Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

APT-15 REFUERZA SU PRESENCIA EN LATAM: ACTIVIDAD SILENCIOSA PERO EFECTIVA

06/ 05 / 2025

CONTENIDO

INTRODUCCIÓN

El grupo de ciberespionaje chino conocido como APT-15 ha intensificado su actividad en los últimos meses, desplegando operaciones sofisticadas para infiltrarse en sistemas gubernamentales y robar información sensible. Su actuar sigiloso, respaldado por tácticas avanzadas y recursos estatales, ha encendido las alarmas en el sector de la ciberseguridad, especialmente por el repunte reciente de ataques en países de la región. Esta amenaza silenciosa representa un riesgo persistente, capaz de operar durante largos periodos sin ser detectada.

APT-15 REFUERZA SU PRESENCIA EN LATAM: ACTIVIDAD SILENCIOSA PERO EFECTIVA

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_05_06_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	06/05/2025
Es día cero (0 day):	No

RESUMEN

El grupo de ciberespionaje chino conocido como APT-15 ha intensificado su actividad en los últimos meses, desplegando operaciones sofisticadas para infiltrarse en sistemas gubernamentales y robar información sensible. Su actuar sigiloso, respaldado por tácticas avanzadas y recursos estatales, ha encendido las alarmas en el sector de la ciberseguridad, especialmente por el repunte reciente de ataques en países de la región. Esta amenaza silenciosa representa un riesgo persistente, capaz de operar durante largos periodos sin ser detectada.

¿Quiénes son APT-15?

APT-15, también conocido como **Ke3chang, Vixen Panda, Nickel o Nylon Typhoon**, es un grupo de ciberespionaje vinculado a intereses estatales chinos. Su actividad comenzó al menos en 2010 y se ha documentado en campañas dirigidas a instituciones diplomáticas, gubernamentales y organizaciones estratégicas en todo el mundo. En su comunicado, las autoridades estadounidenses confirmaron la presencia de una amenaza persistente avanzada (APT), conocida como APT-15, asociada con China y vinculada a intrusiones en organismos gubernamentales a nivel global, con énfasis en países de Centroamérica y Sudamérica.

Este grupo tiene un objetivo claro: obtener información confidencial relacionada con asuntos políticos, estratégicos y de relaciones exteriores, utilizando herramientas digitales avanzadas y técnicas de persistencia silenciosa que dificultan su detección.

¿Cómo opera APT-15?

APT-15 se distingue por su meticulosidad y su capacidad para pasar desapercibido. Una de sus tácticas más comunes son las campañas de spear phishing, donde correos electrónicos diseñados para engañar a empleados estratégicos permiten el acceso a las redes internas. Una vez dentro, los atacantes se mueven con cautela, escalando privilegios, explorando el entorno y estableciendo persistencia a largo plazo.

Estos accesos no son inmediatos ni ruidosos: APT-15 permanece oculto durante semanas o meses, recolectando información crítica sin levantar sospechas. Su sofisticación se muestra en su capacidad para aprovechar tanto vulnerabilidades recientes como brechas de seguridad previamente conocidas, pero sin corregir en muchas organizaciones.

Características clave de sus operaciones:

- Accesos iniciales silenciosos mediante ingeniería social avanzada.
- Uso de exploits zero-day y vulnerabilidades conocidas, pero sin parchar.
- Persistencia profunda, permaneciendo dentro de las redes sin ser detectados.
- Extracción sigilosa de datos sensibles a servidores controlados por los atacantes.

Aumento reciente de actividad

En fechas recientes, se ha observado un aumento sostenido de ataques atribuibles a APT-15 en una institución gubernamental de la región. Este ataque, llevado a cabo con precisión, comprometió redes

internas mediante el acceso a credenciales privilegiadas e instalaciones de puertas traseras que permitieron la exfiltración controlada de documentos sensibles relacionados con relaciones exteriores.

El incidente mostró la capacidad del grupo para evadir controles de seguridad y su interés en acceder a información estratégica de alto nivel, posiblemente vinculada a decisiones diplomáticas o acuerdos internacionales. Estos ataques no buscan causar caos inmediato, sino recolectar inteligencia valiosa para fines geopolíticos.

La presencia activa de APT-15 marca un punto de inflexión: sus tácticas evolucionan y su selección de objetivos demuestra una comprensión profunda del contexto político y tecnológico local.

El impacto de APT-15 en la ciberseguridad global

El impacto de los ciberataques de APT-15 va más allá de la pérdida de información. Afecta directamente la confianza en las infraestructuras digitales de las naciones y empresas objetivo. En particular, las instituciones gubernamentales son los principales blancos, lo que puede tener consecuencias políticas y diplomáticas de gran alcance.

Tácticas y Técnicas de MITRE ATT&CK

APT-15 se caracteriza por el uso de un conjunto sofisticado de tácticas, técnicas y procedimientos (TTPs) que le permiten infiltrarse, mantenerse oculto y extraer información confidencial de sus objetivos. Estas TTPs, documentadas en el marco ATT&CK de MITRE, combinan métodos clásicos de ingeniería social con herramientas avanzadas de explotación, persistencia y exfiltración, adaptándose al entorno específico de cada víctima y aprovechando tanto fallas técnicas como debilidades humanas. A continuación, se detallan algunas de las principales técnicas observadas en sus campañas recientes.

Táctica	Técnica	ID (MITRE ATT&CK)	Uso por APT-15
Initial Access	Spear Phishing Attachment	T1566.001	Envían correos con archivos adjuntos maliciosos para obtener acceso inicial.
Initial Access	Spear Phishing Link	T1566.002	Usan enlaces en correos dirigidos para redirigir a sitios con exploits.
Credential Access	Valid Accounts	T1078	Utilizan credenciales legítimas robadas para acceder y moverse lateralmente.
Persistence	Web Shell	T1505.003	Implementan web shells en servidores comprometidos para mantener el acceso.

Táctica	Técnica	ID (MITRE ATT&CK)	Uso por APT-15
Execution	Command and Scripting Interpreter	T1059	Ejecutan comandos o scripts para moverse, espiar o desplegar herramientas.
Defense Evasion	DLL Side-Loading	T1574.002	Cargan DLLs maliciosas desde ubicaciones legítimas para evadir detección.
Command and Control	Application Layer Protocol	T1071	Comunican datos exfiltrados o comandos usando protocolos comunes como HTTP/HTTPS.
Persistence	Scheduled Task/Job	T1053	Crean tareas programadas para mantener la persistencia en el sistema.
Collection	Data Staged	T1074	Preparan archivos o información para su posterior exfiltración.
Exfiltration	Exfiltration Over C2 Channel	T1041	Extraen datos a través del mismo canal de comando y control que ya tienen activo.
Defense Evasion	Masquerading	T1036	Ocultan archivos o procesos maliciosos como componentes legítimos del sistema.
Command and Control	Remote Access Software	T1219	Utilizan herramientas de acceso remoto para controlar sistemas comprometidos.
Defense Evasion	Obfuscated Files or Information	T1027	Ofuscan scripts o binarios para evitar la detección por herramientas de seguridad.
Defense Evasion	Process Injection	T1055	Inyectan código malicioso en procesos legítimos para evadir controles.
Credential Access	Unsecured Credentials	T1552	Acceden a credenciales almacenadas en texto claro o mal protegidas.

Recomendaciones

- **Monitoreo y detección de intrusiones**: Implementar herramientas avanzadas de monitoreo para detectar actividad sospechosa, como patrones de acceso inusuales o tráfico no autorizado, es esencial para identificar ataques de APT-15 en fases tempranas.
- **Revisión y fortalecimiento de contraseñas**: Aplicar políticas de contraseñas fuertes y únicas, junto con la implementación de autenticación multifactor (MFA) en todos los sistemas sensibles, ayudará a proteger las credenciales contra el robo.
- **Segmentación de redes**: Aislar segmentos críticos de la red para limitar el movimiento lateral en caso de una brecha, dificultando el acceso no autorizado a información sensible.
- **Gestión de parches y actualizaciones**: Asegurarse de que todos los sistemas y aplicaciones estén actualizados con los últimos parches de seguridad para evitar la explotación de vulnerabilidades conocidas, que APT-15 aprovecha con frecuencia.
- **Revisión de la seguridad en la cadena de suministro**: Realizar auditorías y controles de seguridad en los proveedores y socios, ya que APT-15 puede infiltrarse a través de relaciones externas y vulnerabilidades en la cadena de suministro.
- **Pruebas de penetración periódicas**: Realizar pruebas de penetración para identificar brechas de seguridad, simular ataques reales y asegurar que las defensas sean adecuadas frente a amenazas avanzadas como las de APT-15.

NOTICIA COMPLETA

https://devel.group/blog/apt-15-refuerza-su-presencia-en-latam-actividad-silenciosa-pero-efectiva/

CONTACTOS DE SOPORTE

Correo electrónico: info@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/