BOLETÍN DE SEGURIDAD DIGITAL

TLP: CLEAR

CYWEX CSIRT



23.07.2026

CIBERAMENAZA

Starland RAT

WEXLER®

CONTEXTO

Nivel de compromiso del ataque o vulnerabilidad

ALTO

Nombre del ataque

Cisco Talos - Starland RAT

Fecha de la primer evidencia del ataque o vulnerabilidad

Las primeras evidencias públicas de esta campaña fueron documentadas y divulgadas por Cisco Talos en julio de 2026. Durante la investigación se identificó la actividad del actor de amenazas UAT-11795, una operación con motivación financiera que emplea la técnica de ingeniería social ClickFix y distribuye instaladores troyanizados para desplegar el nuevo Starland RAT y el implante de comando y control WLDR. Los investigadores determinaron además que la actividad del grupo se remonta, al menos, a junio de 2025.

Lugar o ubicación de la primera evidencia

Las evidencias analizadas por Cisco Talos corresponden a una campaña con alcance internacional, observada principalmente en víctimas ubicadas en Estados Unidos, Alemania, Rumania y Venezuela. Debido al uso de ingeniería social e instaladores troyanizados, la amenaza no se limita a una ubicación geográfica específica y puede afectar a usuarios y organizaciones en distintas regiones.

¿A quiénes afectó el ataque o vulnerabilidad?

El espectro de víctimas de esta campaña abarca usuarios individuales y organizaciones que descargan o instalan aplicaciones desde fuentes no confiables. Aunque Cisco Talos identificó casos en Estados Unidos, Alemania, Rumania y Venezuela, la naturaleza de la amenaza permite afectar a cualquier sistema Windows cuyos usuarios sean persuadidos mediante ingeniería social o instaladores troyanizados.

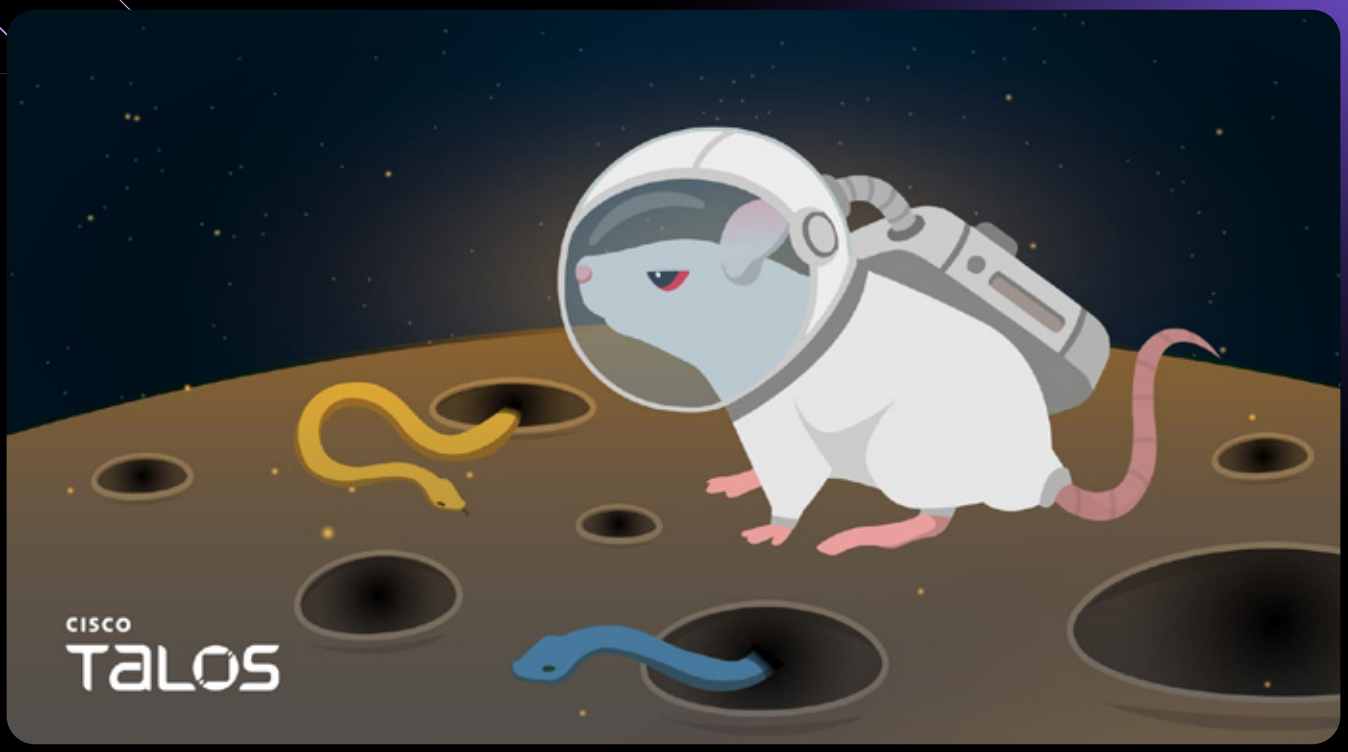


Imagen 1. https://blog.talosintelligence.com/uat-11795-deploys-novel-starland-rat-and-bespoke-wldr-c2-implant-in-financially-motivated-campaign/

CARACTERÍSTICAS

¿Qué hace la vulnerabilidad o ataque?

Esta campaña tiene como objetivo comprometer los sistemas infectados para otorgar a los atacantes **acceso remoto** y control sobre los equipos afectados mediante el **malware Starland RAT** y el **implante WLDR**. Una vez establecida la infección, permite ejecutar comandos de forma remota, recopilar información del sistema, robar credenciales, cookies, datos almacenados en navegadores y billeteras de criptomonedas, así como descargar y ejecutar cargas maliciosas adicionales. Además, implementa mecanismos de persistencia y mantiene comunicación con servidores de comando y control (C2), lo que permite a los atacantes **conservar el acceso al dispositivo** comprometido, ampliar sus capacidades y continuar con **actividades maliciosas** orientadas al robo de información y al beneficio económico.

Cómo actúa y de qué manera se propaga

La campaña inicia mediante **técnicas de ingeniería social**, principalmente a través de ClickFix y la distribución de **instaladores troyanizados de aplicaciones legítimas** como Zoom, WebEx, MobaXterm y DBeaver. Los atacantes persuaden a la víctima para que ejecute comandos en PowerShell o instale software aparentemente confiable desde sitios o enlaces fraudulentos. A diferencia de otros ataques, **no explota una vulnerabilidad del sistema operativo**, sino que depende de que el **propio usuario inicie la ejecución del contenido malicioso.**

Una vez que la víctima ejecuta el archivo o comando, se descarga y ejecuta la **cadena de infección** que instala Starland RAT y el implante WLDR. Estas herramientas permiten a los atacantes obtener **acceso remoto al equipo**, ejecutar comandos, recopilar información del sistema, robar credenciales, cookies, datos almacenados en navegadores y billeteras de criptomonedas. Además, **WLDR opera principalmente en memoria**, establece persistencia y mantiene comunicación con los servidores de comando y control (C2), desde donde los atacantes pueden enviar nuevas instrucciones o descargar malware adicional. La propagación de la campaña depende de la continua distribución de instaladores troyanizados y del **engaño a nuevos usuarios** mediante técnicas de ingeniería social. No posee capacidades de propagación automática entre equipos ni explota vulnerabilidades para moverse lateralmente dentro de una red. En su lugar, los atacantes amplían el alcance de la campaña convenciendo a más víctimas de ejecutar los archivos maliciosos, lo que les permite mantener el acceso a los sistemas comprometidos y continuar con el **robo de información con fines económicos.**

Las brechas de seguridad que aprovechan

La campaña aprovecha principalmente la **confianza de los usuarios** mediante técnicas de ingeniería social, especialmente ClickFix, y la distribución de instaladores troyanizados de aplicaciones legítimas. De esta forma, los atacantes **logran que la propia víctima ejecute comandos** o instale software malicioso creyendo que se trata de una acción legítima, sin necesidad de explotar vulnerabilidades conocidas en el sistema operativo o en las aplicaciones.

Riesgos que se corren por no actuar frente al ataque

Robo de credenciales, cookies de sesión, información almacenada en navegadores, billeteras de criptomonedas y otros datos sensibles, lo que puede derivar en **accesos no autorizados**, fraude financiero, pérdida de información, instalación de malware adicional, **persistencia del atacante** en los sistemas comprometidos y el compromiso de cuentas, equipos y servicios de la organización.

Mapa de victimología de esta campaña.

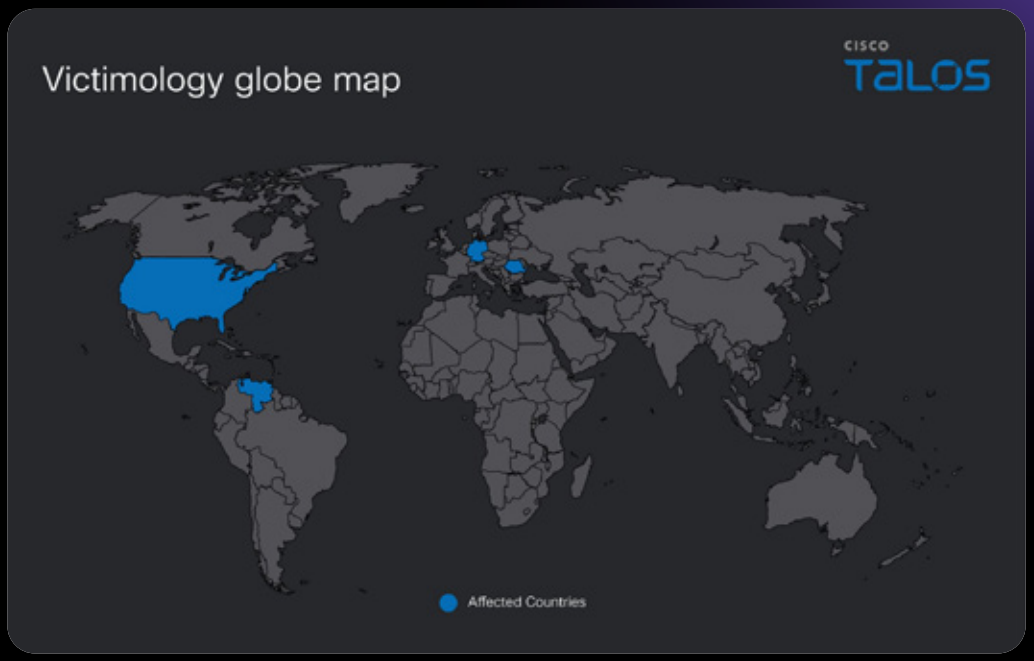


Imagen 2. https://vulners.com/talosblog/TALOSBLOG:988B88E417554B70AB86090EA0458D1F

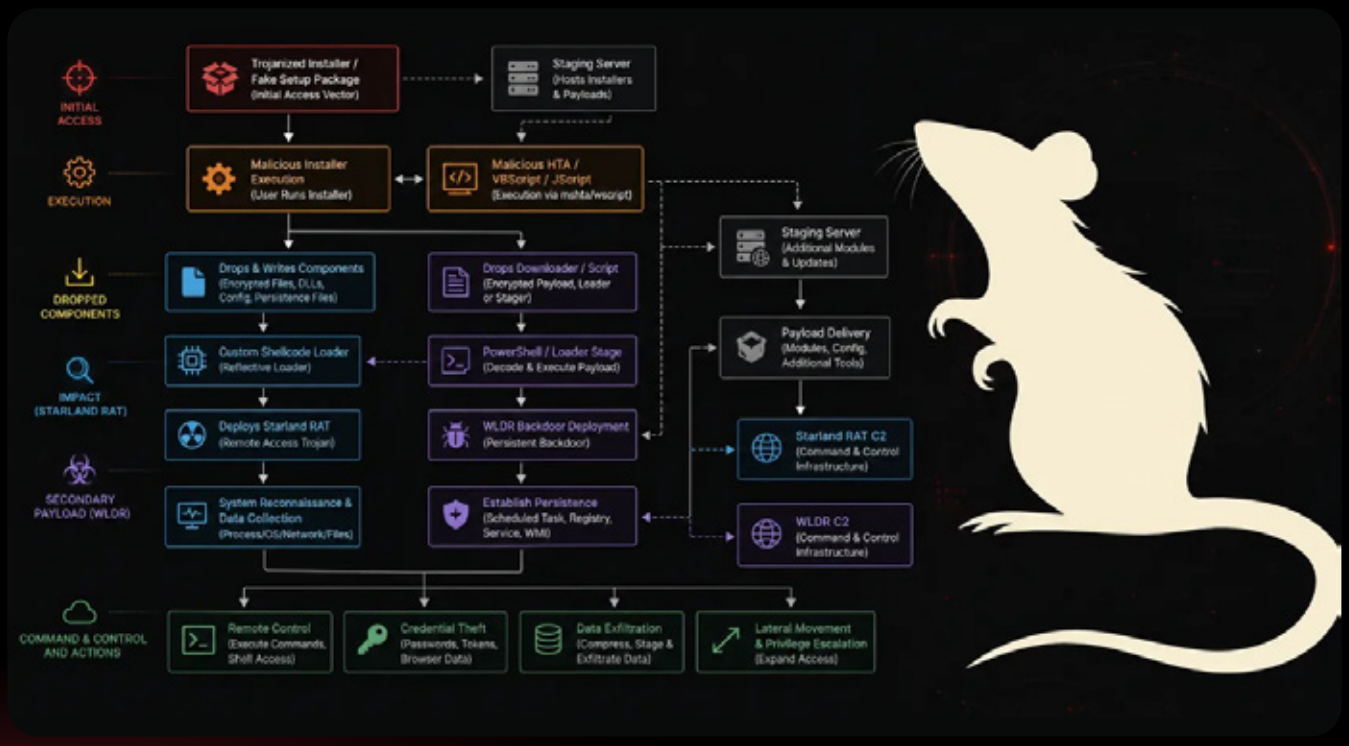


Imagen 3. https://cyberpress.org/uat-11795-spreads-dual-backdoors/

Estadísticas de resolución de dominios Cisco Umbrella para los dominios maliciosos durante la ventana de investigación.

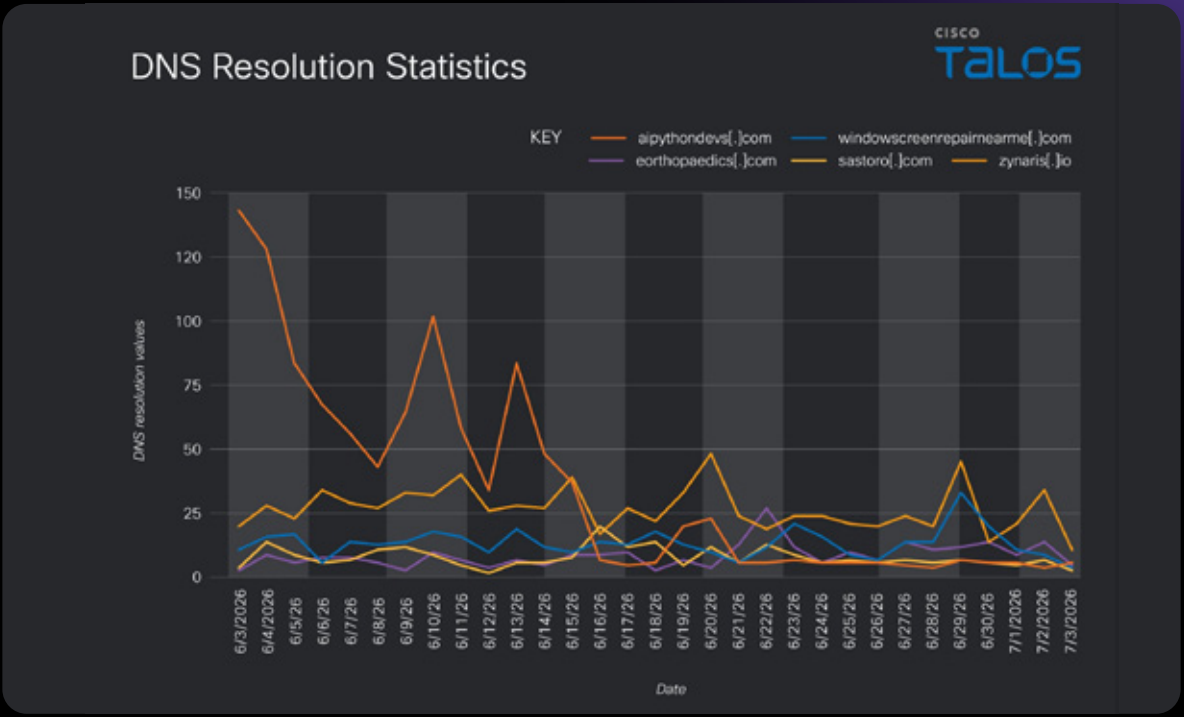


Imagen 4. https://blog.talosintelligence.com/uat-11795-deploys-novel-starland-rat-and-bespoke-wldr-c2-implant-in-financially-motivated-campaign/

ERRADICACIÓN

Método para erradicar el ataque

Restricción de RDP y otros servicios de escritorio remoto

Proteger PowerShell y/o restringir su uso

Actualizar el software a la última versión y aplicar parches periódicamente

Actualizaciones que se deben realizar

Implementar un proceso de **parcheo acelerado**, es decir, que tan pronto se publique una actualización de seguridad crítica, se evalúe e instale en horas o días, no semanas.

RECOMENDACIONES

- Desarrollar e implementar un plan de recuperación efectivo.
- Exigir que todas las cuentas cuenten con inicio de sesión y contraseña (por ejemplo, cuentas de servicio, cuentas de administrador y cuentas de administrador de dominio).
- Requerir autenticación multifactor.
- Mantener todos los sistemas operativos, software y firmware actualizados.
- Segmentar redes.
- Identificar, detectar e investigar actividades anormales y posibles ataques del ransomware indicado, con una herramienta de monitoreo de redes.
- Instalar, actualizar periódicamente y habilitar la detección en tiempo real del software antivirus.
- Auditar cuentas de usuarios.
- Deshabilitar puertos de red no utilizados.
- Deshabilitar los hipervínculos en los correos electrónicos recibidos.
- Deshabilitar las actividades y permisos de la línea de comandos y secuencias de comandos.
- Mantener copias de seguridad de datos fuera de línea.

INDICADORES DE COMPROMISO (IOCS)

SHA256

6ca7a458985350ac082a9c9820d7f8d39128a4c4bda2f5d32f169a45b7b22bc6
6ae334ce60d1a9b7fb96d1d0d0eda5ec7c2c31d3f0cf3e4d7e3056504d50043d
1a01ad25712d306f27f526332fdccf959f2de53207b54e4e80f60faa804d6cb6
ddcf66ecc61dc6b8cd36748d284d8cb45a470201b5373dd2bfc47700c7da32e1
603fd9724de346a06e00c1b8502c2ac1180812a18bbf30032dab8d469e5c18e1
f4491736743a16f1278b8ba01649ee93343764e35ae5e1c0d5e0c0e1d7e32c14
2c7a99f137efd718f89cf8b260379c99af89ea1939568df09314918f2c5999a3
5b9bf7957a9f8869c87ace1a6d76b48e2623073e72739ad0636b5dfa4bb2e0c3
7dc77a5abab119960fbe42b1535c957020cce1b8e0a3cf58d4eddc51b5bf9940
36e3838d07978f49ebe6546d57d2f311b8d6566558bcd58448e921c988cc346a
575ce92c473e6d47810321e309a4e29dd7f52f4152526b0bdca80f54b53aed2f
964256d3259b6e0c701ec04116c45cf0ec381c1c209dc29b09a7930cd7a4810b
a6821c7e9bfe2e6af0f690d906ec6a26161e2198c256fb60f3b4731c317f3ad9
a32ac345e39cb7606322e2155bd7b4d6941c1678619e48d1f14d9301ee53e6c0
2751281d3800d82ecd3fad7c1d2293f3b947875a343b0672b4f4024a261165d2
47dedb08385449d48d8b6543030310317c92cddafa25e14ee0cb9a32d53ced5c
162e436f18fe6099c57855c8d63fd747493624e87702dc749b242eb9a6b758ca
451ac8ca34d5bcdfe476465f69eb517b2608f267c7e8d69f8ef36197a6f1d949
365024336c7681ac0854321ac6c140a245b9593285da02d2a590124cdc592370
a080b5380ccc8fc40b24c02151d305efc32d931dc547881e01a2e6f2b070c7dc
17e41d66ebfd56edc960f58f4285697ceceaa812514bb15092672c747979896e
f8da52ff98e66b137b5d31908f0a5d0fa1eb446034337f8bba3d5bba60f586be
d52540621dec5ed56cac8532f0e4fe10a7575c3e17e984f59646909fa587dd35
a59742d3086924c5f511d248df01601bfbf723359590fb3f3ba355f2792cc455
2a27b3415114b874da295c19cce5227a8b8d9525cc2da331034a1f45528eecae
1b46f761719dce44baa2d7b417c5214fc41c080f7f9ba485e7e489d949097f1f
896185a89bd7eb0520b03fdcfb8db0be98b43cf15f14041d73b23d3988c1bcab
a1835d333ac3db961a8ff1f4864e3c10a6f73a872c040599091390a009ac7804

URL

https://eorthopaedics.com/feed/note
https://web-devtools.com/starlandfox
https://web-devtools.com/x32remka
https://web-devtools.com/dopfile
https://web-devtools.com/file.zip
https://eorthopaedics.com/feed/cew78zwvd2/
https://eorthopaedics.com/feed/gnsmetadyx54/
https://sastoro.com/alpha/nrpilqjnut/
https://sastoro.com/alpha/dpyb8w3ycih8/
https://windowscreenrepairnearme.com/command

IP

104.248.233.104
192.81.216.250
74.114.119.201
178.255.126.39
193.149.176.254
185.238.191.234

DOMINIO

eorthopaedics.com
sastoro.com
zynaris.io
alphabitcapital.info
niggerdemon.in
web-devtools.com
aipythondevs.com
windowscreenrepairnearme.com

REFERENCIAS

https://blog.talosintelligence.com/uat-11795-deploys-novel-starland-rat-and-bespoke-wldr-c2-implant-in-financially-motivated-campaign/

https://cyberpress.org/uat-11795-spreads-dual-backdoors/

https://securityaffairs.com/195532/malware/new-russian-campaign-uses-fake-webex-and-zoom-installers-to-deploy-starland-rat.html

https://imtr.net/article/uat-11795-deploys-novel-starland-rat-and-bespoke-wldr-c2-implant-in-financially-e8bf

https://mallory.ai/stories/019f6a68-7baf-796c-9cbc-be32f9ea141e

https://vulners.com/talosblog/TALOSBLOG:988B88E417554B70AB86090EA0458D1F



CYWEX
CSIRT

WEXLER®

Canales de contacto: csirt_cywex@wexler.com.co +57 (601) 268 8158

© 2026 Wexler SAS. Todos los Derechos Reservados.