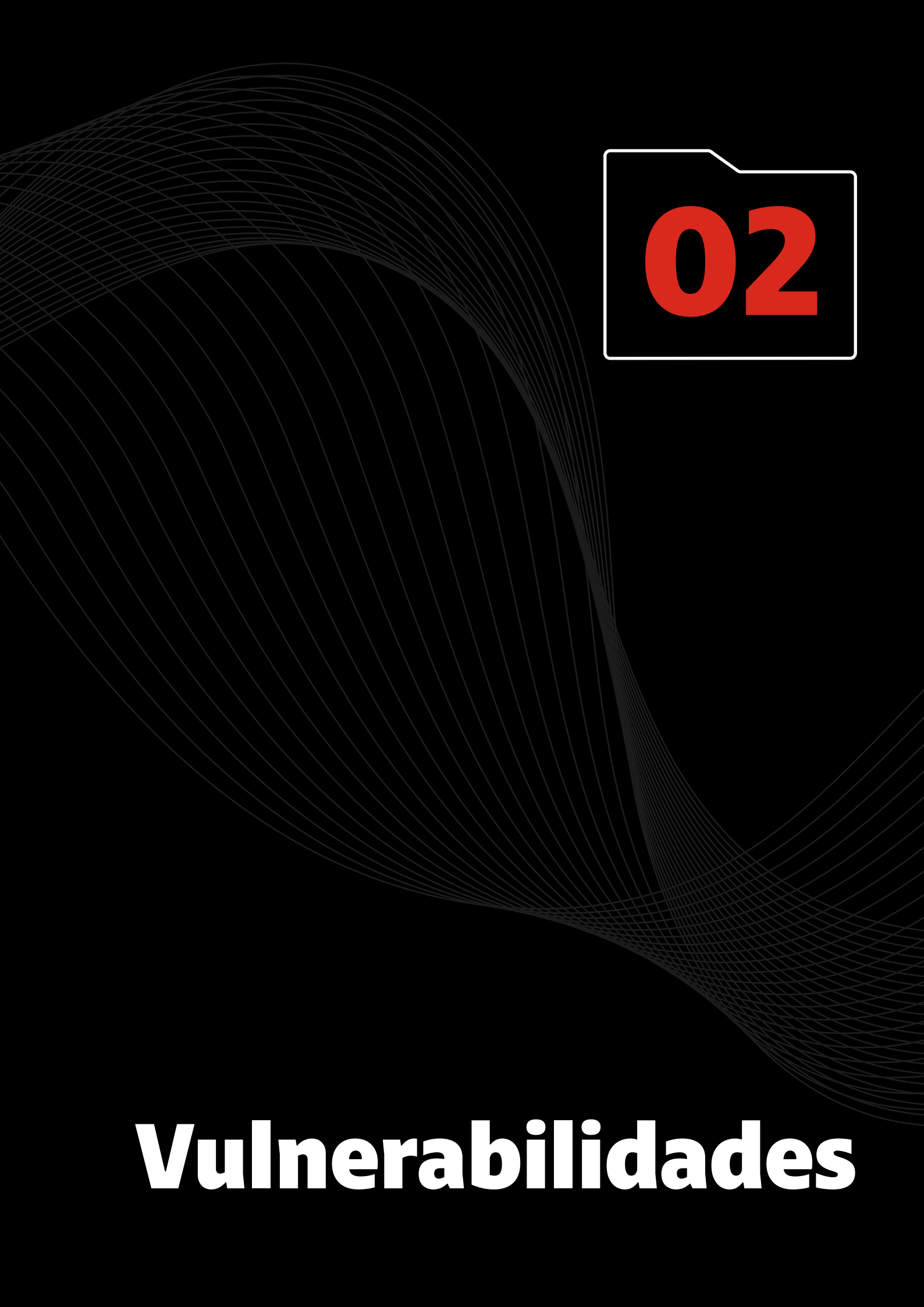
Si bien esta muestra evita la descompilación empleando un método de descompresión que no es compatible en absoluto con su APK, un archivo zip dificulta el análisis completo para muchas herramientas. Sin embargo, aunque es un método antiguo, es de naturaleza sofisticada e implica alterar los algoritmos de compresión APK para evadir el análisis automático del script para evitar el examen estático.

Por ello, dentro del análisis de ciberseguridad se descubrió que las 3.300 muestras estaban utilizando "compresión desconocida no compatible", incluso encontraron algunas demasiado corruptas o complejas que dificultaba su ejecución en los sistemas operativos comprometidos.

De estas muestras maliciosas identificadas, los analistas de seguridad pudieron encontrar solo 71 muestras negativas cargables del sistema operativo Android, y entre estas muestras, ninguna de ellas está disponible en Google Play Store en este momento.

Recomendaciones:

- › Ejecutar el bloqueo de los Indicadores de compromiso detallados en el ítem 5.
- › Descargar aplicaciones solo de fuentes confiables.
- › Implementar campañas de concientización asociado a malware & phishing para que los usuarios puedan abstenerse de abrir enlaces y archivos adjuntos de correo electrónico que no sean de confianza sin verificar su autenticidad.
- › Implementar un control de seguridad que realice actualizaciones periódicas en estaciones de trabajo, dispositivos móviles, portátiles y otros activos críticos de la organización.
- › Implementar soluciones avanzadas de ciberseguridad tales como EDR (Endpoint Detection & Response) para detectar y responder en forma oportuna ante eventos y e incidentes de Ciberseguridad sobre los activos críticos de la organización.
- › Implementar soluciones avanzadas de multi factor de autenticación para correo electrónico, Active Directory, aplicaciones web y dispositivos móviles.



02

Vulnerabilidades



2.1 Vulnerabilidades en el sistema operativo Juniper Junos ponen en riesgo dispositivos frente a ataques remotos

Juniper Networks ha lanzado una actualización de seguridad para abordar múltiples fallas en el componente J-Web del sistema operativo Junos que podrían combinarse para lograr la ejecución remota de código en instalaciones susceptibles. La interfaz J-Web permite a los usuarios configurar, administrar y monitorear dispositivos del sistema operativo Junos.

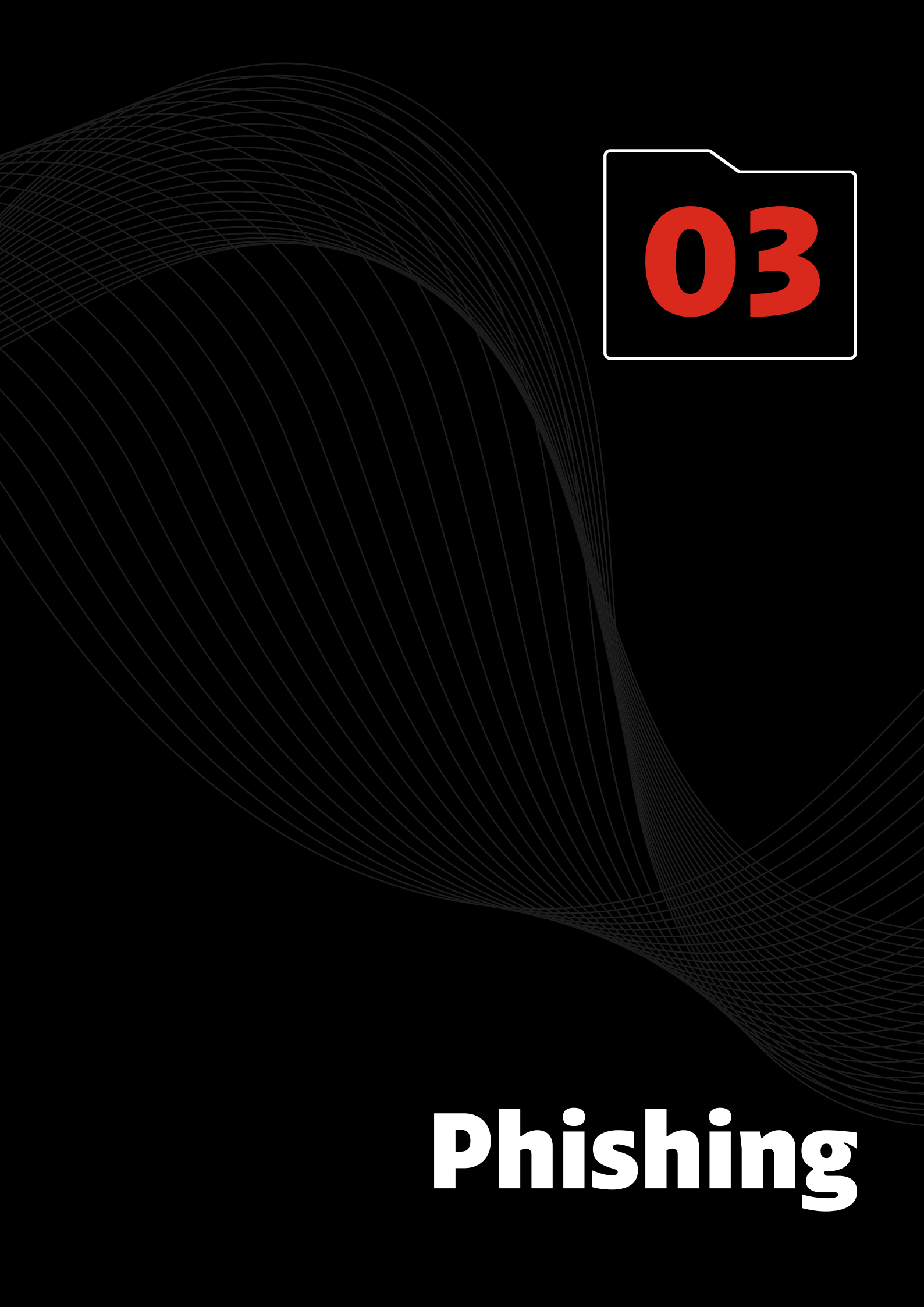
Dichas vulnerabilidades se han resuelto mediante la aplicación de correcciones específicas que permiten abordar cada vulnerabilidad por lo que el fabricante recomienda su aplicación en dispositivos de las series mencionadas.

Las series y sus respectivas versiones afectadas son las siguientes:

SERIE	VERSIONES
EX	20.4R3-S8, 21.2R3-S6, 21.3R3-S5, 21.4R3-S4, 22.1R3-S3, 22.2R3-S1, 22.3R2-S2, 22.3R3, 22.4R2-S1
SRX	20.4R3-S8, 21.2R3-S6, 21.3R3-S5, 21.4R3-S5, 22.1R3-S3, 22.2R3-S2, 22.3R2-S2, 22.3R3, 22.4R2-S1

Recomendaciones:

- › Juniper Networks sugiere que los usuarios deshabiliten J-Web o limiten el acceso a solo hosts confiables.
- › Para evitar la ejecución remota de código (RCE), solo es necesario reparar un PR por plataforma.
- › Actualizar los dispositivos afectados SRX y EX para las últimas versiones de Junos OS, asegurando que estas vulnerabilidades se vean frustradas antes de que puedan ser explotadas.



03

Phishing



3.1 Nueva campaña dirigida a usuarios de Zimbra

Según ESET, recientemente se descubrió una nueva campaña de phishing dirigida a los usuarios de Zimbra con el objetivo de recopilar las credenciales de sus usuarios. Se estima que la presente campaña se encuentra activa desde el mes de abril del 2023 y que continúa en curso.

Esta campaña se encuentra activa principalmente por Europa y Asia, pero también, la telemetría de ESET logró identificar ataques dirigidos a organizaciones de Latinoamérica. El ataque inicia cuando el objetivo recibe un correo electrónico con un archivo HTML phishing adjunto. Este archivo, al ser abierto, muestra a la víctima un acceso falso al portal Zimbra que se encuentra personalizado con imágenes de la organización de la víctima.

Todas las credenciales que el usuario ingresa al formulario de login son enviados, en segundo plano, mediante una solicitud HTTPS POST hacia un servidor controlado por el adversario. Finalmente, esta campaña se basa únicamente en ingeniería social, y aunque no es tan sofisticada técnicamente, todavía es capaz de difundir y

comprometer con éxito la información de las organizaciones que utilizan Zimbra.

TTPs de MITRE ATT&CK

Es una lista estructurada para describir y clasificar los comportamientos conocidos de los atacantes en base a observaciones reales, expresados en varias matrices.

Táctica: corresponden a qué intentan lograr los adversarios.

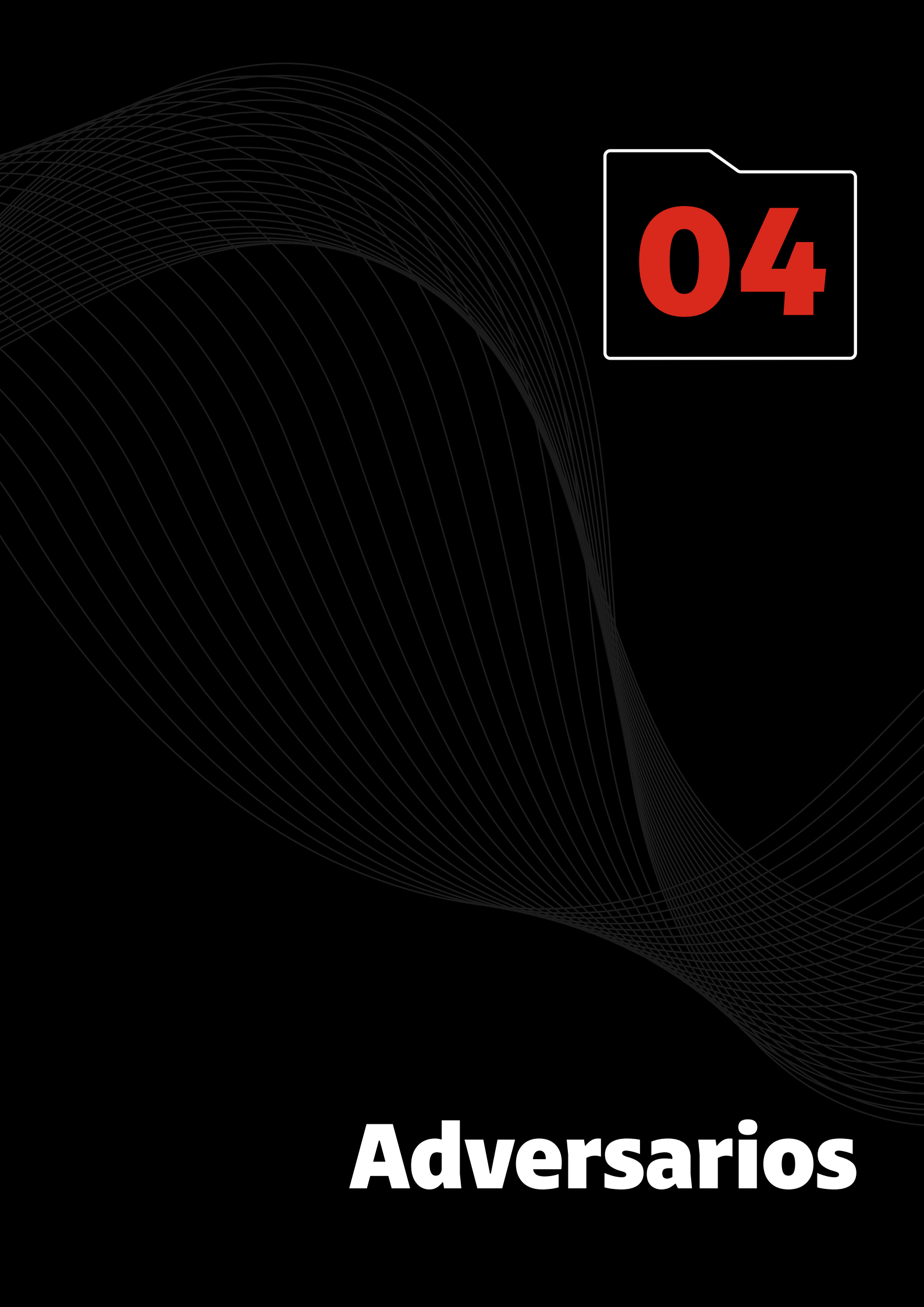
Técnica: describe el cómo de la actividad real realizada por el adversario.

Procedimiento: es la implementación específica que utiliza el adversario para ejecutar las técnicas y/o sub-técnicas.

TÁCTICA	Técnica (ID)	Nombre de la Técnica	Mitigación
DESARROLLO DE RECURSOS	T1586.002	Cuentas comprometidas: cuentas de correo electrónico	M1056
	T1585.002	Establecer cuentas: cuentas de correo electrónico	M1056
ACCESO INICIAL	T1566.001	Phishing: Adjunto de spearphishing	M1049 M1031 M1021 M1054 M1017
EJECUCIÓN	T1204.002	Ejecución del usuario: Archivo malicioso	M1040 M1038 M1017
PERSISTENCIA	T1136	Crear cuenta	M1032 M1030 M1028 M1026
COLECCIÓN	T1056.003	Captura de entrada: captura del portal web	M1026
EXFILTRACIÓN	T1048.002	Exfiltración sobre protocolo alternativo: Exfiltración sobre protocolo asimétrico cifrado no C2	M1057 M1037 M1031 M1030

Recomendaciones:

- › Ejecutar las recomendaciones referentes a las técnicas de Mitre ATT&CK en las cuales se podrá observar la mitigación para cada tipo de técnica y/o sub-técnica de ataque. Para más detalle diríjase a la referencia desde el punto 6.8 hasta el punto 6.14 del boletín.
- › Ejecutar el bloqueo de los Indicadores de compromiso detallados en el ítem 5.
- › Implementar un software EDR en todos los puntos finales de la organización con capacidades de detección y prevención de malware.
- › Implementar un control de seguridad con capacidades de detección y prevención de ataques de phishing.
- › Implementar o tercerizar un servicio de DarkWeb que permita detectar cuentas de correo expuestas y/o comprometidas.
- › Tercerizar un servicio de SOC con disponibilidad 24x7x365.
- › Implementar o desarrollar un programa de concientización para todos los usuarios de la organización considerando la importancia de la salvaguarda de la información.



04

Adversarios



4.1 Nueva campaña de distribución del ransomware HiatusRAT

TheHackerNews nos informa que los actores de amenaza responsables del desarrollo del ransomware HiatusRAT reanudaron sus operaciones después de un periodo de inactividad. Sus actividades estaría enfocadas buscar información publicada relacionada con contratos militares actuales y futuros.

Se desconoce el vector de acceso inicial, pero una vez que el actor logra el acceso se despliega un script bash que descarga y ejecuta el ransomware HiatusRAT junto a un binario de captura de paquetes. Pudiendo recolectar información del router, procesos en ejecución y contactar un servidor remoto para descargar archivos o ejecutar comandos arbitrarios. También es capaz de actuar como proxy para el tráfico de comando y control (C2) a través del router.

Por último, la focalización de activos perimetrales como enrutadores se ha convertido en una especie de patrón en los últimos meses, con actores de amenazas afiliados a China vinculados a la explotación de fallas de seguridad en dispositivos Fortinet y SonicWall sin parches para establecer la persistencia a largo plazo dentro de los entornos objetivo.

Recomendaciones:

- › Ejecutar el bloqueo de los indicadores de compromiso detallados en el ítem 5.
- › Implementar un software EDR en todos los puntos finales de la organización que permita la detección y prevención de cualquier anomalía de seguridad.
- › Implementar o tercerizar un servicio de Inteligencia de Amenazas con alcance 24x7x365.
- › Implementar políticas de seguridad a nivel de contraseñas “fuertes” que cumplan criterios de complejidad específicos.
- › Implementar la arquitectura Zero Trust como parte de la mejora de la postura de ciberseguridad de la organización.
- › Implementar una política de seguridad a nivel de red que considere la segmentación de redes de acuerdo con las áreas que posee la organización.

Indicadores de compromiso

5.1 IPs

145.14.144[.]174	(Ítem Phishing: 3.1)
145.14.145[.]248	(Ítem Phishing: 3.1)
145.14.145[.]122	(Ítem Phishing: 3.1)
145.14.144[.]58	(Ítem Phishing: 3.1)
145.14.145[.]94	(Ítem Phishing: 3.1)
145.14.145[.]36	(Ítem Phishing: 3.1)
173.44.236[.]125	(Ítem Phishing: 3.1)
207.246.80[.]240	(Ítem Adversarios: 4.1)
45.63.70[.]57	(Ítem Adversarios: 4.1)
155.138.213[.]169	(Ítem Adversarios: 4.1)
66.135.22[.]245	(Ítem Adversarios: 4.1)
107.189.11[.]105	(Ítem Adversarios: 4.1)
46.8.113[.]227	(Ítem Adversarios: 4.1)
104.250.48[.]192	(Ítem Adversarios: 4.1)

5.2 DOMINIO

fmaildd.000webhostapp[.]com	(Ítem Phishing: 3.1)
nmailddt.000webhostapp[.]com	(Ítem Phishing: 3.1)
tmaxd.000webhostapp[.]com	(Ítem Phishing: 3.1)
posderd.000webhostapp[.]com	(Ítem Phishing: 3.1)
riddtd.000webhostapp[.]com	(Ítem Phishing: 3.1)
mtatdd.000webhostapp[.]com	(Ítem Phishing: 3.1)
zimbra.y2kportfolio[.]com	(Ítem Phishing: 3.1)

5.3 URL

hxxp[:]//m.essencecuration[.]com/a/rep	(Ítem Malware: 1.1)
hxxp[:]//m.enchantedreign[.]com/a/rep	(Ítem Malware: 1.1)
hxxp[:]//m.articlesagile[.]com/a/rep	(Ítem Malware: 1.1)
hxxps://fmaildd.000webhostapp[.]com/wp-admin/ZimbraNew[.]php	(Ítem Malware: 3.1)
hxxps://mtatdd.000webhostapp[.]com/wp-admin/ZimbraNew[.]php	(Ítem Malware: 3.1)
hxxps://nmailddt.000webhostapp[.]com/wp-admin/ZimbraNew[.]php	(Ítem Malware: 3.1)
hxxps://posderd.000webhostapp[.]com/wp-admin/ZimbraNew[.]php	(Ítem Malware: 3.1)
hxxps://riddtd.000webhostapp[.]com/wp-admin/ZimbraNew[.]php	(Ítem Malware: 3.1)
hxxps://tmaxd.000webhostapp[.]com/wp-admin/ZimbraNew[.]php	(Ítem Malware: 3.1)
hxxps://zimbra.y2kportfolio[.]com/wp-admin/ZimbraNew[.]php	(Ítem Malware: 3.1)

5.4 Hashes

(Ítem Malware: 1.1)

SHA256: c7721ab85bad163576c166a0a71c0dbe4cc491dda68c5a5907fd1d8cac50780d

MD5: f7d4134f1831427a76dd777f037435ae

(Ítem Malware: 1.1)

SHA256: 2d595880cfb1691dd43de02d1a90273919f62311a7668ef078709eff2fd6bd87

MD5: 832aeb75c977ba22e1dc1cdda5e00456

(Ítem Malware: 1.1)

SHA256: d94f62ec4b6ffcec35d5e639d02a52ce226629a5eb3e2a7190174ea8d3b40b5b

MD5: 64239404e3aa349bd8db3b6de165cd14

(Ítem Malware: 1.1)

SHA256: 6587e61a8a7edb312da5798ffccf4a5ef227d3834389993b4df3ef0b173443dc

MD5: a687f039ca8d08034e7ffe49314b4fc6

(Ítem Malware: 1.1)

SHA256: 3d063efde737b7b2e393926358cbb32469b76395e1a05e8c127a12e47550f264

MD5: 22a37cad83df80709fddd07085777413

(Ítem Malware: 1.1)

SHA256: 2fb1d8e6454f43522f42675dcf415569e5df5d731e1d1390f793c282cce4a7aa

MD5: 0ff81151f2b007450d389311d1b63450

(Ítem Malware: 1.1)

SHA256: 956aae546af632ea20123bfe659d57e0d5134e39cdb5489bd6f1ba5d8bbd0472

MD5: c13641967a755b28efa29c79ada65f0b

(Ítem Malware: 1.1)

SHA256: 68b6beb70bd547b75f2d36d70ca49f8b18542874480d39e33b09ee69eb1048b3

MD5: 3996181fc51151416b1aa146fbd61e16

(Ítem Malware: 1.1)

SHA256: 54efc69cb6ee7fde00c0320202371dcdad127d0e7c8babce4659be8230d81a81

MD5: e2f279d566c921968c56047cda518279

(Ítem Malware: 1.1)

SHA256: 7cb10a70fd25645a708c81f44bb1de2b6de39d583ae3a71df0913917ad1dff3

MD5: 17d680825d23e672d23cc82126069c71

(Ítem Malware: 1.1)

SHA256: 1904b705105db4550371d678f8161826b98b1a9fca139fa41628214ed816d2f5

MD5: 161da79a6093dfc9a5fda4919f90cd26

(Ítem Malware: 1.1)

SHA256: 4a7c9829590e1230a448dd7a4272b9fbfbafccf7043441967c2f68f6082dde32

MD5: d13ad9571a4fd8380c3e3fc90116fd69

(Ítem Malware: 1.1)

SHA256: ee9ebdb1d9a7424cd64905d39820b343c5f76e29c9cd60c0cdd3bfe069fb7d51

MD5: f1cb5fc4d248c60959ded6758625be10

(Ítem Malware: 1.2)

SHA256: b3561bf581721c84fd92501e2d0886b284e8fa8e7dc193e41ab300a063dfe5f3

MD5: 2f371969faf2dc239206e81d00c579ff

(Ítem Adversarios: 4.1)

SHA256: 774f2f3a801ddfe5d8a9ab1b90398ee28ee2be3d7ad0fa75eacbfd7ab51f6939

MD5: 5a07d8566930c9ead926c2f079620510

(Ítem Adversarios: 4.1)

SHA256: 766e13d2a085c7c1b5e37fe0be92658932a13cfbcadf5b08977420fc6ac6d3e3

MD5: 2843c0dd5d689de872be924addd2a3f0

(Ítem Adversarios: 4.1)

SHA256: 193481c4e2cbd14a29090f500f88455e1394140b9c5857937f86d2b854b54f60

MD5: 9690a3e310ed96073035c4cc3436fa9c

(Ítem Adversarios: 4.1)

SHA256: 3a21599e0a60b4bce8d31757f0b461a217f30d0ea261f5844004b8cc09fcab35

MD5: 14260ca77ff9362030d769d08f279b94

(Ítem Adversarios: 4.1)

SHA256: a878b0ca6c99e82127cc9ef5e83b5dac5f1f8b9798580346e33e6d6f16267b73

MD5: 3ff316bf1e7a13e0c6ed44e87d71c110

(Ítem Adversarios: 4.1)

SHA256: 6e21e42cfb93fc2ab77678b040dc673b88af31d78fafa91700c7241337fc5db2

MD5: ff8e26ec2573f482abbd1a8fdd80fc81

(Ítem Adversarios: 4.1)

SHA256: 98ec46ac0e3b0b49140f710d0437e03e1f89f9b6fc092be7a5a1fde7d59e312e

MD5: 8c93ee4d1e648da1f289d996baa252f4

Fuentes

- 6.1 <https://thehackernews.com/2023/08/this-malware-turned-thousands-of-hacked.html>
- 6.2 <https://gbhackers.com/3000-android-malware-compression/>
- 6.3 https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US
- 6.4 <https://www.welivesecurity.com/en/eset-research/mass-spreading-campaign-targeting-zimba-users/>
- 6.5 <https://cyware.com/news/hiatusrat-returns-after-a-hiatus-in-a-fresh-wave-of-attacks-dd524dce>
- 6.6 <https://thehackernews.com/2023/08/hiatusrat-malware-resurfaces-taiwan.html>
- 6.7 <https://devel.group/blog/nuevo-malware-hiatusrat-se-enfoca-en-routers-de-grado-empresarial-para-espiar-a-sus-victimas-de-manera-encubierta/>
- 6.8 <https://attack.mitre.org/techniques/T1586/002>
- 6.9 <https://attack.mitre.org/techniques/T1585/002>
- 6.10 <https://attack.mitre.org/techniques/T1566/001>
- 6.11 <https://attack.mitre.org/techniques/T1204/002>
- 6.12 <https://attack.mitre.org/techniques/T1136>
- 6.13 <https://attack.mitre.org/techniques/T1056/003>
- 6.14 <https://attack.mitre.org/techniques/T1048/002>



Conozca las opciones de seguridad que Claro Empresas tiene para ofrecerle contactándose con su **Consultor Corporativo** o escribiéndonos a **claroempresas@claro.com.pe** con el asunto "Ciberseguridad".