

05 de octubre, 2023

# Boletín Ciberseguridad

## CLARO EMPRESAS

BOLETÍN SEMANAL #103

Claro empresas

# Beneficios y riesgos en la administración de parches

Según la publicación de Fortra, el auge de las amenazas cibernéticas está haciendo que cada vez los activos críticos de la organización se vean expuestos a riesgos cibernéticos propensos a convertirse en incidentes de seguridad. Por lo mismo, ante la exposición de los activos en la superficie de ataque puede ocasionar que los ciberdelincuentes identifiquen los servicios asociados y con ello encontrar la forma de explotar las vulnerabilidades encontradas con el propósito de afectar los activos.

Por ello, es importante poder identificar debilidades de los activos con el fin de aplicar los parches correspondientes para subsanarlos y mitigar el riesgo que sean vulnerados y pueda afectar económicamente y reputacional a la organización.

En consecuencia, siempre hay beneficios y riesgos que se pueden presentar durante el proceso, entre ellos:

**Beneficios:**
- Corregir fallas de seguridad o errores, contravenir cualquier intento de vulneración por parte de los adversarios.
- Activos de infraestructura crítica, pueden ser los más beneficiados cuando se corrijan los errores a tiempo
- Mejorar la estabilidad de las aplicaciones

**Riesgos:**
- Indisponer un activo cuando se aplique un parche no compatible o corrupto
- El costo asociado de probar los parches lanzados por los fabricantes
- La indisponibilidad que pueda poner a un activo para desplegar el parche correspondiente

Por último, es importante recalcar que la gestión de vulnerabilidades es más que recibir alertas cada vez que activo dentro de la infraestructura necesite un parche, es prioritario considerar qué activos prescinden de un parche y cómo mitigarlo, posiblemente se tenga que incorporar la telemetría como un recurso para tener visibilidad.

**Fuente:**
https://www.tripwire.com/state-of-security/patch-management-ics-environments

# Índice


**1. Malware** 03

1.1 BunnyLoader, el nuevo malware que se vende como servicio en múltiples foros

1.2 Zanubis, el troyano bancario que está afectando fuertemente a entidades financieras

**2. Vulnerabilidades** 08

2.1 Exploit disponible para error crítico WS_FTP Server

**3. Phishing** 11

3.1 Actor de amenazas utiliza EvilProxy para ataques de phishing

**4. Adversarios** 14

4.1 Grupo de ransomwaare Dark Angels realiza ataque dirigido de gran magnitud

**5. Indicadores de Compromiso** 20

**6. Fuentes** 26


# Prioridad

Crítica Alta Media




# Malware




## 1.1 BunnyLoader, el nuevo malware que se vende como servicio en múltiples foros

Según la publicación de Zscaler, ha aparecido un nuevo malware catalogado como "BunnyLoader", el mismo que se está vendiendo en varios foros. Este malware tiene varias funcionalidades, dentro de las cuales se encuentran la descarga y carga útil de segunta etapa, la extracción de credenciales del navegador, así como del sistema, entre otros, para luego una vez obtenida la información enviarlo a un servidor C2.

Como parte característica del malware se encuentra que emplea varias técnicas anti-sandbox evitando ser detectado por los controles de seguridad. Además, como parte del modus operandi del malware se encuentra la descarga y ejecución de malware adicional, registro de teclas, robo de credenciales, así como la ejecución de comandos remotos en el equipo infectado.

Finalmente, puntualizar que este malware recopila la información en archivos .txt respecto al equipo de la víctima incluyendo su ubicación, Así mismo, información propia del sistema como el historial del navegador para luego comprimirlo en un archivo ZIP y enviarlo al servidor C2.

## Recomendaciones:

- Ejecutar el bloqueo de los Indicadores de compromiso detallados en el ítem 5.
- Implementar una solución antimalware en todos los puntos finales
- Implementar un plan de capacitación para los usuarios de la organización en temas sobre las fuentes de amenazas
- Implementar como política de seguridad la segmentación de redes con el fin de mitigar el riesgo cuando haya un intento de ataque
- Implementar políticas de seguridad para el uso de contraseñas fuertes basado en la norma NIST
- Implementar como parte de las políticas de seguridad el marco de trabajo Zero-Trust

## 1.2 Zanubis, el troyano bancario que está afectando fuertemente a entidades financieras

Según la investigación de SecureList, existe un troyano bancario que se hace llamar “Zanubis”, este malware tiene como target el sector financiero de Perú. La forma como se propaga, lo hace a través de aplicaciones legítimas para Android y solicitando al usuario la habilitación de accesibilidad para tomar el control del dispositivo.

Además, como parte de la información se menciona que este malware utiliza la aplicación de la SUNAT para disfrazarse y lograr su cometido; Además, una vez otorga accesibilidad a la aplicación maliciosa permitiendo ejecutarse en segundo plano y utiliza WebView para cargar un sitio web de SUNAT legítima para buscar deudas. El objetivo aquí es llevar al usuario desprevenido a creer que la aplicación es parte del ecosistema de servicios de SUNAT.

Por último, una vez realizada la infección el malware va a comunicarse con un servidor C2 para robar información de la víctima, así como registrar eventos/claves o también grabar la pantalla. Igual, otro punto interesante de este troyano es que pretende ser una actualización de Android logrando bloquear el teléfono; entonces, a medida que se ejecuta la actualización el dispositivo permanece inutilizable a tal punto que no se puede bloquear y desbloquear como consecuencia de que el malware monitorea los intentos y los bloquea. El contenido de la publicación hace mención que este troyano está orientado a entidades financieras de Perú, siendo preponderante que el malware es capaz de infectar cualquier teléfono Android.

## Recomendaciones:

- Ejecutar el bloqueo de los Indicadores de compromiso detallados en el ítem 5.
- Implementar un control de seguridad de detección y prevención de malware en todos los dispositivos móviles de la organización
- Implementar un plan de capacitación orientado a temas de detección y prevención de malware con alcance para todos los usuarios
- Implementar programas de concientización para todos los usuarios en temas de salvaguarda de la información
- Implementar la política de doble factor de autenticación para todas las aplicaciones utilizadas en los dispositivos móviles corporativos
- Encriptar la información de los dispositivos móviles considerados como críticos




# Vulnerabilidades



## 2.1 Exploit disponible para error crítico WS_FTP Server

De acuerdo con el portal BleepingComputer, investigadores de Assetnote publicaron un exploit de prueba de concepto para una vulnerabilidad de ejecución remota de código de máxima gravedad en la plataforma de intercambio de archivos WS_FTP Server de Progress Software.

La vulnerabilidad catalogada como CVE-2023-40044, descubierto y reportado por investigadores de Assetnote, es una deserialización de .NET que podría permitir que un atacante no autenticado ejecute comandos remotos en el sistema operativo subyacente del servidor WS_FTP y puede explotarse mediante una solicitud HTTPS POST. Progress indica que las instalaciones del servidor WS_FTP sin el módulo de transferencia ad hoc instalado no son vulnerables

Productos afectados:

| PRODUCTO | VERSIÓN(ES) |
|---|---|
| VMware Aria Operation for Networks | 6.2 / 6.3 / 6.4 / 6.5.1 / 6.6 / 6.7 / 6.8 / 6.9 / 6.10 |

## Recomendaciones:

- Evaluar la actualización WS_FTP Server a la versión 8.8.2 parcheada utilizando el instalador completo previo análisis de impacto.
- Eliminar o deshabilitar el Módulo de transferencia ad hoc para el servidor WS_FTP si no está en uso.
- Considere la implementación un WAF para monitorear y filtrar las solicitudes HTTP y HTTPS entrantes




# Phishing



## 3.1 Actor de amenazas utiliza EvilProxy para ataques de phishing

Según informa BleepingComputer, se descubrió una campaña de phishing recientemente que estaría dirigida a cuentas de Microsoft 365 de ejecutivos clave en organizaciones de la región América, utilizando redireccionamientos abiertos desde el sitio web de empleo de Indeed para ofertas de trabajo.

Según los investigadores de Menlo Security, sugieren que el actor de amenazas utiliza el servicio de phishing EvilProxy que puede recopilar cookies de sesión, que se pueden usar para eludir los mecanismos de autenticación multifactor (MFA). También informan que los objetivos de esta campaña de phishing son ejecutivos y empleados de alto rango de diversas industrias, incluida la fabricación electrónica, banca y finanzas, bienes raíces, seguros y administración de propiedades.

Los objetivos reciben correos electrónicos con un enlace indeed.com que parece legítimo. Cuando se accede a ella, la dirección URL lleva al usuario a un sitio de phishing que actúa como proxy inverso para la página de inicio de sesión de Microsoft. Cuando el usuario accede a su cuenta a través de este servidor de phishing, el actor de amenazas puede capturar las cookies de autenticación permitiéndoles el acceso completo a la cuenta de la víctima.

Finalmente, el uso de kits de proxy inverso para phishing está creciendo y combinarlos con redireccionamientos abiertos a sitios auténticos aumenta el éxito de una campaña.

## Recomendaciones:

- Ejecutar el bloqueo de los Indicadores de compromiso detallados en el ítem 5.
- Implementar un control de seguridad con capacidad de detección y prevención de ataques de phishing.
- Implementar un software XDR con alcance a todos los puntos finales de la organización
- Desarrollar un programa de capacitación considerando temas de detección y prevención de ataques
- de phishing con alcance a todos los usuarios de la organización.
- Implementar o tercerizar un servicio de ASM (Attack Surface Management) con el propósito de detectar vulnerabilidades en los activos críticos expuestos en la superficie de ataque
- Tercerizar un servicio de SOC (Security Operations Center) con alcance 24x7x365.




# Adversarios



## 4.1 Grupo de ransomwaare Dark Angels realiza ataque dirigido de gran magnitud

Según la publicación de Bitdefender, informa que la compañía Johnson Controls sufrió un ataque de ransomware durante el fin de semana que dejó datos cifrados y provocó que cerrara secciones de su infraestructura de TI.

La compañía confirmó en un informe ante la comisión de Bolsa y Valores de Estados unidos- que había "experimentado interrupciones en partes de su infraestructura y aplicaciones internas de TI" como resultado del ataque cibernético. El grupo de ransomware Dark Angels se ha atribuido la responsabilidad del ataque y afirma haber exfiltrado más de 25 TB de datos de la organización, con los cuales exige un pago por rescate de $ 51 millones de dólares.

Finalmente, Johnson Controls mencionó que el ataque suscitado se encuentra provocando la interrupción de partes de las operaciones comerciales de la compañía, y aunque se desconoce el impacto real del ataque, se espera consecuencias financieras.

A continuación, se muestran las TTPs del adversario Dark Angels

**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 |
|---|---|---|---|
| RECONOCIMIENTO | T1589 | Recopilar información de identidad de la víctima | M1056 |
| | T1590 | Recopilar información de la red de víctimas | |
| ACCESO INICIAL | T1566 | Phishing | M1049<br>M1031<br>M1021<br>M1054<br>M1017 |
| | T1078 | Cuentas válidas | M1036<br>M1015<br>M1013<br>M1027<br>M1026<br>M1018<br>M1017 |
| ACCESO A CREDENCIALES | T1110 | Fuerza bruta | M1036<br>M1032<br>M1027<br>M1018 |
| | T1555 | Credenciales de almacenes de contraseñas | M1027 |
| | T1003 | Volcado de credenciales del sistema operativo | M1015<br>M1040<br>M1043<br>M1041<br>M1028<br>M1027<br>M1026<br>M1025<br>M1017 |
| | T1552 | Credenciales no seguras | M1015<br>M1047<br>M1041<br>M1037<br>M1035<br>M1028<br>M1027<br>M1026<br>M1022<br>M1051<br>M1017 |

| TÁCTICA | Técnica (ID) | Nombre de la Técnica | Mitigación |
|---|---|---|---|
| EJECUCIÓN | T1047 | Instrumental de administración de Windows | M1040<br>M1038<br>M1026<br>M1018 |
| PERSISTENCIA | T1505 | Componente de software de servidor | M1047<br>M1045<br>M1042<br>M1026<br>M1024<br>M1018 |
| | T1078 | Cuentas válidas | M1036<br>M1015<br>M1013<br>M1027<br>M1026<br>M1018<br>M1017 |
| ESCALADA DE PRIVILEGIOS | T1068 | Explotación para la escalada de privilegios | M1048<br>M1038<br>M1050<br>M1019<br>M1051 |
| | T1078 | Cuentas válidas | M1036<br>M1015<br>M1013<br>M1027<br>M1026<br>M1018<br>M1017 |
| EVASIÓN DE DEFENSA | T1078 | Cuentas válidas | M1036<br>M1015<br>M1013<br>M1027<br>M1026<br>M1018<br>M1017 |
| DESCUBRIMIENTO | T1087 | Descubrimiento de cuentas | M1028 |
| | T1135 | Descubrimiento de recursos compartidos de red | |
| | T1083 | Descubrimiento de archivos y directorios | - |
| | T1018 | Descubrimiento de sistemas remotos | - |
| | T1518 | Descubrimiento de software | - |
| | T1016 | Descubrimiento de configuración de red del sistema | - |
| | T1033 | Descubrimiento del propietario/usuario del sistema | - |

| TÁCTICA | Técnica (ID) | Nombre de la Técnica | Mitigación |
|---|---|---|---|
| MOVIMIENTO LATERAL | T1021 | Servicios remotos | M1032<br>M1018 |
| COLECCIÓN | T1005 | Datos del sistema local | M1057 |
| | T1039 | Datos de la unidad compartida de red | - |
| EXFILTRACIÓN | T1011 | Exfiltración sobre otro medio de red | M1028 |
| | T1537 | Transferir datos a la cuenta en la nube | M1037<br>M1027<br>M1018 |
| IMPACTO | T1485 | Destrucción de datos | M1053 |
| | T1486 | Datos cifrados para el impacto | M1040<br>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 6.10 hasta el punto 6.34 del boletín.
- Ejecutar el bloqueo de los indicadores de compromiso detallados en el ítem 5.
- Implementar o tercerizar un servicio de Inteligencia de Amenazas con alcance 24x7x365.
- Implementar como política de seguridad la segmentación de redes para la prevención de intrusos.
- Desarrollar un plan de detección y respuesta como medida de prevención de ataques cibernéticos.
- Desarrollar un plan de capacitaciones para todos los usuarios de la organización considerando temas como “La importancia de salvaguardar la información de la organización”.
- Tercerizar un servicio de MDR (Managed Detection and Response) con alcance 24x7x365 incluyendo tiempos de respuesta de acuerdo con la criticidad de los incidentes de seguridad.

# Indicadores de compromiso

## 5.1 IPs

37[.]139[.]129[.]145 (Ítem Malware: 1.1)
5[.]252[.]176[.]205 (Ítem Malware: 1.2)
116[.]202[.]2[.]169 (Ítem Malware: 1.2)
116[.]203[.]121[.]140 (Ítem Malware: 1.2)
112[.]189[.]64[.]185 (Ítem Malware: 1.2)
198[.]23[.]217[.]172 (Ítem Malware: 1.2)
161[.]179[.]250[.]142 (Ítem Malware: 1.2)
19[.]69[.]67[.]172 (Ítem Malware: 1.2)
100[.]142[.]222[.]52 (Ítem Malware: 1.2)
7[.]203[.]67[.]172 (Ítem Malware: 1.2)
48[.]54[.]16[.]104 (Ítem Malware: 1.2)
9[.]169[.]203[.]54 (Ítem Malware: 1.2)
53[.]121[.]117[.]34 (Ítem Malware: 1.2)
7[.]173[.]189[.]20 (Ítem Malware: 1.2)
23[.]137[.]64[.]172 (Ítem Malware: 1.2)
195[.]23[.]217[.]172 (Ítem Malware: 1.2)
187[.]30[.]213[.]3 (Ítem Malware: 1.2)
106[.]38[.]67[.]172 (Ítem Malware: 1.2)
48[.]28[.]21[.]104 (Ítem Malware: 1.2)
48[.]53[.]16[.]104 (Ítem Malware: 1.2)
110[.]208[.]58[.]216 (Ítem Malware: 1.2)
101[.]57[.]16[.]104 (Ítem Malware: 1.2)
139[.]7[.]26[.]104 (Ítem Malware: 1.2)
98[.]39[.]251[.]142 (Ítem Malware: 1.2)
9[.]109[.]16[.]96 (Ítem Malware: 1.2)
175[.]87[.]235[.]185 (Ítem Malware: 1.2)
78[.]190[.]64[.]185 (Ítem Malware: 1.2)
201[.]181[.]244[.]35 (Ítem Malware: 1.2)
135[.]240[.]123[.]52 (Ítem Malware: 1.2)
62[.]144[.]67[.]172 (Ítem Malware: 1.2)
53[.]135[.]120[.]34 (Ítem Malware: 1.2)
126[.]157[.]241[.]8 (Ítem Malware: 1.2)
211[.]245[.]197[.]18 (Ítem Malware: 1.2)
100[.]139[.]222[.]52 (Ítem Malware: 1.2)
131[.]179[.]250[.]142 (Ítem Malware: 1.2)
119[.]223[.]16[.]50 (Ítem Malware: 1.2)
170[.]179[.]250[.]142 (Ítem Malware: 1.2)
13[.]7[.]250[.]178 (Ítem Malware: 1.2)
217[.]12[.]206[.]230 (Ítem Malware: 1.2)
95[.]143[.]190[.]57 (Ítem Malware: 1.2)
77[.]91[.]84[.]52 (Ítem Phishing: 3.1)

185[.]241[.]52[.]78 (Ítem Phishing: 3.1)
212[.]224[.]107[.]12 (Ítem Phishing: 3.1)
185[.]250[.]243[.]38 (Ítem Phishing: 3.1)
185[.]250[.]243[.]176 (Ítem Phishing: 3.1)
185[.]241[.]52[.]78 (Ítem Phishing: 3.1)
185[.]250[.]243[.]176 (Ítem Phishing: 3.1)
185[.]250[.]243[.]38 (Ítem Phishing: 3.1)
212[.]224[.]107[.]12 (Ítem Phishing: 3.1)
77[.]91[.]84[.]52 (Ítem Phishing: 3.1)
193.142.30[.]17 (Ítem Adversarios: 4.1)
193.142.30[.]154 (Ítem Adversarios: 4.1)
94.135.24[.]241 (Ítem Adversarios: 4.1)
45.182.189[.]105 (Ítem Adversarios: 4.1)
45.182.189[.]106 (Ítem Adversarios: 4.1)
78.128.112[.]139 (Ítem Adversarios: 4.1)
109.172.45[.]28 (Ítem Adversarios: 4.1)
109.172.45[.]77 (Ítem Adversarios: 4.1)

## 5.2 DOMINIO

liveswords[.]xyz (Ítem Malware: 1.2)
browserupdate[.]zip (Ítem Malware: 1.2)
magydostravel[.]com (Ítem Malware: 1.2)
45[.]9[.]74[.]182[.]figure (Ítem Malware: 1.2)
stats-best[.]site (Ítem Malware: 1.2)
wnimodmoiejn[.]site (Ítem Malware: 1.2)
orkograkula[.]fun (Ítem Malware: 1.2)
parrotorsk[.]fun (Ítem Malware: 1.2)
blockbeerman[.]fun (Ítem Malware: 1.2)
morevita-my[.]xyz (Ítem Malware: 1.2)
tritonbody[.]fun (Ítem Malware: 1.2)
mycollection-my[.]xyz (Ítem Malware: 1.2)
followertv[.]fun (Ítem Malware: 1.2)
khel999[.]com (Ítem Malware: 1.2)
lookingthroughtheturn[.]com (Ítem Malware: 1.2)
documents[.]notificationsapps[.]com (Ítem Malware: 1.2)
select-holidays[.]com (Ítem Malware: 1.2)
ocmtancmi2c5t[.]xyz (Ítem Malware: 1.2)
gapi-node[.]io (Ítem Malware: 1.2)
activeglucol[.]zip (Ítem Malware: 1.2)
booxshistr[.]xyz (Ítem Malware: 1.2)
u0026up[.]page (Ítem Malware: 1.2)
openh264-win64-2e1774ab6dc6c43debb0b5b628bdf122a391d521[.]zip (Ítem Malware: 1.2)
126[.]157[.]241[.]8[.]in-addr[.]arpa (Ítem Malware: 1.2)
1private[.]pro (Ítem Malware: 1.2)

vipcloud-my[.]xyz (Ítem Malware: 1.2)
aloowforest[.]xyz (Ítem Malware: 1.2)
traftech[.]pro (Ítem Malware: 1.2)
slading[.]xyz (Ítem Malware: 1.2)
jornesfree[.]xyz (Ítem Malware: 1.2)
modifesistem[.]xyz (Ítem Malware: 1.2)
promomilk[.]xyz (Ítem Malware: 1.2)
jxh[.]us (Ítem Phishing: 3.1)
andrealynnsanders[.]com (Ítem Phishing: 3.1)
chiromaflo[.]com (Ítem Phishing: 3.1)
na-7[.]com (Ítem Phishing: 3.1)
dl2b[.]com (Ítem Phishing: 3.1)
cmzo-eu[.]cz (Ítem Phishing: 3.1)
dsena[.]net (Ítem Phishing: 3.1)
pbcinvestment[.]com (Ítem Phishing: 3.1)
nilyn[.]us (Ítem Phishing: 3.1)
kofisch[.]com (Ítem Phishing: 3.1)
farmacgroup[.]ca (Ítem Phishing: 3.1)
ae-lrmed[.]com (Ítem Phishing: 3.1)
837[.]best (Ítem Phishing: 3.1)
fdh[.]aero (Ítem Phishing: 3.1)
ssidaignostica[.]com (Ítem Phishing: 3.1)
concursolution[.]us (Ítem Phishing: 3.1)
wattsmed[.]com (Ítem Phishing: 3.1)
nilyn[.]us (Ítem Phishing: 3.1)
na-7[.]com (Ítem Phishing: 3.1)
wattsmed[.]com (Ítem Phishing: 3.1)
farmacgroup[.]ca (Ítem Phishing: 3.1)
ae-lrmed[.]com (Ítem Phishing: 3.1)
ssidaignostica[.]com (Ítem Phishing: 3.1)
837[.]best (Ítem Phishing: 3.1)
dsena[.]net (Ítem Phishing: 3.1)
fdh[.]aero (Ítem Phishing: 3.1)
dl2b[.]com (Ítem Phishing: 3.1)
kofisch[.]com (Ítem Phishing: 3.1)
jxh[.]us (Ítem Phishing: 3.1)
andrealynnsanders[.]com (Ítem Phishing: 3.1)
cmzo-eu[.]cz (Ítem Phishing: 3.1)
concursolution[.]us (Ítem Phishing: 3.1)
pbcinvestment[.]com (Ítem Phishing: 3.1)
chiromaflo[.]com (Ítem Phishing: 3.1)
malware[.]in (Ítem Phishing: 3.1)
p66slxmtum2ox4jpayco6ai3qfehd5urgrs4oximjzklxcol264driqd.onion (Ítem Adversarios: 4.1)

## 5.3 URL

hxxp[:]//37[.]139[.]129[.]145/Bunny/Echoer.php (Ítem Malware: 1.1)
hxxp[:]//37[.]139[.]129[.]145/Bunny/ResultCMD.php (Ítem Malware: 1.1)
hxxps[:]//5[.]252[.]176[.]205:8000/ (Ítem Malware: 1.2)
hxxp[:]//116.202.2.169[:]1333/ (Ítem Malware: 1.2)
hxxps[:]//magydostravel[.]com/cdn/zwmrqqgqnaww[.]php (Ítem Malware: 1.2)
hxxp[:]//liveswords[.]xyz/c2conf (Ítem Malware: 1.2)
hxxp[:]//yachtracingopt[.]fun/api (Ítem Malware: 1.2)
hxxp[:]//firmpanacewa[.]fun/ (Ítem Malware: 1.2)
hxxp[:]//116[.]203[.]121[.]140/eee[.]exe (Ítem Malware: 1.2)
hxxp[:]//castomdroms[.]xyz/c2conf (Ítem Malware: 1.2)
hxxp[:]//closhemone[.]fun/c2conf (Ítem Malware: 1.2)
hxxp[:]//astrolco[.]fun/ (Ítem Malware: 1.2)
hxxp[:]//curtainjors[.]fun/ (Ítem Malware: 1.2)
hxxp[:]//116[.]203[.]121[.]140/eee[.]exe (Ítem Malware: 1.2)
hxxp[:]//funnycox[.]fun/ (Ítem Malware: 1.2)
hxxp[:]//valleydod[.]fun/ (Ítem Malware: 1.2)
hxxp[:]//choserowboatfly[.]fun/ (Ítem Malware: 1.2)
hxxp[:]//boothroundupdow[.]fun/ (Ítem Malware: 1.2)
hxxp[:]//divineservicecity[.]fun/ (Ítem Malware: 1.2)
hxxp[:]//satanakop[.]fun/api (Ítem Malware: 1.2)
hxxp[:]//bearboll[.]fun/ (Ítem Malware: 1.2)
hxxp[:]//gougeflying[.]fun/ (Ítem Malware: 1.2)
hxxp[:]//coldwinded[.]fun/api (Ítem Malware: 1.2)
hxxps[:]//blockbeerman[.]fun/ (Ítem Malware: 1.2)
hxxps[:]//documents[.]notificationsapps[.]com/Document[.]iso (Ítem Malware: 1.2)
hxxp[:]//gapi-node[.]io/c2conf (Ítem Malware: 1.2)
hxxp[:]//khel999[.]com/vks6o (Ítem Malware: 1.2)
hxxps[:]//lookingthroughtheturn[.]com/vbu4b (Ítem Malware: 1.2)
hxxps[:]//select-holidays[.]com/vfk6c (Ítem Malware: 1.2)
hxxp[:]//94[.]142[.]138[.]20/version_s/upd[.]exe (Ítem Malware: 1.2)
hxxp[:]//booxshistr[.]xyz/c2conf (Ítem Malware: 1.2)
hxxp[:]//booxshistr[.]xyz/c2sock (Ítem Malware: 1.2)
hxxp[:]//booxshistr[.]xyz/ (Ítem Malware: 1.2)
hxxp[:]//217[.]12[.]206[.]230/c2sock (Ítem Malware: 1.2)
hxxp[:]//1private[.]pro/c2sock (Ítem Malware: 1.2)
hxxp[:]//vipcloud-my[.]xyz/c2conf (Ítem Malware: 1.2)
hxxp[:]//agustfreeday-my[.]xyz/c2sock (Ítem Malware: 1.2)
hxxp[:]//clonecloud-my[.]xyz/c2sock (Ítem Malware: 1.2)
hxxp[:]//fastcloudlife-my[.]xyz/c2sock (Ítem Malware: 1.2)
hxxp[:]//aloowforest[.]xyz/c2sock (Ítem Malware: 1.2)
hxxp[:]//slading[.]xyz/c2sock (Ítem Malware: 1.2)
hxxp[:]//jornesfree[.]xyz/c2sock (Ítem Malware: 1.2)
hxxp[:]//colomndead[.]xyz/ (Ítem Malware: 1.2)
hxxp[:]//modifesistem[.]xyz/c2sock (Ítem Malware: 1.2)

hxxp[:]//promomilk[.]xyz/c2sock (Ítem Malware: 1.2)
hxxp[:]//laynchcontrol[.]xyz/ (Ítem Malware: 1.2)
hxxp[:]//gbbsoft[.]xyz/ (Ítem Malware: 1.2)
hxxp[:]//trapmusics[.]xyz/ (Ítem Malware: 1.2)
hxxp[:]//deadpip[.]xyz/ (Ítem Malware: 1.2)
hxxp[:]//colomna[.]xyz/ (Ítem Malware: 1.2)
hxxp[:]//beerword[.]xyz/ (Ítem Malware: 1.2)
hxxps[:]//95[.]143[.]190[.]57[:]15648/ (Ítem Malware: 1.2)
h x x p s [ : ] / / l m o [ . ] b a r t m f i l [ . ] c o m / ? c 2 9 t Z W 9 u Z U B z b 2 1 l b 2 5 l L m 9 y Z w = = & - session=e6ec0fe49fbfb31608198b22eaa2d00fe6ec0fe49fbfb31608198b22eaa2d00f&sso_reload=t rueAnother (Ítem Phishing: 3.1)

## 5.4 EMAIL

chris_evans@aesinc.us[.]com (Ítem Malware: 1.1)
bandai.namco.ma@kakao[.]comalthough (Ítem Malware: 1.1)
adobesign@adobesign[.]com (Ítem Phishing: 3.1)
dse@eumail.docusign[.]net (Ítem Phishing: 3.1)
autonotification@concursolutions[.]com (Ítem Phishing: 3.1)

## 5.5 HASHES

**(Ítem Malware: 1.1)**
**SHA256:** 9b8efc369c7ff541f885c605c462c7d5a16acfbdfef3b28adc4e5418e890142f
**MD5:** 59ac3eacd67228850d5478fd3f18df78

**(Ítem Malware: 1.1)**
**SHA256:** 454bd68088f17718527b300134cae3eed1c7db3ba7ed9e08d291ef7729229a79
**MD5:** dbf727e1effc3631ae634d95a0d88bf3

**(Ítem Malware: 1.1)**
**SHA256:** 90e6ebc879283382d8b62679351ee7e1aaf7e79c23dd1e462e840838feaa5e69
**MD5:** bbf53c2f20ac95a3bc18ea7575f2344b

**(Ítem Malware: 1.2)**
**SHA256:** 752af3347e278fea9dca3349b5a706dd366c7a36b6769383ccf83278a89ca353Z
**MD5:** e95d176c1dee5dc9d4d21f3d3858b489

**(Ítem Malware: 1.2)**
**SHA256:** 94152a3994acc89013449bf2298cd156f277eae0b8299404920b52cca1451801
**MD5:** 40d722fb3c2610b1d24372da4d8d34ac

**(Ítem Malware: 1.2)**
**SHA256:** ad4cdeca5e669d83e89f785f0e10d0de8ad6409412c43984c484e56b6a5d114c
**MD5:** 315e9881f2d022824e81b1d41c24f691

**(Ítem Malware: 1.2)**
**SHA256:** e29a724b6844b848014d68575a458e59cbcc002bd16a1d08c16742cc2c549dce
**MD5:** 309d5233e7eec6080ccbf6db983b7873

**(Ítem Malware: 1.2)**
**SHA256:** e756e44290ccf5f9d6864444bbd9044c2345c60a0352de5724eb5928d29e0018
**MD5:** 17fa297998833bad8fb12ee779288807

**(Ítem Malware: 1.2)**
**SHA256:** a3b341c702638deb872243d97c81e9050697a9c07bfb6ef425d9d3efe25302a4
**MD5:** 0f114f0b44d1b85aa1994bdc7e6c2155

**(Ítem Malware: 1.2)**
**SHA256:** 4560c27d6656bcf5f5f4d101daab3ccdd5f0edd4f5b279b66464019a7cbe9aba
**MD5:** 73af7aea83b7b9002ceedf0a1155b325

**(Ítem Malware: 1.2)**
**SHA256:** ad729ff3963682680bbef0d1345e743938dac29792a96b6f64fd048509aea140
**MD5:** b9715e5d66f4ad0d611983c909ffa6a5

**(Ítem Malware: 1.2)**
**SHA256:** 44dd79ed23516673af9084ea8120f3d412e815ab3df36e9c7e2028363cd086de
**MD5:** 8fd20775c61eeba1d83f52104afacaa9

**(Ítem Malware: 1.2)**
**SHA256:** 6f643819b96ca4b0451293954100b1739865fc593d6c75048563ac5d9a34479a
**MD5:** 6f598c04986602a2bb56ad3cae78d10e

**(Ítem Malware: 1.2)**
**SHA256:** 95242e1d105de9c33b2c9d8a9514f58327ca32d7d24af9af19ff3f0d075ea451
**MD5:** e7495ddd6f4e5c686c2ee68b3db91f9b

**(Ítem Adversarios: 4.1)**
**SHA256:** df154dee8539aeb8dccade9d392e04dc0a8d44c46829d673784d0a05c927b69c
**MD5:** 5787d9fbcbc95dd636a9d1f6685b39f3

**(Ítem Adversarios: 4.1)**
**SHA256:** 2cf979e3a79853225e5e17856721d1256c8f319e3883e65db794f187dc424304
**MD5:** 1f011cd53435514ddfaa14dcb3d142f4

**(Ítem Adversarios: 4.1)**
**SHA256:** 97342ed6f55bb14d5a817df188c9321c7cc143909be481e387124ea0b1c1edb0
**MD5:** 418f104289bcbc9afcd35d822170fb52

# Fuentes


6.1 https://thehackernews.com/2023/10/bunnyloader-new-malware-as-service.html
6.2 https://www.zscaler.com/blogs/security-research/bunnyloader-newest-malware-service
6.3 https://cybersecuritynews.com/bunnyloader-malware-as-a-service/
6.4 https://thehackernews.com/2023/10/zanubis-android-banking-trojan-poses-as.html
6.5 https://securelist.com/crimeware-report-asmcrypt-loader-lumma-stealer-zanubis-banker/110512/
6.6 https://cybersecuritynews.com/new-android-banking-malware-government-app/
6.7 https://www.bleepingcomputer.com/news/security/exploit-available-for-critical-ws-ftp-bug-exploited-in-attacks/
6.8 https://www.bleepingcomputer.com/news/security/evilproxy-uses-indeedcom-open-redirect-for-microsoft-365-phishing/
6.9 https://www.bitdefender.com/blog/hotforsecurity/ransomware-group-demands-51-million-from-johnson-controls-after-cyber-attack/
6.10 https://attack.mitre.org/techniques/T1589/
6.11 https://attack.mitre.org/techniques/T1590/
6.12 https://attack.mitre.org/techniques/T1566/
6.13 https://attack.mitre.org/techniques/T1078/
6.14 https://attack.mitre.org/techniques/T1110/
6.15 https://attack.mitre.org/techniques/T1555/
6.16 https://attack.mitre.org/techniques/T1003/
6.17 https://attack.mitre.org/techniques/T1552/
6.18 https://attack.mitre.org/techniques/T1047/
6.19 https://attack.mitre.org/techniques/T1505/
6.20 https://attack.mitre.org/techniques/T1068/
6.21 https://attack.mitre.org/techniques/T1087/
6.22 https://attack.mitre.org/techniques/T1135/
6.23 https://attack.mitre.org/techniques/T1083/
6.24 https://attack.mitre.org/techniques/T1018/
6.25 https://attack.mitre.org/techniques/T1518/
6.26 https://attack.mitre.org/techniques/T1016/
6.27 https://attack.mitre.org/techniques/T1033/
6.28 https://attack.mitre.org/techniques/T1021/
6.29 https://attack.mitre.org/techniques/T1005/
6.30 https://attack.mitre.org/techniques/T1039/
6.31 https://attack.mitre.org/techniques/T1011/
6.32 https://attack.mitre.org/techniques/T1537/
6.33 https://attack.mitre.org/techniques/T1485/
6.34 https://attack.mitre.org/techniques/T1486/

Claro empresas

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”.