

02 de agosto, 2023



Boletín Ciberseguridad

CLARO EMPRESAS

BOLETÍN SEMANAL #95

Principales industrias que necesitan aumentar defensas cibernéticas

Según Bitdefender, en los últimos años, las industrias aceleraron sus esfuerzos de transformación digital, aumentando su dependencia del trabajo remoto y aprovechar los servicios basados en la nube a mayor escala. Este cambio rápido, junto con la persistente incertidumbre sobre el futuro, ha creado nuevos desafíos y riesgos para las empresas. Asimismo, es cada vez más claro que algunas industrias deben priorizar la ciberseguridad o, de lo contrario, arriesgarse a un aumento desmesurado de los incidentes y compromisos cibernéticos.

Los riesgos que enfrentan estas industrias se deben a una gran variedad de factores internos, ambientales y basados en amenazas. Por ejemplo, las industrias que han enfrentado un rápido crecimiento y una mayor adopción digital en los últimos años pueden tener lagunas en los

protocolos de seguridad, mientras que otras se enfrentan a un mayor número de ataques por parte de actores malintencionados. Para muchas empresas, la creciente interconectividad y la dependencia de las cadenas de suministro globales han creado vulnerabilidades adicionales que aún deben abordarse.

Por ello, se identificó cuatro industrias que necesitan priorizar más la ciberseguridad:

- Sector salud
- Sector financiero
- SaaS y software
- Sector manufactura

En este artículo, se profundiza en las preocupaciones únicas de seguridad cibernética que enfrenta cada industria y qué soluciones pueden utilizar.

Fuentes:

<http://businessinsights.bitdefender.com/the-four-industries-that-need-to-prioritize-cybersecurity-the-most>

Índice

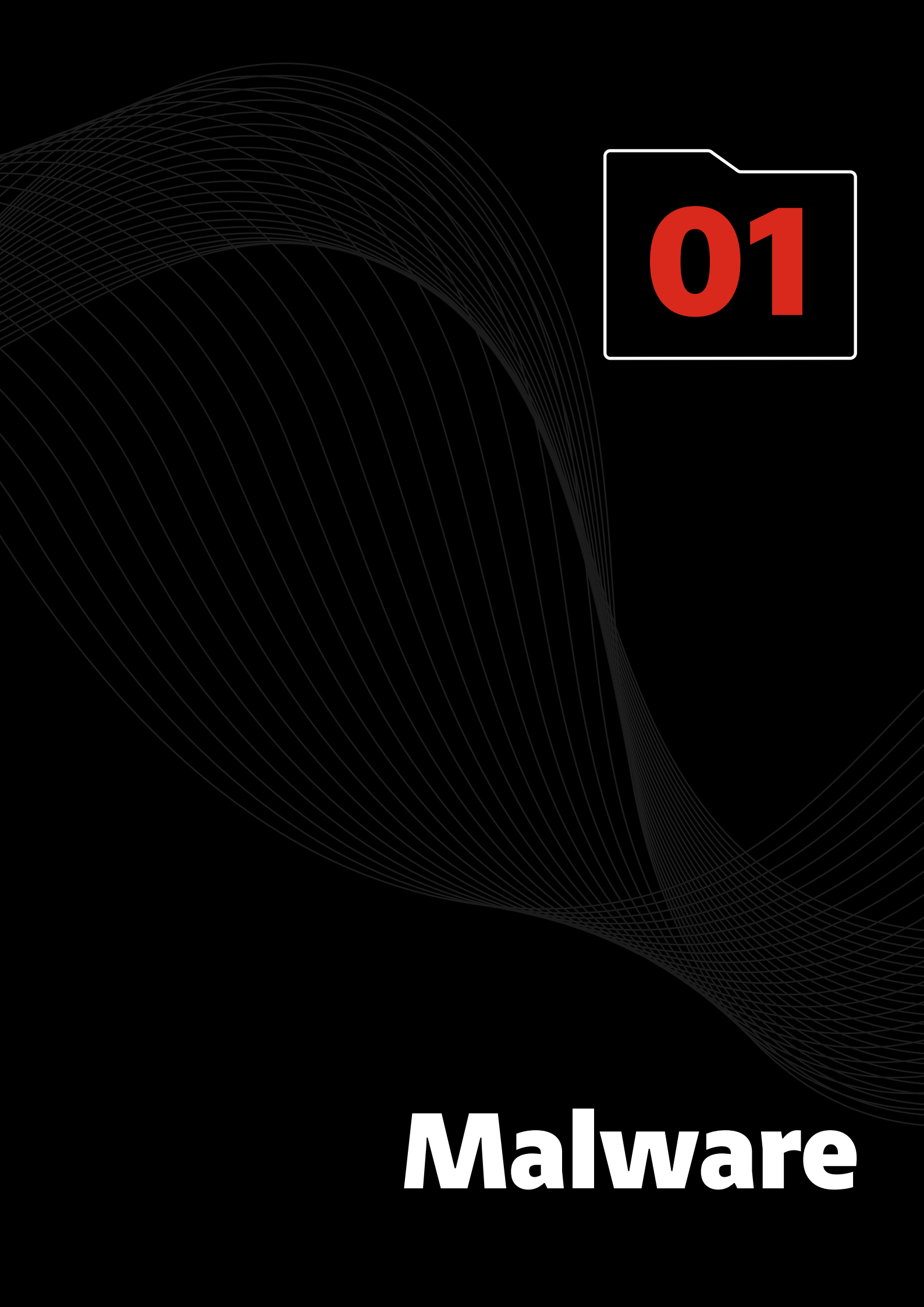
1. Malware	04
1.1 Nueva campaña de propagación de malware Remcos RAT	
1.2 Ransomware Abyss Locker ataca servidores VMware ESXi	
2. Vulnerabilidades	09
2.1 Vulnerabilidad RCE en servidores CITRIX	
3. Phishing	12
3.1 NodeStealer reaparece robando cuentas comerciales de Facebook	
4. Adversarios	15
4.1 ALPHV Ransomware adopta la integración de API	
5. Indicadores de Compromiso	18
6. Fuentes	22

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 Nueva campaña de propagación de malware Remcos RAT

Según Dr.Web, se acaba de descubrir una nueva campaña de propagación de malware que se propagan a través de sitios web fraudulentos que descargan payloads para instalar herramientas de troyanos remotos como Remcos RAT. Los registros detectados evidencian que la actividad de la campaña lleva ejecutándose aproximadamente 1 año a los usuarios de Windows.

El vector de acceso inicial utilizado en la no está claro, pero podría variar desde phishing hasta descargas automáticas y anuncios maliciosos. Los usuarios que aterrizan en los sitios web falsos se les pide que descarguen un paquete de instalación ZIP. Luego, se activa el proceso de instalación estándar, dejando caer sigilosamente el troyano Fruity, un malware basado en Python que desempaqueta un archivo MP3 ("Idea.mp3") para cargar un archivo de imagen ("Fruit.png") para activar la infección en múltiples etapas. Fruity también está diseñado para evitar la detección de antivirus en el host comprometido y, en última instancia, lanzar la carga útil Remcos RAT utilizando una técnica llamada doppelganging de procesos.

A pesar de que Trojan.Fruity está distribuyendo actualmente la aplicación de spyware Remcos RAT, los actores de amenazas pueden usar este troyano para infectar equipos con otro malware. Al mismo tiempo, este archivo malicioso puede descargarse de Internet o distribuirse junto con Trojan.Fruity como parte de los instaladores de software troyanos. Como resultado, los ciberdelincuentes tienen más oportunidades de ejecutar varios escenarios de ataque.

Esta campaña de publicidad maliciosa conduce a la propagación de malware después de la exposición inicial. Mientras permanezcan en la red de la víctima, el objetivo principal de los atacantes es obtener credenciales, establecer la persistencia en sistemas importantes y filtración de datos con la finalidad de extorsionar a sus objetivos.

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 Ransomware Abyss Locker ataca servidores VMware ESXi

Según MalwareHunterTeam, se descubrió recientemente una nueva variante del ransomware Abyss Locker diseñado específicamente para atacar servidores VMware ESXi basados en Linux. Esta variante es parte de la familia más grande de ransomware Abyss, que ha estado activa desde 2019 y se dirige a varias plataformas y sistemas.

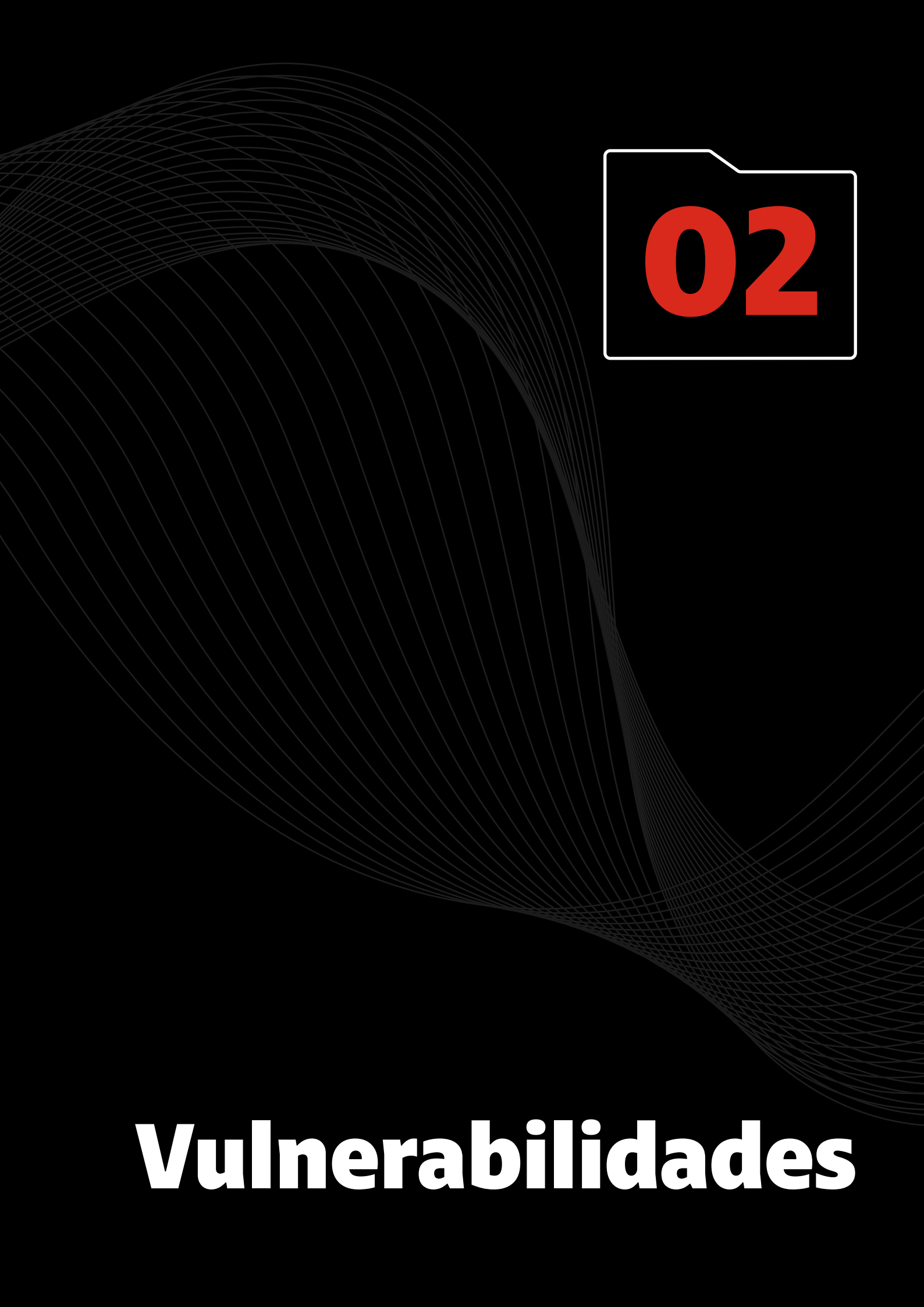
La versión Linux de Abyss Locker utiliza técnicas de ataque sofisticadas para obtener acceso no autorizado a los servidores VMware ESXi. Aprovecha los ataques de fuerza bruta SSH para explotar credenciales débiles o comprometidas para obtener acceso al sistema.

Una vez que el ransomware obtiene acceso al servidor VMware ESXi, procede a cifrar las máquinas virtuales, dejándolas inaccesibles e inutilizables. Después del cifrado, los actores de amenazas arrojan notas de rescate que exigen el pago en criptomoneda por la clave de descifrado.

El descubrimiento de la variante Linux de Abyss Locker subraya la naturaleza evolutiva de los ataques de ransomware. Además, los operadores detrás de Abyss Locker están altamente calificados y tienen un historial de lanzamiento de ataques dirigidos contra activos de alto valor.

Recomendaciones:

- › No utilizar nombres de usuario y contraseñas predeterminadas de fábrica.
- › Utilizar contraseñas robustas o complejas, mínimo 12 caracteres.
- › Ejecutar el bloqueo de los Indicadores de compromiso detallados en el ítem 5.
- › 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 authentication para correo electrónico, Active Directory, aplicaciones web y dispositivos móviles.
- › Implementar reglas YARA para escanear la memoria de los procesos recién iniciados y detectar cualquier presencia de cadenas sospechosas.
- › Implementar un control de seguridad que permita monitorear la instalación de software original proveniente de los sitios oficiales de descarga.



02

Vulnerabilidades



2.1 Vulnerabilidad RCE en servidores CITRIX

Según la publicación de Unit42 informa acerca de una nueva vulnerabilidad identificada como CVE-2023-3519, que permitiría a un atacante ejecutar secuencias de comando y control a través de un webshell PHP en dispositivos NetScaler, con el cual realizarían exfiltración de información.

En respuesta a la vulnerabilidad descubierta, CITRIX publicó en detalle las características de éste junto a los métodos de detección de explotación, controles de seguridad y la actualización que contiene el parche que mitigaría dicha vulnerabilidad.

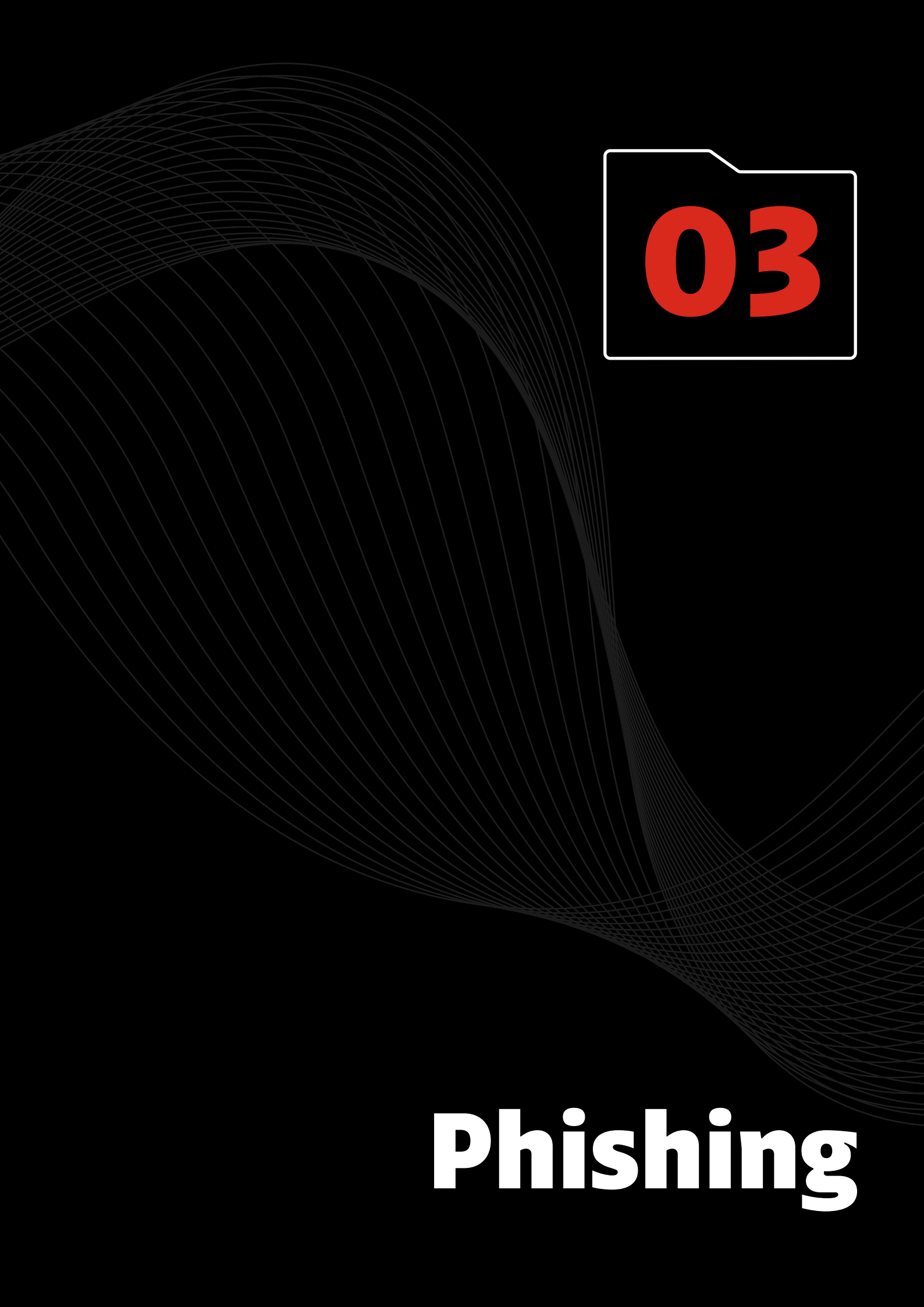
Finalmente, CITRIX recomienda a los usuarios administradores actualizar los sistemas de los dispositivos mencionados a la última versión presente con el parche de seguridad.

Productos afectados:

- Citrix NetScaler ADC y NetScaler Gateway

Recomendaciones:

- › Ejecutar las recomendaciones referentes a las vulnerabilidades corregidas por CITRIX. Para más detalle diríjase a la referencia del punto 6.4.
- › Implementar y mantener un programa de “Patch Management” (Actualizaciones de ciberseguridad) a nivel de servidores y endpoints de la organización.
- › Implementar un programa de análisis de vulnerabilidades que considere activos críticos, aplicaciones que se utilizan dentro de la organización.
- › Implementar una tecnología AntiSpam con capacidades de detección de Spam y archivos adjuntos maliciosos.



03

Phishing



3.1 NodeStealer reaparece robando cuentas comerciales de Facebook

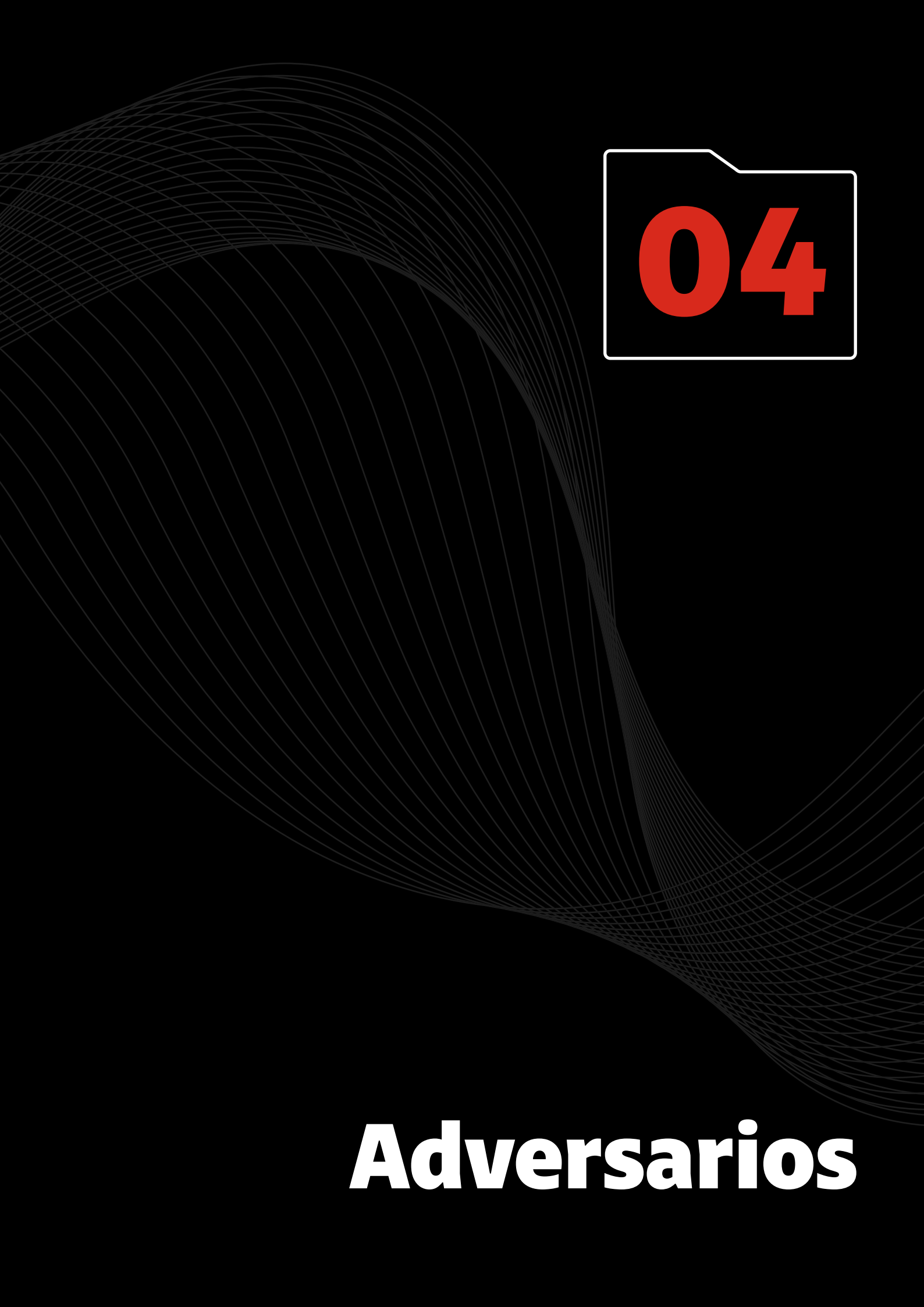
Según la investigación de Unit42, recientemente se ha descubierto una campaña de distribución de malware Infostealer con capacidades de exfiltrar datos sensibles de cuentas comerciales de Facebook; sugiriendo que esta campaña se encontraría relacionada con otra de julio del 2022 por parte de NodeStealer pero con la diferencia de que ésta ahora se encuentra escrita en python.

El principal vector de infección para el Infostealer fue una campaña de phishing dirigido a empresas, publicitando a través de páginas y usuarios de Facebook material de descarga donde se encontraría el ejecutable malicioso Infostealer. Éste, al ser ejecutado, iniciaría con un escaneo al navegador para verificar la existencia de cuentas comerciales durante la sesión, posteriormente intentaría encontrar las credenciales de acceso desde las cookies del navegador, por último, éste realizaría la exfiltración de los datos a través del api de Telegram hacia un canal asociado al actor de amenazas.

Finalmente, el Infostealer realizaría la instalación de malware adicional para incrementar sus capacidades como: deshabilitar Windows defender, manipular la cuenta de facebook y leer el contenido de los correos vinculados al dispositivo infectado.

Recomendaciones:

- › Ejecutar el bloqueo de los Indicadores de compromiso detallados en el ítem 5.
- › Ejecutar el bloqueo de los indicadores de compromiso detallados en el ítem 5.
- › Implementar un control de seguridad que tenga como alcance la detección de URLs y enlaces maliciosos como contenido de una página web.
- › Implementar soluciones avanzadas de multi factor de autenticación para el uso de aplicaciones en dispositivos móviles.
- › Implementar soluciones avanzadas de ciberseguridad tales como Next Generation Firewall con módulos de filtrado avanzado de URL, control de aplicaciones y antivirus para responder frente a los vectores de ataque email y web.
- › Desarrollar un programa de concientización para todos los usuarios sobre campañas, identificación y prevención de phishing.
- › Implementar un control de seguridad con capacidades de detección y prevención de URLs maliciosas.



04

Adversarios



4.1 ALPHV Ransomware adopta la integración de API

Según la publicación de Cyble, nos informa que el actor de amenaza ALPHV o Blackcat recientemente habilitó funciones API a su servicio bajo el modelo Ransomware as a service (RaaS) que permite a sus usuarios acceder a ransomware pre-desarrollado.

En el artículo también se mencionan los posibles usos para esta nueva API desarrollada por ALPHV, los cuales implicaría reducir la carga de procesamiento de sus servidores debido a la alta demanda de recursos que éstos presentan por parte de sus usuarios registrados.

Finalmente, la implementación de una API en un sitio de extorsión de datos genera preocupaciones, debido a los que los actores de amenaza novatos podrían explotarla con fines maliciosos, también amplía el alcance de las actividades, lo que permite a dichos actores de amenaza dirigirse a un mayor número de víctimas potenciales y fortalece.

Por último, según el fabricante Microsoft ya han revocado todas las claves de firma de MSA válidas para bloquear todos los intentos de generar nuevos tokens de acceso; sin embargo, a pesar de los cambios realizados es muy posible que los atacantes ya estén utilizando otras técnicas.

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
ACCESO INICIAL	T1078	Cuentas válidas	M1036 M1015 M1013 M1027 M1026 M1018 M1017
EJECUCIÓN	T1059	Intérprete de comandos y secuencias de comandos	M1049 M1040 M1045 M1042 M1038 M1026 M1021
	T1059	Intérprete de comandos y secuencias de comandos	M1049 M1040 M1045 M1042 M1038 M1026 M1021
ESCALACIÓN DE PRIVILEGIOS	T1548	Mecanismo de Control de Elevación de Abuso	M1047 M1038 M1028 M1026 M1022 M1052
EVASIÓN DE LA DEFENSA	T1112	Modificar Registro	M1024
	T1027	Debilitar defensas: deshabilitar o modificar herramientas	M1049 M1047 M1040
	T1562.001	Deshabilitar o modificar herramientas	M1038 M1022 M1024 M1018
IMPACTO	T1490	Inhibir la recuperación del sistema	M1053 M1028 M1018
	T1489	Parada de servicio	M1030 M1022 M1024 M1018
	T1486	Datos cifrados para impacto	M1040 M1053

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 6.18 del boletín.
- › Ejecutar el bloqueo de los indicadores de compromiso detallados en el ítem 5.
- › Tercerizar un servicio de MDR que permita la detección y respuesta ante cualquier incidente con alcance 24x7x365.
- › Implementar un software EDR con capacidades de Machine Learning e IA que permitan la detección de anomalías en el sistema en los puntos finales.
- › Implementar una solución que permita la autenticación multifactor con alcance en todos los activos de la organización a nivel de login y uso de aplicaciones.
- › Implementar o tercerizar un servicio de Inteligencia de amenazas con la finalidad de identificar oportunamente indicadores de compromiso relacionados con el sector de la organización.
- › Implementar un software Antivirus de última generación que considere todos los puntos finales de la organización.

Indicadores de compromiso

5.1 IPs

62[.]197.48.186 (Ítem Malware: 1.1)
37[.]1.221.132 (Ítem Malware: 1.1)
65[.]108.244.82 (Ítem Malware: 1.1)
37[.]1.221.249 (Ítem Malware: 1.1)
216[.]41.162.172 (Ítem Vulnerabilidades: 2.1)
216[.]51.171.17 (Ítem Vulnerabilidades: 2.1)
185[.]220.102.253 (Ítem Adversarios: 4.1)
31[.]44.184.84 (Ítem Adversarios: 4.1)
45[.]227.253.98 (Ítem Adversarios: 4.1)
45[.]227.253.99 (Ítem Adversarios: 4.1)
45[.]227.253.107 (Ítem Adversarios: 4.1)
104[.]243.41.123 (Ítem Adversarios: 4.1)
185[.]99.135.115 (Ítem Adversarios: 4.1)
45[.]61.138.109 (Ítem Adversarios: 4.1)
185[.]141.62.123 (Ítem Adversarios: 4.1)
45[.]227.253.106 (Ítem Adversarios: 4.1)

5.2 DOMINIO

more-power-tool[.]com (Ítem Malware: 1.1)
ryzen-master[.]com (Ítem Malware: 1.1)
atiflash[.]ru (Ítem Malware: 1.1)
polaris-bios-editor[.]ru (Ítem Malware: 1.1)
btc-tools[.]ru (Ítem Malware: 1.1)
techpowerup-gpu-z[.]com (Ítem Malware: 1.1)
sapphire trixx[.]com (Ítem Malware: 1.1)
srbpolaris[.]ru (Ítem Malware: 1.1)
clockgen64[.]com (Ítem Malware: 1.1)
balena-etcher[.]com (Ítem Malware: 1.1)
nvidiaInspector[.]ru (Ítem Malware: 1.1)
riva-tuner[.]com (Ítem Malware: 1.1)
atikmdagpatcher[.]com (Ítem Malware: 1.1)
overdriventool[.]ru (Ítem Malware: 1.1)
secure-rbcbank[.]net (Ítem Adversarios: 4.1)

5.3 URL

hxxps://tinyurl[.]com/batkyc (Ítem Phishing: 3[.]1)
hxxps://tinyurl[.]com/ratkyc2 (Ítem Phishing: 3[.]1)
hxxp://adgowin66[.]site/ratkyc/4/bat[.]zip (Ítem Phishing: 3[.]1)
hxxp://adgowin66[.]site/ratkyc/4/ratkyc[.]zip (Ítem Phishing: 3[.]1)
hxxps://172[.]86[.]123[.]127:8443/work2z (Ítem Adversarios: 4[.]1)
hxxps://172[.]86[.]123[.]226:8443/work3z (Ítem Adversarios: 4[.]1)
hxxps://events[.]drdivyaclinic[.]com/ (Ítem Adversarios: 4[.]1)
hxxps://193[.]42[.]32[.]58:8443/work2z (Ítem Adversarios: 4[.]1)
hxxps://procurri[.]org/ (Ítem Adversarios: 4[.]1)
hxxp://www[.]threatmon[.]io/ (Ítem Adversarios: 4[.]1)
hxxps://64[.]227[.]80[.]81/ (Ítem Adversarios: 4[.]1)
hxp://185[.]141[.]62[.]123[:]10228/update[.]exe (Ítem Adversarios: 4[.]1)

5.4 EMAIL

ralph.barreiro@consultingservice.shop (Ítem Adversarios: 4.1)
farusbig@tutanota.com (Ítem Adversarios: 4.1)
phandaledr@onionmail.org (Ítem Adversarios: 4.1)
angelralphvhentetrez@yahoo.com (Ítem Adversarios: 4.1)
ralphvanhoutem@yahoo.com (Ítem Adversarios: 4.1)
blackcat001@gmail.com (Ítem Adversarios: 4.1)
blackcat.myako@gmail.com (Ítem Adversarios: 4.1)

5.5 Hashes

(Ítem Malware: 1.1)

SHA256:e9262441ef8e401acce28d13100c63e90e3de2ffb0ec6763611eebdc1aa60dbd

MD5:cbf3222386c700fa260fea086193af

SHA256:4bba89c86c316afef869c0360fbc91946eb8a92a0168eb67d8f7cc7d5f0ad04b

MD5:868091ae8a185d9c98ec9828d76242c3

SHA256:1076ddd7e6fe20814b354fe9ea5f6becf4fdc3cb836cafd8fda2feae756a686

MD5:09516548a6dbf6193be55683f8bed52f

SHA256:0c8c431a1f589fdcf453c7afada63c2e2e2a887e49abdbb222983fa6044fdf66

MD5:0bd497e905a9ebd04eb0ec6adaf27a23

SHA256:62f9501d1ecd2fe15b6330aa1a08964be89ccb75106f3797d35d8908cfdc62d2

MD5:5b6c3a0797b578850cf380334e96b914

SHA256:fef86b6fd9bc5dd19f1121afe600a0bb36f5950e60f89e349305102aa13ffb12

MD5:9dd5355186c0fca00dfbc781e5699444

SHA256:7cde707a08ebdec6e8b52826113f85eb1bedb2db1dc5130fc5a4432a1825155f

MD5:aa331b442f0d28086997c9cb60c0e99e

SHA256:0effd2071b2a997159066d3aeb1d5f0f6b041900e6461df475835b168c7e38b2

MD5:d1705ac9c378a0026d41339e814e72c8

SHA256:a79f980e1b093f0700b9ffc7f3b075f24c5dd889f6a34fe428f305dd8e6f2dda

MD5:e77cc49d823c19842003bb0c9dc6f61d

SHA256:ebddd0bb9b41fb1ac46b15049885b53367a19dcba91f5b1a2b447a9dbf3d8c0e

MD5:ccc33245047087d4bc508bfe33d82c11

(Ítem Vulnerabilidades: 2.1)

SHA256:293fe23849cffb460e8d28691c640a5292fd4649b0f94a019b45cc586be83fd9

MD5:0377dc9c7cfcd1e64598c619821ca114

(Ítem Phishing: 3.1)

SHA256:fb887dbcbac146adde68ae15bf0fadab144f2ed60e2db62a6acf5f13e31b80e

MD5:dd672d466ab73c3938c47dda527aa1c1

SHA256:80547ae27cc389bede392ea34503553304c44f72fe7d4ff4f4375baf42a0e60b

MD5:8396176caef1e8af00d93fdf3b0846f4

SHA256:1a4e8bcf7dc4ad7215957210c8e047f552b45a70daf3d623436940979c38f94c

MD5:7b979b43eebeb4b9969312695601dab1

SHA256:92657c3a108bbedc6f05b4af0a174e99a58e51e69c15c707d9c9cc63cdf1b4ea
MD5:f135f1d24ad1cf2dd000a3eed2e7b681

SHA256:fed5ea7840461984fa40784d84ed1a0961cbf48b03d8b79c522286bf6e220922
MD5:2dc8f6c04d059348451cf38c798b5732

SHA256:1f093f818d2d3bd146c34d10bdb9de0a33931d3586f0bb942f881052a20114f9
MD5:f1635f9ebb4b136a1268bf36ebd86857

SHA256:14000dc5c64ad50e534739afa86ce37c30b04a8aba48feb0f645b0a74b545744
MD5:8ed38dbacdd411b07e471ce60b83a82c

(Ítem Adversarios: 4.1)

SHA256:731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161
MD5:173c4085c23080d9fb19280cc507d28d

SHA256:b809d6c1d643d1206ebaa1289ab38c20f4dceffd144a0131c7ea49943d26e683
MD5:fcf3a6eeb9f836315954dae03459716d

SHA256:94a8e1332402f01e5bcf9be8d7ccd0e434507d72958eb326b9bd9831a3be71f8
MD5:4d7153e88f96df3206163977a9d0d1a8

SHA256:52d5c35325ce701516f8b04380c9fbb78ec6bcc13b444f758fdb03d545b0677
MD5:a837302307dace2a00d07202b661bce2

SHA256:31eb1de7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fc
MD5:a3cb3b02a683275f7e0a0f8a9a5c9e07

SHA256:9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff
MD5:9880fae6551d1e9ee921f39751a6f3c0

SHA256:40da7968b86654b9af30178540a4cacaf1c61476c4fcb95e438697bb5e47854f
MD5:392cbe841c7bb1ead1a00213e750648c

Fuentes

- 6.1 <https://thehackernews.com/2023/07/fruity-trojan-uses-deceptive-software.html>
- 6.2 <https://cyware.com/news/vmware-esxi-servers-face-new-threat-from-abyss-locker-086083>
- 6.3 <https://unit42.paloaltonetworks.com/threat-brief-citrix-cve-2023-3519/>
- 6.4 <https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467>
- 6.5 <https://unit42.paloaltonetworks.com/nodestealer-2-targets-facebook-business/>
- 6.6 <https://cyble.com/blog/alphv-ransomware-data-leak-site-embrace-api-integration/>
- 6.7 <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-201a>
- 6.8 <https://attack.mitre.org/techniques/T1078/>
- 6.9 <https://attack.mitre.org/techniques/T1059/>
- 6.10 <https://attack.mitre.org/techniques/T1059/>
- 6.11 <https://attack.mitre.org/techniques/T1548/>
- 6.12 <https://attack.mitre.org/techniques/T1112/>
- 6.13 <https://attack.mitre.org/techniques/T1027/>
- 6.14 <https://attack.mitre.org/techniques/T1562/001/>
- 6.15 <https://attack.mitre.org/techniques/T1562/001/>
- 6.16 <https://attack.mitre.org/techniques/T1490/>
- 6.17 <https://attack.mitre.org/techniques/T1489/>
- 6.18 <https://attack.mitre.org/techniques/T1486/>



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".