Nro. Alerta:	AL-2026-042	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	19-ago-2026	Dysphoria: Evolución de una botnet y uso de infraestructura C2 basada en blockchain	Pág.: **1** of **7**

I. DATOS GENERALES:

Clase de alerta: Alerta de seguridad
Tipo de Incidente: Botnet / Malware
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Dysphoria: Evolución de una botnet y uso de infraestructura C2 basada en blockchain - Figura referencial

La botnet Dysphoria comprende una red de dispositivos IoT (Internet de las cosas) compuesta por más de 200.000 bots distribuidos en todo el mundo. Esta amenaza posee una arquitectura de resiliencia sofisticada, basada en un mecanismo encubierto de resolución de la infraestructura de comando y control (C2) mediante dominios de blockchain, como ENS (Ethereum Name Service) y SNS (Solana Name Service). Siendo capaz de transformar los dispositivos comprometidos en nodos de retransmisión o servidores proxy para la infraestructura C2, lo que dificulta significativamente las operaciones destinadas a desmantelar la botnet.

III. INTRODUCCIÓN

Dysphoria ha comprometido un gran número de dispositivos de uso cotidiano, entre ellos routers, DVR, repetidores y otros dispositivos IoT, incorporándolos a una extensa red de bots (botnet). Un bot es un dispositivo infectado con un malware que permite su control remoto por parte de un atacante. La incorporación de estos equipos a la botnet se debe, principalmente, a la ejecución de versiones obsoletas del firmware, la

exposición a Internet de servicios de administración remota vía SSH o Telnet con el uso de credenciales débiles o predeterminadas.

Dos organizaciones chinas dedicadas a la ciberseguridad, CNCERT, Equipo nacional chino de respuesta a emergencias informáticas y XLab, Laboratorio de inteligencia sobre amenazas de la empresa china Qi'anxin, han rastreado esta botnet y estiman que su población de bots asciende aproximadamente a 296.000 dispositivos comprometidas, que presentan vulnerabilidades sin parchear desde el 2017, debido a su obsolescencia y a la falta de soporte de sus proveedores.

Una vez comprometidos por Dysphoria, los dispositivos son utilizados para generar tráfico malicioso en ataques de denegación de servicio distribuido (DDoS). XLab informó un pico de 740.000 pings diarios desde equipos infectados, incluyendo 239.000 conexiones hacia clientes en el extranjero, afectando la disponibilidad de sitios web y servicios en línea. Además, sus operadores afirman que la botnet puede alcanzar una capacidad de ataque de hasta 4 Tbps.

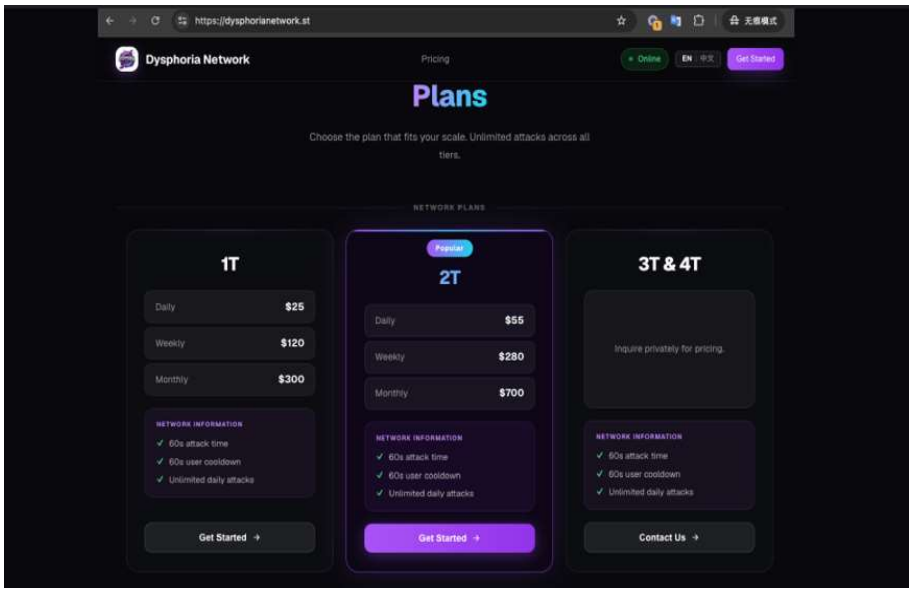

Figura 2.- Dysphoria: Sitio web y planes de servicios.

IV. VECTOR DE ATAQUE

XLab afirmó que Dysphoria utiliza una arquitectura de alta resiliencia, en la que el malware emplea sistemas de nombres basados en blockchain, como Ethereum Name Service (ENS) y Solana Name Service (SNS) e incluso puede convertir los dispositivos

de las víctimas en nodos de retransmisión o proxy para las comunicaciones de comando y control (C2), agregan también que estas direcciones en el C2 están ocultas dentro de cadenas IPv6 falsas y se obtienen mediante un algoritmo de transformación de bytes personalizado.

Los dominios ENS y SNS son sistemas de nombres descentralizados basados en tecnología blockchain (cadena de bloques), que funcionan de manera similar al DNS tradicional de Internet, pero están orientados al ecosistema Web3. Este concepto hace referencia a una nueva generación de Internet que utiliza tecnologías como cadenas de bloques, criptomonedas y tokens no fungibles (NFT), con el objetivo de brindar a los usuarios un mayor control sobre sus datos, identidad digital y activos.

En lugar de utilizar direcciones largas y complejas compuestas por letras y números, estos sistemas permiten asociarlas con nombres legibles, como **tunombre.eth** en ENS o **tunombre.sol** en SNS. En el caso de Dysphoria, estos registros son utilizados para localizar servidores de control activos, lo que dificulta su interrupción mediante mecanismos tradicionales de bloqueo o desactivación de dominios.

Dysphoria presenta vínculos con la infraestructura y actividad asociada a la botnet JackSkid, la cual en marzo fue objeto de acciones coordinadas por parte de autoridades de Estados Unidos, Alemania y Canadá. Posteriormente, Nokia Deepfield y el laboratorio de amenazas de Comcast documentaron que JackSkid recurría al dominio ENS **m3rnbvs5d[.]eth** para su infraestructura de comando y control (C2), el mismo dominio identificado posteriormente en Dysphoria.

A finales de abril, XLab observó que Dysphoria recibió una actualización que incorporó un nuevo algoritmo de cifrado de cadenas basado en RC4 y un mecanismo de adquisición de infraestructura C2, mediante el uso del dominio ENS **ukranianhorseriding[.]eth**, empleado para obtener información de infraestructura de red. A comienzos de mayo, la botnet incorporó el dominio SNS **24carnforth2merseyside[.]sol**, utilizado para obtener información de infraestructura mediante registros específicos. Posteriormente, en junio, incorporó el dominio ENS **burrberry[.]eth**, cuyo registro **node** permite obtener las direcciones IP de nodos de distribución.

Tipo de dominio	dominio objetivo	Clave de consulta correspondiente	efecto
ENS (Ethereum)	burrberry.eth	node	Obtener la dirección IP del nodo de distribución del relé
ENS (Ethereum)	ukranianhorseriding.eth	network	Infraestructura básica de red
SNS (Solana)	24carnforth2merseyside.sol	deserialized	Infraestructura básica de red

Figura 3.- Dysphoria: Mecanismo de resolución encubierta C2 de nombres de dominio de blockchain.

A finales de junio, XLab identificó un mecanismo de C2 dinámico mediante el cual las muestras DDoS consultan los nodos de distribución a través de HTTP para obtener una lista actualizada de direcciones. Estas direcciones corresponden a dispositivos infectados que funcionan como nodos de retransmisión, ocultando la infraestructura real de control y dificultando su identificación.

Asimismo, XLab identificó una variante independiente que eliminó la funcionalidad DDoS y convirtió los dispositivos infectados en nodos de retransmisión o proxy. Esta variante utiliza el protocolo UPnP para realizar automáticamente el reenvío de hasta 155 puertos, permitiendo conexiones externas hacia los dispositivos comprometidos y reforzando su función como infraestructura de intermediación.

V. IMPACTO

- **Ataques DDoS:** los dispositivos comprometidos pueden integrarse en una botnet y utilizarse para generar tráfico masivo contra sitios web, servidores y servicios en línea, afectando su disponibilidad.

- **Ampliación de la infraestructura de ataque:** Dysphoria puede convertir dispositivos infectados en nodos de retransmisión/proxy, de modo que el tráfico no tenga que dirigirse directamente desde los bots hacia los servidores de control. Esto dificulta identificar y bloquear la infraestructura real.

- **Mayor resiliencia de la botnet:** el uso de ENS, SNS y mecanismos dinámicos de descubrimiento de infraestructura dificulta la interrupción de las comunicaciones. Los dispositivos pueden obtener nuevas direcciones de nodos

de distribución y mantener la comunicación incluso cuando parte de la infraestructura queda fuera de servicio.

- **Exposición de los dispositivos comprometidos**: la variante que utiliza UPnP para crear reglas de reenvío de puertos puede hacer que los dispositivos infectados sean accesibles desde Internet, convirtiéndolos en infraestructura de intermediación para los operadores.

VI. INDICADORES DE COMPROMISO

Los siguientes Indicadores de Compromiso (IoC) se encuentran asociados con la infraestructura de Dysphoria:

Se identificaron las siguientes direcciones IP asociadas con servidores de descarga y/o infraestructura de Comando y Control (C2):

Dirección IP	Descripción
217.60.195.160	Servidor de descarga/C2
76.164.203.171	Servidor de descarga/C2
92.42.100.131	Servidor de descarga/C2
78.153.155.152	Servidor de descarga/C2

Tabla 1.- Direcciones IP – Servidores de descarga/C2 - Dysphoria: Evolución de una botnet y uso de infraestructura C2 basada en blockchain.

Banner FTP asociado:

220 cool ftp server hosted on brian krebs' giant ass 4head

Indicador de Compromiso (IoC)	Tipo
i.peer4you.net	Dominio
o.peer4you.net	Dominio
login.trees4sale.net	Dominio
www.trees4sale.net	Dominio
c2.saintpetersburgresident.ru	Dominio C2
peer.saintpetersburgresident.ru	Dominio
kieron.androiddebugbridge.su	Dominio
dysphoria.androiddebugbridge.su	Dominio C2
telaviv.androiddebugbridge.su	Dominio
jerusalem.androiddebugbridge.su	Dominio
node.androiddebugbridge.su	Dominio
wow.androiddebugbridge.su	Dominio

Tabla 2.- Dominios asociados a infraestructura crítica - Dysphoria: Evolución de una botnet y uso de infraestructura C2 basada en blockchain.

Dominio	Tipo / Red
m3rnbvs5d.eth	ENS
burrberry.eth	ENS
ukranianhorseriding.eth	ENS
24carnforth2merseyside.sol	SNS

Tabla 3.- Dominios asociados a infraestructura Blockchain - Dysphoria: Evolución de una botnet y uso de infraestructura C2 basada en blockchain.

Hash SHA-1
c1bedea261f325441fb9a75c50b11d0c8fb01ac6
a3b9575897c16cbf6afe3af1aa8b55171ea6edf9
8db6c78533c176f13b61405cdc3f8fad703325f1
9c1716d770ea69e8e1418d96d52222396ecb4362
73651c02b29f1c07e3177e86c967fc45e9f30f0f
955ff909972958098f0d4a06bcc4d6b9eea90449
25081bdec05f64eb4f313420c82d8de957e30026
dcea71b9ab9de8efca301de9e2f7bf11c7132364
df510f6f69a5c149c216c7b3accc4f460d8cf363
b0782a9d6eef2ce02f734a6e5e1d8e0f9a2b65be
e7e1694162639ed587625432a79cfaa49f560d11
b7faa44ab0772047a8581bbfdd9c561e28fc66de

Tabla 4.- Hashes SHA-1 - Dysphoria: Evolución de una botnet y uso de infraestructura C2 basada en blockchain.

VII. RECOMENDACIONES

- Los responsables de la seguridad deben actualizar los equipos IoT expuestos, reemplazar los dispositivos que ya no se pueden actualizar, eliminar las credenciales predeterminadas y débiles y deshabilitar la administración remota y UPnP donde no sean necesarias.
- También deberían colocar las cámaras y dispositivos similares en una red separada siempre que sea posible, restringir el acceso a las interfaces de administración.
- Los operadores de red que reciban el informe especial deberán investigar rápidamente los sistemas mencionados, utilizando el campo "última conexión" para determinar con qué frecuencia se observó actividad.
- Pueden aislar dispositivos sospechosos, comprobar los cambios de cuenta y configuración, actualizar o reemplazar el hardware y supervisar el tráfico saliente renovado.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

GBHACKERS. (2026). *Dysphoria Hijacks Routers to Build a Stealthy IoT Botnet with Blockchain C2.* https://gbhackers.com/dysphoria-hijacks-routers/

CYBER SECURITY NEWS. (2026). *Dysphoria Botnet: New IoT Malware Campaign Targets Routers and IoT Devices.* https://cybersecuritynews.com/dysphoria-botnet/

THE HACKER NEWS. (2026). *Dysphoria IoT Botnet Adds Blockchain-Based C2 for Resilient Communication.* https://thehackernews.com/2026/07/dysphoria-iot-botnet-adds-blockchain-c2.html

DATACONOMY. (2026). *La botnet Dysphoria infecta 200.000 dispositivos IoT.* https://it.dataconomy.com/2026/07/28/la-botnet-disforia-infetta-200-000-dispositivi-iot/

XLAB / QIANXIN. (2026). *Dysphoria: Technical Analysis of the IoT Botnet.* https://blog.xlab.qianxin.com/dysphoria/