Alerta

Técnica

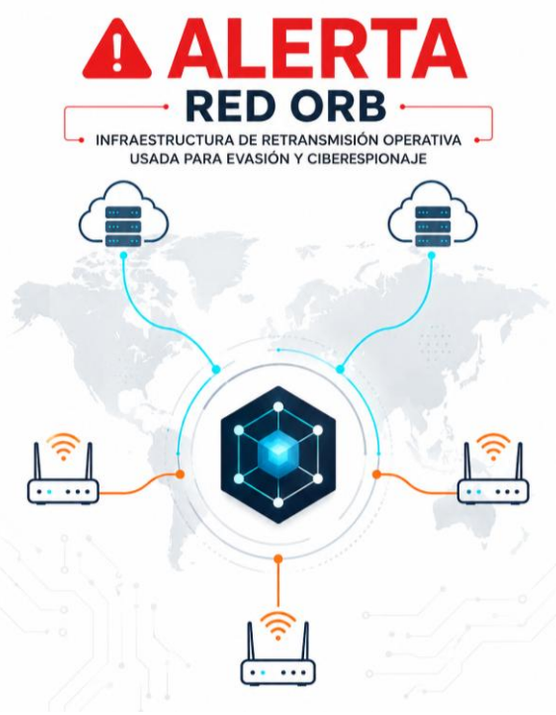
Red de Retransmisión Operativa CHARLIE

COLCERT AL – 20260710 - 102

TIC

TLP:CLEAR

Resumen Ejecutivo



Se han analizado 16 nodos confirmados de red de retransmisión operativa (ORB) denominada CHARLIE, también catalogada como ORB3, SPACEHOP o SuperJump, dicha red constituye infraestructura compartida y multi-inquilino alquilada y administrada por ciberdelincuentes de espionaje alineados con la República Popular China, sirviendo de canal encubierto a múltiples grupos APT del ecosistema chino, principalmente APT5 y APT15.

La totalidad de los 16 nodos identificados pertenecen al bloque de red 103.97.203.0/24, alojado bajo el Sistema Autónomo ASN 136258 de BrainStorm Network, Inc., con sede registrada en India. Es crítico advertir que estos nodos presentan tasas de detección extremadamente bajas en las plataformas de análisis de malware (entre 0 y 2 motores de detección), comportamiento técnico esperado para este tipo de infraestructura proxy de tránsito; por lo tanto, la ausencia de alertas en soluciones antivirus tradicionales no debe interpretarse en ningún caso como un indicador de bajo riesgo.

La inteligencia de amenazas caracteriza una campaña ofensiva activa ejecutada por el clúster de intrusiones UAT-9244 (estrechamente vinculado con los actores Famous Sparrow y Tropic Trooper), éste utiliza de forma táctica la infraestructura de la red ORB CHARLIE para focalizar sus ataques contra proveedores de infraestructura crítica del sector de las telecomunicaciones en América del Sur.

Se hace especial énfasis en que Colombia ha sido identificada como un objetivo prioritario y constante de esta campaña desde el año 2024, en conjunto con operaciones dirigidas hacia Chile, Perú, Argentina, Brasil y Venezuela.

Contexto de la Amenaza Global)

Las redes ORB (Operational Relay Box) representan la evolución estructural más significativa en la infraestructura de intrusiones de nexo chino desde el auge de las botnets tradicionales. A diferencia de los servidores C2 dedicados atribuibles a un solo actor, éstas redes operan bajo un modelo de IaaS malicioso: una infraestructura de servicios alquilada que varios grupos APT comparten de manera simultánea y transitoria.

El ciclo de vida promedio de una dirección IPv4 activa dentro de la red SPACEHOP/ORB3 es de apenas 31 días, periodo tras el cual el nodo es rotado o eliminado del clúster activo. Este dinamismo provoca que las estrategias de defensa basadas únicamente en listas de bloqueo de IoCs resulten estructuralmente ineficaces; para el momento en que un analista detecta y documenta una IP de salida, es muy probable que esta ya haya sido reemplazada.

Impacto para Colombia

- **Identificación como Objetivo Prioritario:** El clúster de actividad UAT-9244 evidencia un interés sostenido y documentado en comprometer a operadores de telecomunicaciones y proveedores de comunicaciones en Sudamérica. Es importante señalar que Colombia figura explícitamente como un objetivo prioritario dentro de esta campaña de espionaje desde 2024, a la par de naciones como Chile, Perú, Argentina, Brasil y Venezuela.
- **Sectores en Riesgo:** Telecomunicaciones: Operadores móviles, proveedores de internet de banda ancha, operadores de fibra óptica e infraestructura de backhaul.
- **Infraestructura crítica:** Infraestructura Crítica Nacional: Entidades estratégicas de los sectores de energía, acueducto y transporte que mantengan redes de tecnología operativa (OT) expuestas o con segmentación deficiente hacia sus canales de comunicación.

NIVEL DE RIESGO

ALTO

COLCERT

Riesgos específicos en el contexto nacional

- Las empresas de telecomunicaciones colombianas en proceso de modernización de su infraestructura (migración a 5G, o la expansión de redes de fibra óptica) frecuentemente exponen, de forma transitoria, interfaces de administración de sus dispositivos de borde, convirtiéndolos en vectores de reclutamiento altamente atractivos para la expansión de redes ORB.
- Los dispositivos SOHO de fabricantes con alta penetración en el mercado colombiano (Cisco, Asus, D-Link, MikroTik) son objetivos primarios para clústeres como FLORAHOX/ORB2, cuyo modus operandi incluye explotación de firmware desactualizado.
- La explotación de la cadena de vulnerabilidades conocida como BruteEntry permite que una organización colombiana comprometida sea convertida en plataforma de ataque hacia terceros.
- La ofuscación geográfica empleada por la red ORB3, mediante la tercerización de nodos en India (ASN 136258) reduce la eficacia de los controles de geofencing enfocados exclusivamente en países con perfil de alto riesgo cibernético, facilitando que el tráfico hostil ingrese a las redes nacionales bajo la apariencia de conexiones legítimas.

Perfil de Actor Identificado

La designación UAT-9244 corresponde a un clúster de actividad de intrusiones identificado por Mandiant, enfocado de manera persistente en comprometer a proveedores de telecomunicaciones. El análisis de inteligencia evalúa con un alto nivel de confianza que este conjunto de operaciones está alineado estratégicamente con los intereses de la República Popular China, compartiendo capacidades tácticas, herramientas especializadas y un ecosistema de TTPs en común con los actores de amenazas Famous Sparrow y Tropic Trooper.

Motivación Primaria	**Ciberespionaje estatal:** **Obtención de inteligencia militar, diplomática y de telecomunicaciones.** **Exfiltración de metadatos de red e información sobre rutas de comunicación crítica.**
Capacidades Técnicas	Muy elevadas. Exploits de día cero en dispositivos de borde, manipulación de firmware de routers, desarrollo de controladores de kernel Windows firmados para evadir EDRs, uso de protocolos P2P para C2 descentralizado.
Victimología	Operadores de telecomunicaciones e infraestructura crítica en América del Sur (Colombia, Chile, Perú, Argentina, Brasil, Venezuela) desde 2024.
Herramientas Exclusivas	TernDoor (backdoor Windows), PeerTime (backdoor Linux/IoT ELF), BruteEntry (escaner masivo en Go).
Infraestructura	ORB3/SPACEHOP como proxy multi-hop. Servidores C2 en Vultr/Stark Industries. Rotación de nodos cada 31 días.
Afiliaciones	Famous Sparrow (SilkBean, IronHusky), Tropic Trooper (KeyBoy), APT5 (Mandiant), APT15 (UNC2630).

Infraestructura Multi-Inquilino: El Desafío de Atribución

Un hallazgo estructural derivado de las investigaciones de inteligencia determina que las redes ORB no pertenecen ni son controladas directamente por las unidades APT que ejecutan las intrusiones. **Son administradas de forma independiente por ciberdelincuentes o intermediarios**, quienes bajo un modelo de servicio alquilan acceso temporal y simultáneo a diversos grupos de ciberespionaje. Como consecuencia operativa directa, la dirección IP de origen observada durante un ataque pierde su validez como indicador único para la atribución del incidente.

Para lograr una identificación precisa del actor de amenaza, es prioritario realizar un análisis forense exhaustivo enfocado en el arsenal técnico desplegado y en las Tácticas, Técnicas y Procedimientos (TTPs) evidenciados dentro de la infraestructura comprometida.

Técnicas y Tácticas — MITRE ATT&CK

Las siguientes técnicas han sido identificadas en la campaña UAT-9244 y la infraestructura ORB3/SPACEHOP asociada:

Técnica ID	Nombre	Táctica	Descripción Operacional
T1574.002	DLL Side-Loading	Evasion	wsprint.exe (firmado) fuerza la carga de BugSplatRc64.dll maliciosa desde C:\ProgramData\WSPrint\. Payload inyectado en msiexec.exe en memoria sin escritura en disco.
T1055.001	DLL Injection / Process Injection	Evasion	TernDoor inyecta shellcode en el proceso legítimo msiexec.exe para ocultar actividad de red y evitar detección de herramientas de seguridad.
T1543.003	Windows Service (Kernel Driver)	Persistencia / Escalación	WSPrint.sys instalado como servicio de kernel. Crea \Device\VMTool. Suspende, reanuda o termina procesos de AV/EDR (técnica BYOVD).
T1053.005	Scheduled Task	Persistencia	Tarea programada 'WSPrint' ejecuta wsprint.exe como SYSTEM en /sc onstart. Claves de registro del Task Scheduler modificadas para ocultar la tarea de herramientas de administración estándar.
T1547.001	Registry Run Keys	Persistencia	Clave en HKCU\Software\Microsoft\Windows\CurrentVersion\Run para garantizar ejecución de TernDoor incluso si la tarea programada es eliminada (persistencia redundante).
T1562.001	Disable/Modify Security Tools	Evasion	WSPrint.sys (nivel kernel) termina procesos de agentes EDR y antivirus, cegando la visibilidad de seguridad del host afectado antes de la exfiltración.
T1610	Deploy Container	Evasion	PeerTime detecta Docker en el host víctima y se autoejecutar dentro de un contenedor para aislarse del sistema operativo anfitrión y evadir detección de seguridad.
T1036.005	Process Masquerading	Evasion	PeerTime renombra su proceso en caliente para suplantar demonios legítimos de Linux (sshd, syslogd) mientras mantiene sockets de red externos abiertos.
T1071.005	BitTorrent P2P C2	C2	PeerTime usa protocolo BitTorrent para recibir comandos y transferir archivos. El tráfico C2 se mimetiza con distribución legítima de datos, rompiendo detección basada en dominios C2 fijos.
T1090.003	Multi-hop Proxy (ORB)	C2	Red ORB3/SPACEHOP enruta tráfico de intrusiones a través de 16+ nodos VPS en India (ASN 136258) antes de llegar a la víctima. Impide atribución por IP de origen.
T1573	Encrypted Channel (TLS Custom)	C2	Servidores C2 de UAT-9244 usan certificados SSL autofirmados con metadatos específicos: Subject CN=8.8.8.8, validez 2022-2023. Nodos ORB usan cert. genéricos C=US,CN=SERVER.
T1110.001	Password Guessing (BruteEntry)	Acceso Inicial / Lateral	BruteEntry (Go) realiza fuerza bruta masiva contra SSH:22, PostgreSQL:5432 y Apache Tomcat:8080 en lotes de hasta 1,000 IPs objetivo. Reporta éxitos al C2 en formato JSON.
T1595	Active Scanning	Reconocimiento	BruteEntry solicita al C2 lotes de objetivos externos y los escanea desde el host comprometido, convirtiendo a la víctima en nodo de la red ORB para ataques secundarios.
T1584.004	Compromise Server (VPS)	Recurso	Administradores ORB aprovisionan VPS clonados en Tencent, Alibaba, Stark Industries y BrainStorm Network como nodos de reté provisionales de la red de tránsito.
T1584.008	Compromise Network Devices	Recurso	FLORAHOX/ORB2 explota vulnerabilidades en firmware de routers SOHO (Cisco, Asus, D-Link, Draytek) para reclutarlos como nodos híbridos con implantes PETALTOWER/SHIMMERPICK.

Hallazgos Técnicos Detallados - Cadena de Ejecución: Modus Operandi UAT-9244 (Tres Capas)

PASO 1 Acceso Inicial y Evasión en Windows: TernDoor

Mecanismo: El atacante deposita el ejecutable legítimo y firmado wsprint.exe junto a la DLL maliciosa BugSplatRc64.dll en C:\ProgramData\WSPrint\. Cuando wsprint.exe se ejecuta (vía tarea programada o Run key), carga automáticamente la DLL maliciosa mediante el mecanismo de búsqueda de DLLs de Windows (DLL Side-Loading). La DLL ejecuta shellcode directamente en memoria para inyectar a TernDoor dentro del proceso legítimo msiexec.exe, evitando depositar el payload en disco en cualquier forma reconocible.

Evasión de defensas: TernDoor instala WSPrint.sys como servicio de kernel de Windows. Este controlador opera en Ring 0 y crea el dispositivo \Device\VMTool, empleado para suspender o terminar directamente los procesos de agentes EDR y antivirus activos en el sistema, cegando toda telemetría de seguridad local antes de iniciar la operación de espionaje.

PASO 2 — Persistencia Multi-Arquitectura en Linux/IoT: PeerTime

Mecanismo: PeerTime es un backdoor ELF compilado para múltiples arquitecturas (ARM, MIPS, MIPSEL, PPC, AARCH64, x86_64), diseñado para infectar enrutadores, servidores de virtualización y sistemas Linux sin agentes de seguridad instalados. El script de instalación en Bash evalúa la presencia de Docker en el host; si existe, PeerTime se ejecuta de forma aislada dentro de un contenedor para evadir por completo la monitoración del SO anfitrión.

C2 Descentralizado (BitTorrent): El método de comunicación con el operador emplea el protocolo BitTorrent para recibir comandos y transferir archivos exfiltrados. Al comunicarse de manera peer-to-peer con otros hosts comprometidos de la botnet, el tráfico de C2 se mimetiza con redes de distribución de datos legítimas, invalidando defensas basadas en detección de dominios C2 fijos o listas de bloqueo de IPs.

PASO 3 — Expansión de la Red ORB y Movimiento Lateral: BruteEntry

Mecanismo: BruteEntry (escrito en Go) es instalado en los servidores perimetrales comprometidos de las empresas de telecomunicaciones víctimas. El binario registra el equipo con el servidor C2 de UAT-9244 y solicita lotes de hasta 1,000 direcciones IP de objetivos externos. El servidor comprometido inicia entonces un escaneo masivo de fuerza bruta contra SSH (TCP/22), PostgreSQL (TCP/5432) y Apache Tomcat (TCP/8080).

Las intrusiones exitosas se reportan automáticamente al C2 via JSON ({"success": true}), permitiendo a los atacantes apalancarse en el ancho de banda y los recursos computacionales de la víctima para realizar ataques secundarios a escala global.

Ciclo de Ofuscación Redes ORB

El panorama actual del ciberespionaje exige una comprensión profunda de las infraestructuras de ofuscación avanzadas, específicamente de las redes de retransmisión operativa (ORB) como CHARLIE, las cuales operan bajo un modelo de infraestructura como servicio malicioso. Esta red es administrada de forma independiente y alquilada a múltiples actores de amenazas alineados con la República Popular China, incluyendo a los grupos APT5 y APT15, proporcionando un canal encubierto para sus operaciones tácticas. El ecosistema utiliza servidores ACOS para orquestar la conexión del Comando y Control (C2) a través de una malla de nodos efímeros, cuya vida útil de apenas 31 días y nula detección en motores antivirus anulan la eficacia de los bloqueos estáticos tradicionales. Para Colombia, esta evolución técnica representa un riesgo crítico e inminente, dado que el clúster de intrusiones UAT-9244 emplea activamente esta infraestructura compartida para vulnerar proveedores de telecomunicaciones y entidades de infraestructura crítica a nivel nacional. Debido a la naturaleza multi-inquilino de estas redes, la dirección IP pierde total validez para la atribución, obligando a los analistas a priorizar la identificación de las tácticas, técnicas y procedimientos (TTPs) del adversario en cada incidente.

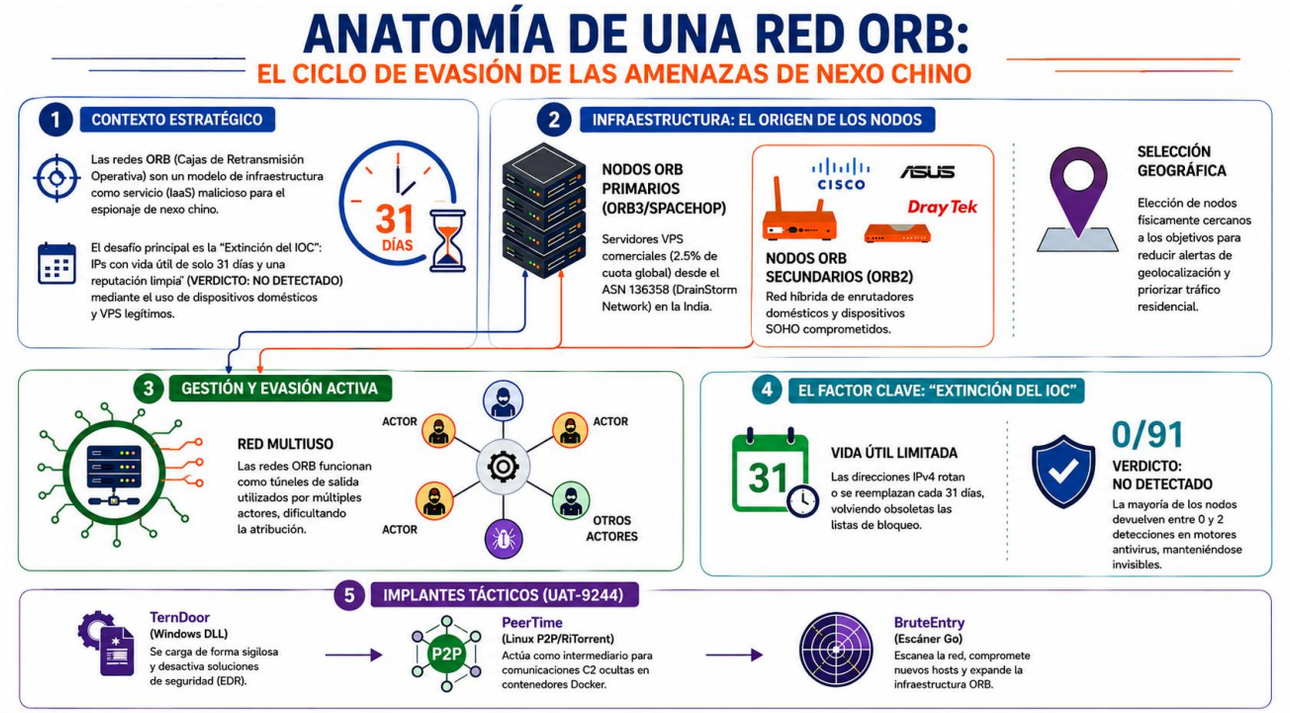
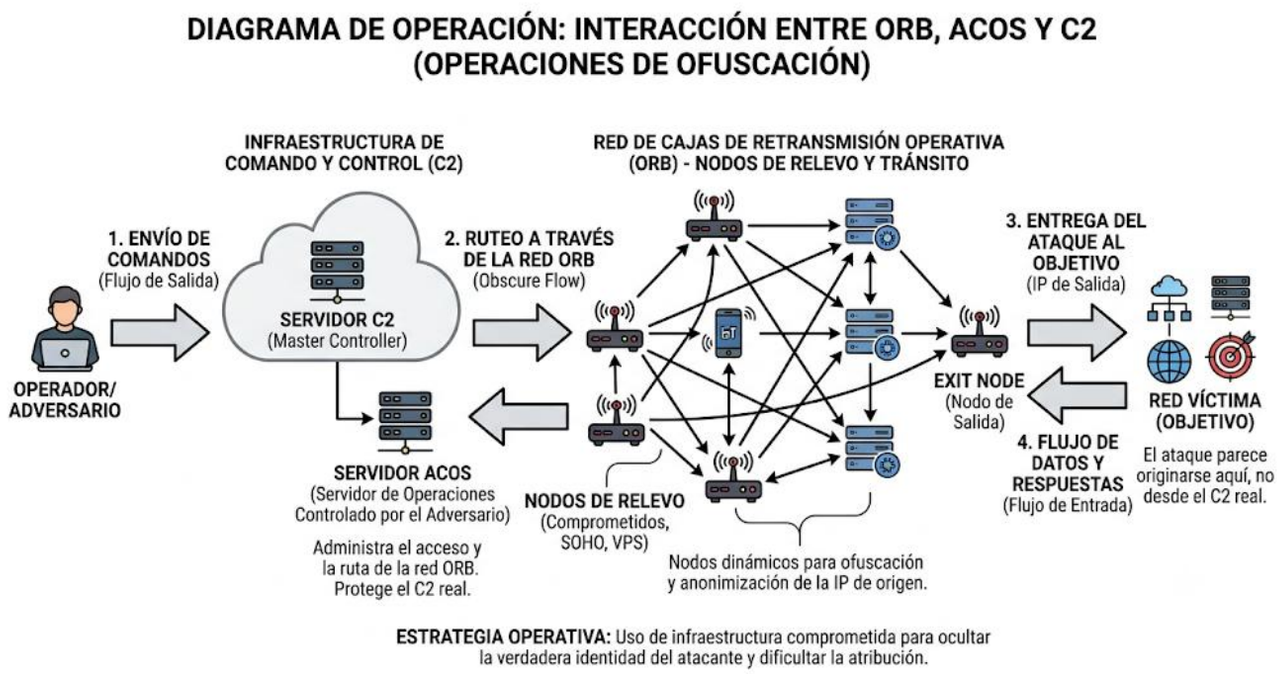


Diagrama de Operación ORB, ACOS y C2



El diagrama detalla la sincronización encubierta donde el servidor ACOS actúa como el cerebro operativo que configura y administra dinámicamente los nodos de la red ORB. Gracias a esta orquestación, el servidor C2 logra enrutar sus comandos tácticos a través de la compleja malla de dispositivos de tránsito de la ORB. En consecuencia, cuando el ataque alcanza a la red víctima desde el nodo de salida final, la ubicación e identidad real de la infraestructura central (C2 y ACOS) quedan totalmente ofuscadas.

Recomendaciones de Detección y Mitigación

FASE 1: Prevención Proactiva

Endurecimiento de Dispositivos de Borde

- ❑ Deshabilitar las interfaces de administración web (HTTP/HTTPS), SSH y Telnet expuestas directamente a WAN en todos los routers perimetrales, firewalls, concentradores VPN y balanceadores de carga.
- ❑ Reemplazar dispositivos en EOL (End-of-Life) de Cisco, Asus, Draytek, D-Link y Ruckus que no reciben actualizaciones de firmware. Son vectores primarios de FLORAHOX/ORB2.
- ❑ Implementar segmentación del plano de administración: toda gestión de red debe requerir canal seguro aislado o acceso local; nunca expuesto a la WAN.

Controles de Identidad y Acceso (Zero Trust)

- ❑ Implementar autenticación multifactor resistente a phishing (FIDO2/hardware security keys) para todos los usuarios remotos, con acceso condicional reforzado para conexiones desde ISPs residenciales o proveedores de hosting desconocidos.
- ❑ Bloquear automáticamente o requerir verificación adicional para accesos desde ASNs de VPS comerciales (Stark Industries, BrainStorm Network, Tencent Cloud, Vultr) que no correspondan al perfil geográfico habitual del usuario.

Defensa contra TernDoor (Capa Windows)

- ❑ Implementar Windows Defender Application Control (WDAC) o AppLocker para bloquear la carga de controladores de kernel no aprobados, especialmente WSPrint.sys. Activar la Microsoft Vulnerable Driver Blocklist (BYOVD prevention).
- ❑ Habilitar Safe DLL Search Order via GPO. Restringir permisos de escritura en C:\ProgramData\ a usuarios no administrativos para impedir el depósito de BugSplatRc64.dll.

Defensa contra PeerTime (Capa Linux/IoT)

- ❑ Implementar inspección profunda de paquetes (DPI) en NGFW para bloquear tráfico BitTorrent originado en redes de servidores de producción, data centers y enrutadores de telecomunicaciones.
- ❑ Montar particiones /tmp y /dev/shm con la opción noexec en /etc/fstab para impedir ejecución de binarios ELF descargados por el script de instalación de PeerTime.

Defensa contra BruteEntry (Capa de Red)

- ❑ Segmentar estrictamente la red de salida: prohibir a servidores de bases de datos y aplicaciones internas iniciar conexiones directas a Internet en puertos SSH (22), PostgreSQL (5432) y Apache Tomcat (8080/8443).
- ❑ Implementar reglas de rate-limiting para conexiones salientes simultáneas. Una explosión de conexiones a cientos de IPs externas desde un servidor interno es el indicador más visible de compromiso por BruteEntry.

FASE 2: Detección de compromisos activos

Reglas SIEM — Lógica de Correlación

Regla SIEM	Condición	Acción
REGLA-ORB-001 Rot. de ASN Residencial	Mismo User ID autentica exitosamente desde 2 IPs con ASNs residenciales de países distintos en <2 horas, sin viaje físico plausible.	**ALERTA CRITICA:** Posible secuestro de sesión vía nodo de salida ORB. Suspender sesión. Solicitar re-autenticación MFA.
REGLA-ORB-002 Proc. Crítico a IP VPS	Proceso del endpoint (powershell.exe, wscript.exe, msiexec.exe) realiza conexión saliente a IP en ASN de hosting VPS comercial con 0-2 detecciones en VirusTotal.	**ALERTA:** Investigar como posible C2 sigiloso de TernDoor. Aislar endpoint para análisis forense.

Regla SIEM	Condición	Acción
REGLA-ORB-003 SSH en Puerto 64719	Cualquier dispositivo de la red interna establece conexión SSH saliente en TCP/64719 hacia IP externa.	ALERTA CRITICA: Puerto característico de SPACEHOP. Aislar dispositivo. Adquirir volcado de memoria RAM.
REGLA-ORB-004 BitTorrent en Produc.	Servidor de producción, router o PLC inicia tráfico BitTorrent (peer-to-peer) hacia IPs externas.	ALERTA CRITICA: Indicador de infección por PeerTime. Aislar inmediatamente.
REGLA-ORB-005 Explosion Conexiones	Servidor interno genera >500 conexiones salientes simultáneas TCP a IPs únicas externas en <5 minutos.	ALERTA: Posible compromiso por BruteEntry. Bloquear salida de red del host. Iniciar IR.

Búsqueda Activa de Amenazas (Threat Hunting)

- ❑ Buscar en hosts Windows el proceso wsprint.exe cargando DLLs no firmadas desde C:\ProgramData\. Cualquier coincidencia es un indicador crítico de TernDoor.
- ❑ Auditar la existencia del servicio de kernel WSPrint.sys y del dispositivo \Device\VMTool en todos los endpoints Windows del entorno.
- ❑ En sistemas Linux/IoT: detectar procesos que se renombran en caliente usando /proc/[PID]/cmdline divergente del nombre de proceso real, especialmente suplantando sshd, syslogd u otros demonios del sistema.
- ❑ Monitorear creación de contenedores Docker no registrados en herramientas de orquestación (Kubernetes, Docker Swarm) desde usuarios o scripts no administrativos.

Detección TLS/SSL — Zeek/Suricata/Censys

- ❑ Buscar certificados SSL con Subject/Issuer C=US,CN=SERVER y C=US,CN=CA en tráfico de red interno. Son firmas genéricas reutilizadas por nodos ORB3.
- ❑ Alertar sobre certificados con validez superior a 10 años (ej. 2022-2042) en conexiones HTTPS hacia rangos de IP no clasificados como productivos.
- ❑ Buscar el SHA-256 0c7e36683a100a96f695a952cf07052af9a47f5898e1078311fd58c5fdbdecc8 y SHA-1 2b170a6d90fceba72aba3c7bc5c40b9725f43788 en logs de inspección TLS.

FASE 3: Respuesta y Contención

Protocolo de Respuesta ante Compromiso Confirmado.

- ❑ Aislamiento previo a reinicio: Desconectar físicamente o aislar mediante VLAN el equipo comprometido antes de reiniciar. TernDoor inyecta payloads en memoria y borra rastros del disco al finalizar; un reinicio destruirá evidencia forense irremplazable.
- ❑ Adquisición de memoria RAM: Capturar volcado de memoria del sistema afectado (ej. WinPmem en Windows, LiME en Linux) como primer paso forense.
- ❑ Reset masivo de credenciales: Forzar cambio de contraseñas para todas las cuentas de administración local y de dominio que interactuaron con el dispositivo afectado.
- ❑ Eliminar persistencias: Remover la tarea programada 'WSPrint', limpiar HKCU\...\Run, deshabilitar el servicio WSPrint.sys y revocar el dispositivo \Device\VMTool.
- ❑ Firma AV: Verificar que las consolas antivirus cuentan con firmas para Win.Malware.TernDoor, Unix.Malware.PeerTime y Unix.Malware.BruteEntry y que SNORT SID 65551 está activo.

Fuentes

Cisco Talos. (2026, 10 de marzo). UAT-9244 targets South American telecommunication providers with three new malware implants. Talos Intelligence Group. https://www.virustotal.com/gui/collection/report--170726c5be37fdea5e01246bd5f7f9db7577e7df1e585e481fadce828c205e9f

Cybersecurity and Infrastructure Security Agency. (2024, 8 de julio). CISA Advisory AA24-190A: PRC State-Sponsored Cyber Actors Target U.S. Critical Infrastructure. CISA.

Mandiant. (2024, 22 de mayo). ¿Extinción del COI? Actores de ciberespionaje China-Nexus utilizan redes ORB para aumentar el coste de los defensores (M. Raggi, Ed.). Mandiant Intelligence. https://www.virustotal.com/gui/collection/report--23-00066288

Mandiant Group. (2024, 26 de mayo). OT Threat Watch: May 20–26, 2024 - ARCMAZE ORB Network Used by Chinese Espionage Actors. Google Threat Intelligence. https://www.virustotal.com/gui/collection/report--24-10014692

MITRE. (2024, abril). MITRE ATT&CK Framework v15 — Enterprise Matrix. The MITRE Corporation.

National Security Agency & Cybersecurity and Infrastructure Security Agency. (2023, mayo). People's Republic of China State-Sponsored Cyber Actors Target US Critical Infrastructure (Joint Cybersecurity Advisory). NSA.

SecurityScorecard. (2025, 24 de junio). Widespread Chinese cyberespionage campaign powered by ORB network. SecurityScorecard Strike Analysis. https://www.virustotal.com/gui/collection/report--648751eb8b74a121ca838d3c9cacc56d5af4c7cceff0bdb1ea355d0502305b8d

Team Cymru. (2026, 18 de febrero). ORB Networks Mask Cyberattacks Using Compromised IoT Devices and SOHO Routers. Pure Signal Scout Portal. https://www.virustotal.com/gui/collection/report--d427c946717522401e7ce8c5ada5f5c9556a9012c52575ec9b1adab6c6be480a