digital

5ta Edición

REPORTE CIBERSEGURIDAD 2025

Desarrollado por el Centro de Ciberinteligencia

Índice

BIENVENIDA DEL GERENTE SERVICIOS CIBERSEGURIDAD

En esta quinta edición del reporte anual de ciberseguridad de Entel Digital, el escenario global y en Latinoamérica no parece cambiar radicalmente con el año pasado.

El Ransomware se consolida como la amenaza predominante. Los actores del cibercrimen logran, mediante técnicas más eficientes y mayores recursos, penetrar los sistemas de las organizaciones, exfiltrar datos y afectar la continuidad de los negocios.

Aunque las defensas mejoran, los programas de ciberseguridad son adoptados en todas las organizaciones y todas las soluciones declaran integrar Inteligencia Artificial (IA) y mejorar su efectividad, ¿qué tipo de recursos les falta a las empresas y organizaciones?

Creemos que son dos: la ciberinteligencia y la capacidad de análisis y anticipación.

Este reporte que aborda el año 2025, presenta investigaciones, análisis y recomendaciones de nuestros equipos expertos. Ponemos a disposición de nuestra comunidad, tanto privada como pública, un trabajo experto para explicar, compartir y reflexionar sobre las técnicas de ataques, el cibercrimen organizado, las nuevas brechas de la IA y las nuevas regulaciones con las cuales Chile se ha dotado.

Me complace además contarles que Entel ha sido reconocida este año como la empresa privada de mayor aporte al MISP nacional y por nuestra colaboración desde Entel Digital.

Si bien los impactos reales son cada vez más importantes -pagos por extorsión de información, negocios paralizados, imposibilidad de facturar a los clientes, atender pacientes en hospitales y consultorios, realizar transacciones o despachar mercancías-, al final podemos afirmar que 'Good guys are winning'.

Efectivamente, el conjunto de políticas aplicadas, las inversiones, la formación, la concientización del usuario y las soluciones tecnológicas que combinan automatización y autoaprendizaje, tienen un impacto en los tiempos de respuesta, la recuperación tras incidentes y la reducción de riesgos y vulnerabilidades explotables.

Espero que el reporte anual de Entel Digital les ayude a anticipar amenazas, desarrollar capacidades y abordar riesgos con nuevos conocimientos y conceptos.

Les deseo éxito en sus esfuerzos por mejorar la ciberseguridad de sus organizaciones.

Cyril Delaere
Gerente Servicios
Ciberseguridad Entel Digital

digital

Capítulo

01.

INTRODUCCIÓN

Según el Centro de Ciberinteligencia de Entel Digital, en 2024 las amenazas avanzaron a nivel global, lideradas por el Ransomware, que concentra el 38% de los ataques.

INTRODUCCIÓN

El Reporte de Ciberseguridad 2025 ha sido elaborado en un escenario de amenazas cibernéticas en constante transformación, marcado por la acelerada digitalización, la creciente sofisticación de los actores maliciosos y la adopción masiva de tecnologías como la Inteligencia Artificial (IA) y el Internet de las Cosas (IoT). Este informe tiene como propósito ofrecer un análisis exhaustivo de las principales tendencias, técnicas y actores que definieron el año 2024, junto con una proyección de los desafíos y oportunidades que enfrentará la región durante 2025.

Dirigido a empresas, instituciones gubernamentales y especialistas en ciberseguridad, este reporte busca no solo proporcionar un diagnóstico del panorama actual de ciberseguridad, sino también entregar recomendaciones prácticas que permitan fortalecer las defensas cibernéticas, mejorar la resiliencia organizacional y fomentar la colaboración entre sectores estratégicos. Con un enfoque que combina una visión global y regional, se destacan los sectores más afectados, los incidentes más relevantes y los avances tecnológicos que marcaron el año.

RESUMEN EJECUTIVO

Durante 2024, el panorama de ciberseguridad estuvo marcado por un aumento sostenido en la frecuencia y sofisticación de los ciberataques, consolidando al Ransomware como la principal amenaza, tanto a nivel global como en Latinoamérica y el Caribe. Según los registros de CCI Entel Digital, el Ransomware representó el 38% de todas las ciberamenazas registradas, con los meses de mayo y octubre destacándose como los de mayor actividad, concentrando el 13% y 12% del total anual, respectivamente.

En Latinoamérica y el Caribe, los países más afectados fueron Brasil (46%), México (17%) y Argentina (10%), que en conjunto acumularon más del 73% de los incidentes. Chile, por su parte, se posicionó como el cuarto país más afectado, representando el 7% de los ataques en la región, lo que refleja una atención constante de los ciberactores hacia las economías emergentes con infraestructuras tecnológicas en desarrollo. En conjunto, los cinco principales países, que incluyen también a Colombia (7%) y Perú (6%), concentraron el 86% de los ataques.

El impacto financiero de los ciberataques siguió una tendencia al alza, con un costo promedio de violación de datos de 4,88 millones de dólares, un 9,7% más que en 2023, lo que refleja la creciente sofisticación de las tácticas de los ciberactores.

Entre las tácticas y métodos más utilizados destacó el uso de tecnologías de Inteligencia Artificial (IA) para automatizar campañas, evadir defensas y dirigir ataques de forma más precisa. Además, el crecimiento de plataformas de Ransomware-as-a-Service (RaaS) facilitó que incluso actores menos experimentados realizaran ataques a gran escala, contribuyendo a un incremento del 30% en el cibercrimen organizado.

A nivel global, los sectores más afectados por el Ransomware fueron:

30% **Comercio mayorista y servicios**

7% **Salud**

7% **Construcción**

En Latinoamérica, los tres principales actores de Ransomware fueron:

18% **RansomHub**

14% **LockBit**

6% **Akira**

Estos dominaron el panorama regional, evidenciando su capacidad de operar a gran escala en sectores estratégicos.

Por otro lado, los incidentes de Data Breach mostraron una dinámica relevante. Aunque en 2024 se registró una disminución del 15% respecto al peak histórico de 442 casos en 2023, con un total de 374 incidentes, la cifra sigue siendo considerablemente alta. Este comportamiento subraya la persistencia de esta amenaza y destaca la necesidad urgente de fortalecer las estrategias de seguridad de los datos para mitigar su impacto.

Finalmente, el 32% de los ataques de Ransomware en 2024 se originaron en vulnerabilidades no parchadas, evidenciando la importancia crítica de mantener los sistemas actualizados y aplicar controles de seguridad más robustos. Además, el Ransomware evolucionó hacia modelos más agresivos de doble y triple extorsión, con el 90% de las víctimas enfrentando amenazas de publicación de datos.

El 2024 fue un año de transformación en el ámbito de la ciberseguridad, caracterizado por un crecimiento sostenido en amenazas dirigidas y el impacto del cibercrimen organizado. Este reporte no solo documenta las tendencias más relevantes, sino que también ofrece proyecciones clave para 2025, destacando la importancia de tomar medidas proactivas y colaborativas para fortalecer las capacidades defensivas en la región.

digital

Capítulo

02.

VISIÓN GLOBAL DE CIBER AMENAZAS

En 2024, los sectores más afectados globalmente por Ransomware, según CCI Entel Digital, fueron Comercio mayorista y servicios (30%), Salud (7%) y Construcción (7%).

2.1 TENDENCIAS GENERALES DE AMENAZAS

Los Grupos de Amenaza Persistente Avanzada (APT) son actores, respaldados frecuentemente por estados-nación o financiados por organizaciones criminales sofisticadas, que se especializan en ataques dirigidos y altamente estratégicos. A diferencia de los cibercriminales convencionales, los grupos APT operan con un enfoque de largo plazo.

Utilizan tácticas avanzadas para:

- Conseguir información sensible
- Robar propiedad intelectual
- Realizar espionaje estratégico

Su capacidad para adaptarse y mantenerse activos dentro de redes comprometidas los convierte en una amenaza persistente y de alto impacto para sectores críticos, como:

- Gobiernos
- Infraestructuras esenciales
- Corporaciones de alto valor estratégico

Entre los 5 grupos APT con mayor presencia en 2024, se encuentran:

Lazarus Group

Origen:
Corea del Norte

Alcance:
Global

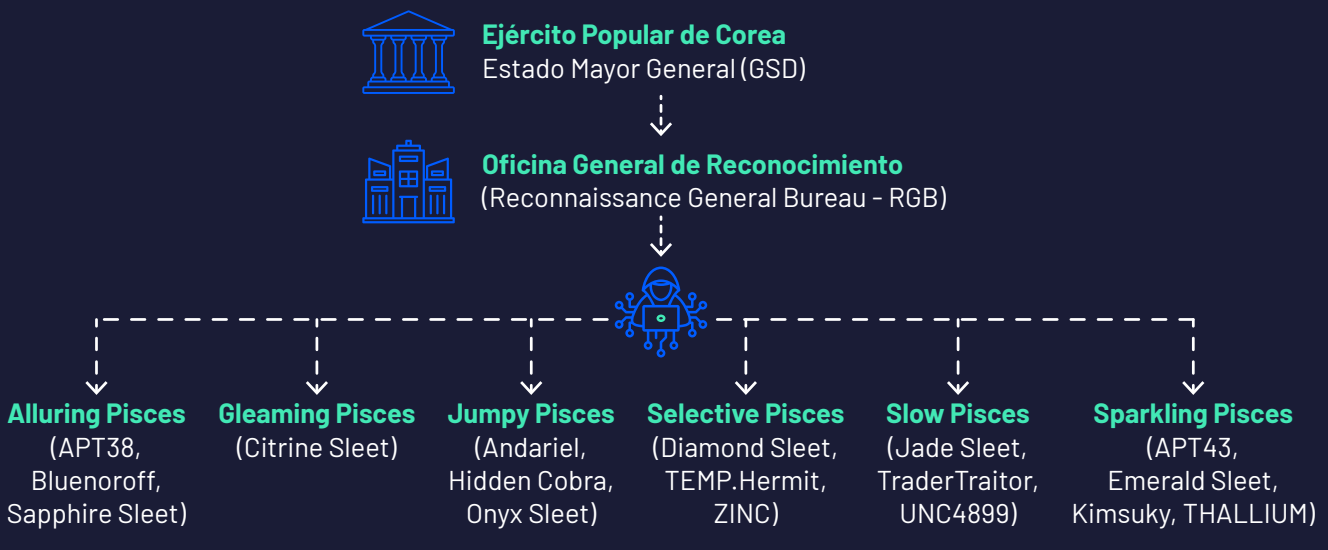
Herramientas:
RATANKBA, WannaCry

(aka: APT 38, Bluenoroff, Hidden Cobra, Dark Seoul)

Es un grupo de ciberamenazas patrocinado por el estado de Corea del Norte, que se ha atribuido a la Oficina General de Reconocimiento (OGR), la principal fuente de inteligencia y operaciones especiales de Corea del Norte. Se especializa en espionaje militar, operaciones clandestinas y actividades cibernéticas ofensivas, actuando como el núcleo de la estrategia de inteligencia del régimen norcoreano.

La OGR es responsable de coordinar y dirigir grupos de hackers como Lazarus Group, Kimsuky y Andariel, que llevan a cabo actividades de ciberespionaje, ataques a Infraestructuras Críticas y robos de criptomonedas para financiar al régimen.

Actores de amenaza patrocinados por el Estado de Corea Del Norte



Fuente: Unit42

Actividad

- **Sony:** en 2014, un ataque a Sony involucró información confidencial y personal de la empresa.
- **Banco de Bangladesh:** en 2016, Lazarus robó millones de dólares de la institución financiera.
- **WannaCry:** su campaña más destructiva hasta la fecha fue con el Ransomware WannaCry, en 2017, que afectó entre 230,000 y 300,000 computadoras en 150 países. El ataque explotó una vulnerabilidad en el sistema operativo Windows, enfocándose en equipos que no habían aplicado un parche de seguridad crítico publicado por Microsoft.
- **WazirX:** en julio del 2024, Lazarus ejecutó un ataque dirigido contra WazirX, una de las principales plataformas de intercambio de criptomonedas en India. Los atacantes comprometieron la infraestructura de la billetera multisig de la plataforma, logrando sustraer aproximadamente $234.9 millones en activos digitales.
- **Criptomonedas:** recientemente, Lazarus ha utilizado el Malware RATANKBA para atacar a empresas de criptomonedas.

TTP's

Estas son las principales Tácticas, Técnicas y Procedimientos que utiliza Lazarus para sus ataques.

Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Drive-by Compromise	Exploitation for Client Execution	Account Manipulation	Account Manipulation	Debugger Evasion	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Fallback Channels	Exfiltration Over C2 Channel	Data Destruction
Gather Victim Org Information	Valid Accounts	Native API	Valid Accounts	Valid Accounts	Deobfuscate/ Decode Files or Information		Debugger Evasion		Data from Local System	Ingress Tool Transfer		Service Stop
		Windows Management Instrumentation			Impersonation		File and Directory Discovery			Multi-Stage Channels		System Shutdown/ Reboot
					Indicator Removal		Network Service Discovery			Non-Standard Port		
					Indirect Command Execution		Process Discovery					
					Reflective Code Loading		Query Registry					
					System Binary Proxy Execution		System Information Discovery					
					Template Injection		System Network Configuration Discovery					
					Valid Accounts		System Network Connections Discovery					
					XSL Script Processing		System Owner/ User Discovery					
							System Time Discovery					

Backdoors

El backdoor abre una "puerta trasera" en un sistema infectado, permitiendo que atacantes accedan de forma remota y sin autorización. Esto les da la capacidad de controlar el sistema, extraer información o instalar otros programas dañinos, a menudo evadiendo los mecanismos de seguridad y permaneciendo activos por largos periodos.

Para ganar persistencia en las redes comprometidas, Lazarus utiliza los siguientes Malware:

HardRain

Familia:
Hidden Cobra.

Propósito Principal:
Acceso Persistente.

Atributos Principales:

Sigilo
- Capacidad de evasión de sandboxes.
- Detección de máquinas virtuales.

Comunicaciones
- Cifrado AES y RC4.
- Canal seguro con servidor C2.

Duuzer

Clasificación:
Troyano / Spyware

Objetivo Principal:
Sistemas empresariales (Manufactura y Tecnología)

Atributos Principales:

Espionaje
- Sistema de keylogging avanzado.
- Capacidad de captura de pantalla.

Escalación
- Creación de usuarios privilegiados.
- Manipulación de permisos del sistema.

Destover

Clasificación:
Wiper (Malware Destructivo)

Objetivo Principal:
Corporaciones y Entidades Gubernamentales

Atributos Principales:

Destrucción
- Sobrescritura profunda de archivos.
- Corporación del MBR.
- Daño permanente a particiones.

Impacto
- Daño irreversible al sistema.
- Pérdida total de datos.

Remote access Trojans (RATs)

Es un Malware que permite obtener acceso remoto no autorizado a un sistema infectado. Con esta herramienta, los atacantes pueden controlar el sistema a distancia, robar información, registrar pulsaciones de teclas o instalar otros programas maliciosos, frecuentemente sin ser detectados y manteniendo el acceso por largos periodos de tiempo.

Fallchill

Origen:
APT - Patrocinio Estatal

Propósito:
Espionaje y Control Remoto

Atributos Principales:

Reconocimiento
- Scanner de procesos activos.
- Enumeración de sistema operativo.
- Mapeo de red.

Control
- Ejecución remota de comandos.
- Shell remoto.
- Gestión de tareas.

Comunicaciones
- Canal cifrado con C2.
- Transferencia segura de datos.
- Capacidad de actualización modular.

Joanap

Propósito Principal:
Espionaje a Largo Plazo

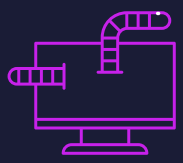
Especialidad:
Control de Red Distribuida

Atributos Principales:

Control de Red
- Gestión de botnet.
- Capacidad de proxy.
- Operaciones distribuidas.

Espionaje
- Robo de documentos.
- Captura de credenciales.
- Exfiltración sigilosa.

Persistencia
- Inyección en procesos.
- Tareas programadas.
- Auto-supervivencia.



Brambul

Clasificación:
Gusano de Red

Propósito:
Ciberespionaje y Propagación Automatizada

Atributos Principales:

Propagación
- Scanner de red activo.
- Explotación de SMB.
- Auto-replicación en recursos compartidos.

Fuerza Bruta
- Ataque a credenciales débiles.
- Diccionario de contraseñas por defecto.
- Persistencia en intentos.

Reconocimiento
- Mapeo de red.
- Recolección de credenciales.
- Enumeración de IP.

Mirror Face

Origen: Japón

Alcance: Japón y Unión Europea

Herramientas: HiddenFace

(aka: Earth Kasha)

Este grupo fue detectado por primera vez atacando una entidad en Europa. El ataque se dirigió contra una organización diplomática de la Unión Europea y utilizó como señuelo la Exposición Mundial de Osaka, que se celebrará en Japón en 2025.

Para llevar a cabo la intrusión, MirrorFace envió un correo electrónico de Spear Phishing que incluía un enlace a un archivo ZIP. Dentro, con un LNK disfrazado como un documento de Word. Al abrirse, mostraba un documento señuelo y ejecutaba la versión 5.5.5 del backdoor ANEL.

Al día siguiente, los atacantes desplegaron su principal herramienta maliciosa, HiddenFace (también conocida como NOOPDOOR), consolidando su acceso y capacidad para comprometer a la víctima.

Actividad

Organizaciones japonesas

En julio de 2024 llevó a cabo ataques dirigidos contra organizaciones japonesas, incluyendo medios de comunicación, entidades políticas y académicas. También utilizó la herramienta NOOPDOOR, empleando correos electrónicos de spear-phishing para infiltrarse en las redes de las víctimas para obtener el acceso inicial.

TTP's

Estas son las principales Tácticas, Técnicas y Procedimientos que utiliza Mirror Face para sus ataques.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Impact
External Remote Services	Inter-Process Communication	Boot or Logon Autostart Execution	Access Token Manipulation	Access Token Manipulation	OS Credential Dumping	Account Discovery	Remote Services	Archive Collected Data	Application Layer Protocol	Data Encrypted for Impact
Phishing	Native API	External Remote Services	Boot or Logon Autostart Execution	Deobfuscate/ Decode Files or Information		File and Directory Discovery		Data from Local System	Data Encoding	
	Scheduled Task/Job	Hijack Execution Flow	Hijack Execution Flow	Hide Artifacts		Process Discovery		Data from Network Shared Drive	Data Obfuscation	
	User Execution	Scheduled Task/Job	Process Injection	Hijack Execution Flow		System Information Discovery		Email Collection	Dynamic Resolution	
			Scheduled Task/Job	Impair Defenses		System Location Discovery			Encrypted Channel	
				Indicator Removal		System Owner/ User Discovery				
				Obfuscated Files or Information						
				Process Injection						

GAMAREDON

Origen: Rusia

Alcance: Ucrania, OTAN

Herramientas: PteroGraphin, PteroPSDoor, PteroSig

(aka: Armageddon, Iron Tilden, Primitive Bear)

Esta APT ha estado activa en ataques contra Ucrania, desde al menos 2013, perfeccionando herramientas maliciosas existentes y desarrollando nuevas capacidades. En agosto de 2024, se identificó una herramienta inédita basada en PowerShell llamada PteroGraphin. Este descargador persistente distribuye cargas útiles cifradas utilizando telegra.ph, la plataforma de publicación de Telegram.

Gamaredon realizó importantes modificaciones a uno de sus backdoors escritos en PowerShell, conocido como PteroPSDoor. Estas mejoras incluyeron la incorporación de múltiples capas de ofuscación y el almacenamiento de componentes clave en el registro de Windows, lo que aumentó significativamente su capacidad de operar de forma encubierta.

Por otro lado, el grupo también optimizó su herramienta de exfiltración de datos diseñada para la aplicación de escritorio de Signal. Este ajuste se implementó para adaptarse a los cambios recientes en Signal Desktop. Ahora, PteroSig puede analizar y descifrar la clave protegida por DPAPI utilizada por la aplicación, lo que le permite acceder nuevamente a los datos cifrados y extraerlos de manera efectiva.

Actividad

OTAN

En octubre de 2024 ESET informó que, aunque tradicionalmente Gamaredon ha centrado sus ataques en instituciones gubernamentales ucranianas, recientemente ha intentado comprometer objetivos en varios países de la OTAN.

TTP's

Estas son las principales Tácticas, Técnicas y Procedimientos que utiliza Gamaredon para sus ataques.

Execution	Persistence	Defense Evasion	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Native API	Office Application Startup	Deob-fuscate/ Decode Files or Information	File and Directory Discovery	Internal Spear-phishing	Automated Collection	Data Obfuscation	Automated Exfiltration
Windows Mana-gement Instrumen-tation		Execution Guardrails	Peripheral Device Discovery	Taint Shared Content	Data from Local System	Dynamic Resolution	Exfiltration Over C2 Channel
		Modify Registry	Process Discovery		Data from Network Shared Drive	Ingress Tool Transfer	
		Obfuscated Files or Information	System Information Discovery		Screen Capture	Web Service	
		Template Injection	System Owner/ User Discovery				

MuddyWater

Origen: Irán

Alcance: África, Oriente Próximo

Herramientas: Atera

(aka: Mercury, ATK51, G0069, Cobalt Ulster)

Es un grupo de ciberespionaje que se considera un elemento subordinado del Ministerio de Inteligencia y Seguridad de Irán. Ha pasado un tiempo considerable moviéndose lateralmente y realizando actividades manuales en distintos entornos objetivos.

En varios casos, ha utilizado recursos compartidos de red internos, como ubicaciones intermedias de almacenamiento de C&C. Sus operadores suelen recopilar información de reconocimiento y volcar credenciales en ubicaciones centralizadas de la red, antes de exfiltrar esos datos desde una única fuente.

También se ha centrado en varias empresas de servicios financieros en Kenia y Zambia, y en una víctima no identificada en Ghana. Además, atacó a una empresa de transporte de Israel, desplegando diversas herramientas.

Actividad

PowerShell

En noviembre de 2024 Sophos Managed Detection and Response (MDR) detectó una campaña en la que MuddyWater utilizaba correos electrónicos de Phishing para persuadir a las víctimas a descargar la herramienta legítima de gestión remota Atera. Una vez instalada, los atacantes emplearon comandos remotos para ejecutar scripts de PowerShell destinados a la extracción de credenciales y la creación de copias de seguridad del registro del sistema.

TTP's

Estas son las principales Tácticas, Técnicas y Procedimientos que utiliza MuddyWater para sus ataques.

Initial Access	Execution	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Exploit Public-Facing Application	Exploitation for Client Execution	Deob-fuscate/ Decode Files or Information	Credentials from Password Stores	File and Directory Discovery	Exploitation of Remote Services	Screen Capture	Ingress Tool Transfer	Exfiltration Over C2 Channel
	Windows Mana-gement Instrumen-tation			Process Discovery			Multi-Stage Channels	
				Software Discovery			Remote Access Software	
				System Information Discovery				
				System Network Confi-guration Discovery				
				System Network Connec-tions Discovery				
				System Owner/ User Discovery				

Kimsuky

(aka: Thallium)

Origen:
Corea del Norte

Alcance:
Corea del Sur, Instituciones Académicas

Herramientas:
Archivos de MSC

Es un grupo de ciberespionaje con sede en Corea del Norte, que ha estado activo desde al menos 2012. Se enfoca principalmente en think tanks, ONG y expertos en temas relacionados con Corea del Norte, utilizando señuelos como solicitudes de entrevistas, asesoramiento sobre tesis académicas o invitaciones a presentaciones públicas.

Con frecuencia, Kimsuky ha abusado de plataformas como Google Drive y Microsoft OneDrive para alojar documentos señuelo y como servidores de comando y control (C&C). Además, para la exfiltración de datos, el grupo empleó cuentas de Dropbox.

Una de sus tácticas más recientes incluye el uso de archivos de Microsoft Management Console (MSC). Estos archivos, habitualmente utilizados por administradores de sistemas, pueden ser manipulados para ejecutar cualquier comando en el sistema operativo. Los atacantes incluso pueden modificar el icono de un archivo MSC para que se asemeje a un documento PDF o Word.

Actividad

- **Korea Hydro & Nuclear Power**
  En 2014, atacó a la empresa energética.

- **CHM**
  En marzo de 2024, inició una campaña utilizando archivos Compiled HTML Help (CHM) maliciosos. Al abrirlos, se mostraba una pantalla de ayuda mientras se ejecutaba un script malicioso que recopilaba información del sistema.

- **Colaboraciones**
  En abril de 2024, colaboró con grupos como Lazarus y Andariel en ataques coordinados contra cerca de 10 empresas de defensa de Corea del Sur.

TTP's

Estas son las principales Tácticas, Técnicas y Procedimientos que utiliza Kimsuky para sus ataques.

Reconnaissance	Resource Development	Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Org Information	Acquire Infrastructure	Exploit Public-Facing Application	Browser Extensions	Process Injection	Deobfuscate/ Decode Files or Information	Adversary-in-the-Middle	File and Directory Discovery	Internal Spearphishing	Adversary-in-the-Middle	Ingress Tool Transfer	Exfiltration Over C2 Channel	Financial Theft
Phishing for Information	Develop Capabilities	External Remote Services	External Remote Services		Modify Registry	Multi-Factor Authentication Interception	Network Sniffing		Data from Local System	Remote Access Software		
Search Victim-Owned Websites					Obfuscated Files or Information	Network Sniffing	Process Discovery					
					Process Injection		Query Registry					
					Reflective Code Loading		System Information Discovery					
							System Network Configuration Discovery					
							System Service Discovery					

2.2 CIBERAMENAZAS EN INFRAESTRUCTURAS CRÍTICAS

Definición y normativa internacional

Las infraestructuras críticas son industrias que proporcionan servicios esenciales cuya interrupción puede tener graves consecuencias para la sociedad, la economía o la seguridad nacional.

Marco internacional

- **Directiva de Infraestructuras Críticas Europeas (ECI)** de la Unión Europea.
- **Departamento de Seguridad Nacional (DHS)** de EE.UU., con sectores críticos identificados por **CISA**.
- **Foro Económico Mundial (WEF):** Enfoque en riesgos globales.

Normas y estándares de seguridad

- **ISO 22301:** Gestión de la continuidad del negocio.
- **NIST Cybersecurity Framework:** Protección de infraestructuras críticas.

Legislaciones nacionales

La Ley 21663 o Ley Marco de Ciberseguridad, fue promulgada en Chile y publicada en el Diario Oficial el 8 de abril de 2024, y tiene por objeto establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares. Si bien es cierto, no define explícitamente el término "infraestructura crítica", establece un marco legal que regula los servicios esenciales y los operadores de importancia vital que son componentes críticos dentro de esta infraestructura.

Tanto los servicios esenciales como los operadores de importancia vital están sujetos a obligaciones específicas para proteger la infraestructura crítica de ciberataques. Estas obligaciones incluyen:

- Implementar sistemas de gestión de seguridad de la información
- Mantener registros de las acciones de seguridad
- Elaborar e implementar planes de continuidad operacional y ciberseguridad
- Realizar operaciones continuas de revisión y análisis de sus sistemas
- Adoptar medidas para reducir el impacto y la propagación de incidentes
- Informar a los afectados sobre incidentes
- Tener programas de capacitación en ciberseguridad
- Designar un delegado de ciberseguridad

Clasificación de Infraestructuras Críticas

Energía
Generación, transmisión y distribución de electricidad, petróleo y gas.

Agua y Saneamiento
Sistemas de agua potable y tratamiento de aguas residuales.

Salud
Hospitales, medicamentos y sistemas de emergencia.

Transporte
Aeropuertos, puertos, redes ferroviarias y transporte público.

TIC
Redes de telecomunicaciones, ciberseguridad y servicios en la nube.

Finanzas
Bancos, mercados financieros y pagos electrónicos.

Seguridad y Defensa Infraestructura militar, emergencias y fuerzas de seguridad.

Alimentación y Agricultura
Producción y almacenamiento de alimentos.

Industria Química y Nuclear Plantas químicas y nucleares.

Gobierno
Sistemas de gestión pública y de importancia estratégica.

Análisis de amenazas globales a Infraestructuras Críticas

Legislaciones como la Ley Marco de Ciberseguridad buscan resguardar los servicios esenciales de amenazas como:

Sector Eléctrico

- **Sandworm:** Malware destructivo en Ucrania.
- **DragonFly 2.0:** Ataques a energía en Europa y América del Norte.

Sector Agua

- **APT33 (Elfin Team):** Ataques a sistemas de tratamiento de agua.
- **Cyber Av3ngers:** Compromiso de estaciones de agua en Israel.

Sector Petróleo y Gas

- **Lazarus Group (APT38):** Robo financiero y sabotaje.
- **APT34 (Helix Kitten):** Ataques dirigidos a telecomunicaciones y energía.

Sector Manufacturero

- **FIN7:** Ataques financieros en retail y hospitalidad.
- **DarkSide:** Ransomware disruptivo en Infraestructura Crítica.

Sector Financiero

- **APT iraní Muddy Water:** Ataques dirigidos a instituciones financieras especialmente a organizaciones en Africa.
- **Trinity:** Robo de 560 GB de datos de la Agencia Tributaria Española.

Sector Salud

- **Qilin Ransomware (Ruso):** Ataque a Synnovis en Reino Unido.
- **Ascension Health System:** Sufrió ataque de ransomware ruso Conti en mayo 2024.

Sector Gobierno

- **Grupo APT Chino Webworm APT:** Ha utilizado SoftEther VPN Bridge en máquinas de organizaciones gubernamentales en la UE.
- **Grupos APT chinos:** Incidente en el Departamento del Tesoro de EE. UU., accediendo a sistemas mediante credenciales comprometidas.
- **TetrisPhantom:** Campaña contra entidades gubernamentales mediante explotación USB segura
- **Grupo APT Ruso:** Sednit atribuido a ataques a entidades gubernamentales y académicas.

Sector TI

- **Famous Chollima:** Parte del colectivo Lazarus, se infiltró en más de un centenar de empresas tecnológicas y fintech a nivel mundial.
- **APT31:** Campaña denominada "EastWind" contra organizaciones empresas informáticas rusas.
- **Midnight Blizzard:** Brecha que comprometió las cuentas de correo electrónico de los ejecutivos de la compañía.

Sector Telecomunicaciones

- **Infiltración en SingTel:** Por el grupo Volt Typhoon.
- **Salt Typhoon:** Dirigió una operación contra las redes de AT&T y Verizon.
- **Ataque a Snowflake:** Afectando a AT&T.

Sector Transporte

- **Tropic Trooper:** Campaña de ciberespionaje, apuntando a sectores gubernamental, sanitario, de transporte e industrias de alta tecnología en regiones como Taiwán, Filipinas y Hong Kong.
- **Mustang Panda:** Comenzó a atacar la industria de transporte de carga europea a principios de 2024.

Línea de tiempo de incidentes en Infraestructuras Críticas 2024

ENERO 2024

- **Ataque de Ransomware a LoanDepot:** 16.6 millones de clientes afectados.
- **Explotación de vulnerabilidades en Ivanti.**
- **Infiltración de Volt Typhoon** en sectores críticos.

FEBRERO 2024

- **Ransomware a Change Healthcare:** rescate de $22M.

MAYO 2024

- **Robo de datos en MediSecure:** 12.9 millones de afectados.

JUNIO 2024

- **Ataque al NHS del Reino Unido:** interrupción de servicios médicos.

JULIO 2024

- **Ransomware en Columbus:** exposición de 3.1 TB de datos sensibles.

AGOSTO 2024

- **Ataque al Aeropuerto de Seattle:** retrasos en operaciones críticas.

OCTUBRE 2024

- **Ataque a American Water:** compromiso de sistemas internos.

NOVIEMBRE 2024

- **Espionaje por Salt Typhoon:** en empresas de telecomunicaciones.

Tendencias y estadísticas clave

Sectores más afectados a nivel global

30% Comercio mayorista y servicios

7% Salud

7% Construcción

Sectores más afectados en Chile

21% Infraestructura TI

17% Banca y finanzas

13% Agricultura y ganadería

Grupos Activos en ICS

50 grupos identificados en ataques industriales

LockBit: responsable del 25% de los incidentes

Vulnerabilidades en ICS

80% De las vulnerabilidades detectadas en redes internas

Recomendaciones estratégicas para Infraestructuras Críticas

- **Plan de respuesta a incidentes:** Simulaciones específicas para entornos OT.
- **Arquitectura defensible:** Control robusto de accesos y segmentación de redes.
- **Visibilidad y monitoreo:** Inventarios y mapeo de vulnerabilidades.
- **Acceso remoto seguro:** Uso de MFA o herramientas seguras.
- **Gestión de vulnerabilidades:** Priorización de riesgos y mitigación proactiva.

2.3 RANSOMWARE

Durante el año 2024, el Ransomware siguió siendo una de las mayores amenazas en el panorama global de ciberseguridad.

Grupos altamente organizados, como LockBit, Play y RansomHub, lideraron los ataques en sectores clave, como:

Gobierno

Educación

Logística

Finanzas

El enfoque de estos actores evolucionó hacia tácticas de doble extorsión, donde los atacantes:

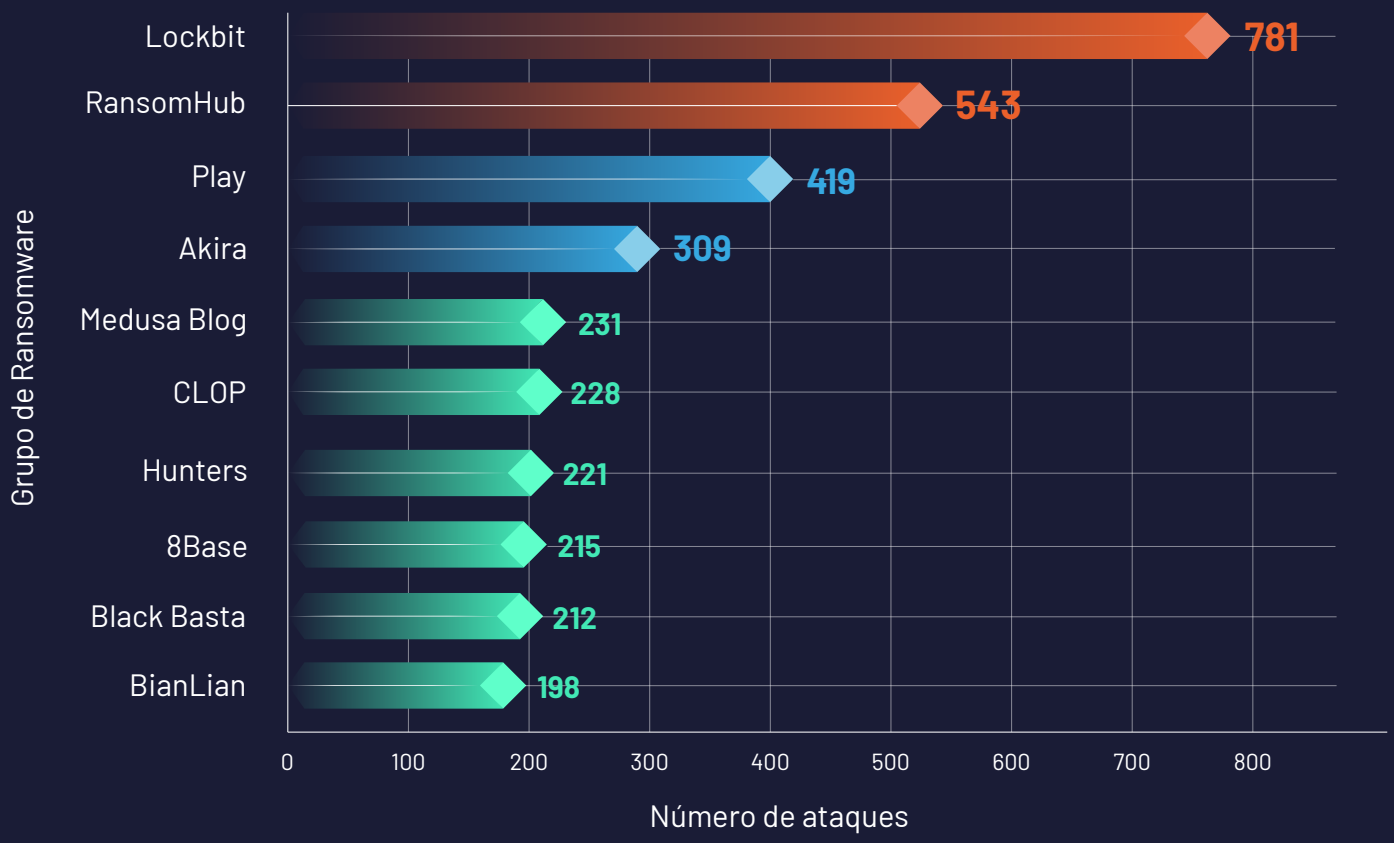
- Cifran los datos privados de la víctima en cuestión.
- Amenazan con publicarlos si no reciben el pago.

Además, ha habido un aumento significativo en el uso de plataformas automatizadas de Ransomware como Servicio (RaaS), lo que ha facilitado la entrada de atacantes menos experimentados en el mercado del cibercrimen.

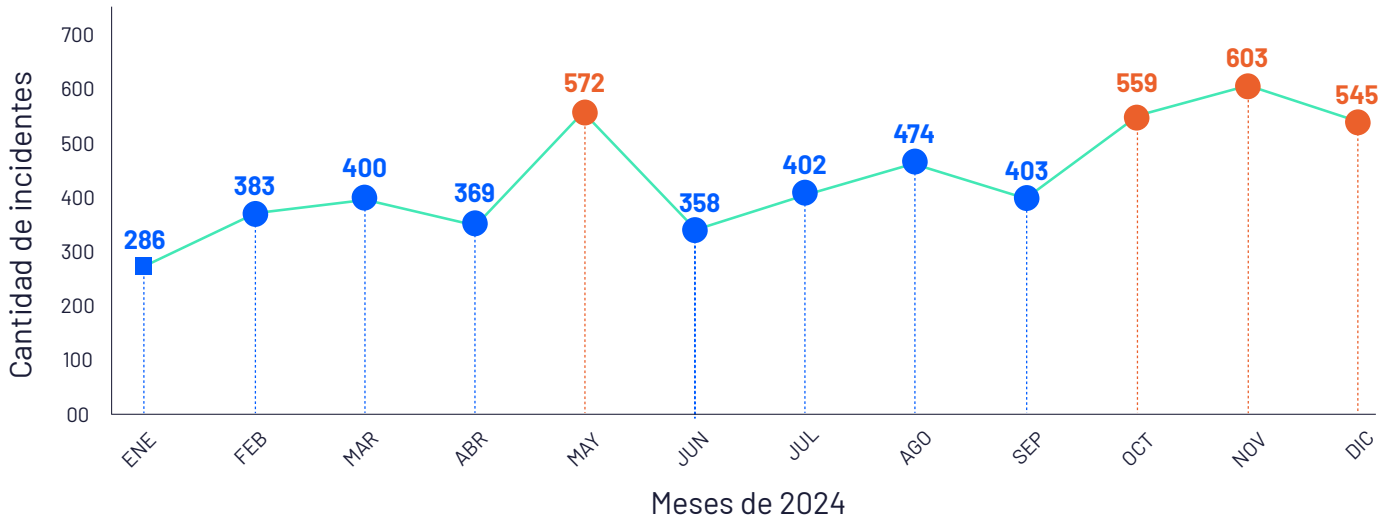
Una revisión de incidentes muestra que, debido a la sensibilidad de la información que manejan, los dos sectores que enfrentaron mayores desafíos fueron:

- Sector Gubernamental.
- Sector Educativo.

TOP 10 grupos de Ransomware a nivel global



Incidentes de Ransomware por mes en 2024



Industrias más afectadas por Ransomware en 2024

1343
Comercio mayorista y servicios

321
Salud

300
Construcción

246
Manufactura

196
Equipamiento Industrial

181
Finanzas

180
Tecnología

169
Legal

167
Retail

163
Educación

Causas de los ataques de Ransomware

Las causas raíz de estos ataques varían según el sector y los ingresos de la organización:

36%
Explotación de vulnerabilidades

29%
Correo electrónico malicioso

29%
Compromiso de credenciales

Explotación de vulnerabilidades: La amenaza principal

Por segundo año consecutivo, la explotación de vulnerabilidades se posiciona como la causa raíz más común de los ataques de Ransomware. Esto subraya la importancia crítica de mantener los sistemas y software actualizados con los últimos parches de seguridad.

Las organizaciones que son víctimas de ataques iniciados por la explotación de vulnerabilidades sin parchear enfrentan consecuencias más graves que otros casos.

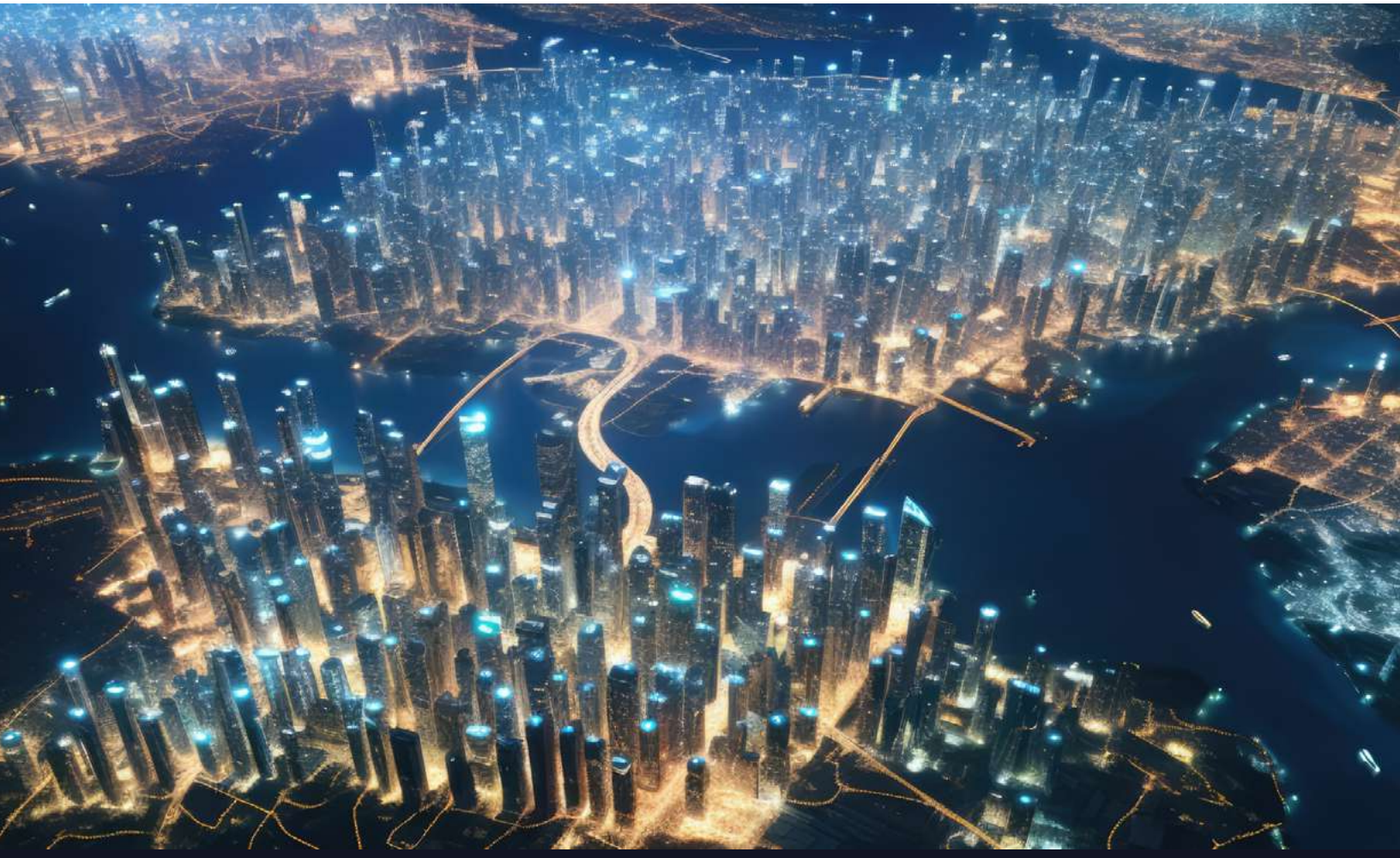
	Consecuencias de la explotación de vulnerabilidades	Consecuencias del compromiso de credenciales
Probabilidades de compromiso de las copias de seguridad	75%	54%
Índice de cifrado de datos	67%	43%
Predisposición a pagar rescate	71%	45%
Costos de recuperación	USD 3.000.000	USD 750,000
Víctimas que necesitan más de un mes para recuperarse	45%	37%

Correo electrónico malicioso: Un vector de ataque prevalente

Dentro de esta categoría, los correos electrónicos que contienen archivos maliciosos adjuntos o enlaces que descargan Malware son dos veces más comunes que en los ataques de Phishing. Es importante destacar que el Phishing, que generalmente se utiliza para robar credenciales de inicio de sesión, puede considerarse el primer paso en un ataque de compromiso de credenciales.

Compromiso de credenciales: Una amenaza creciente

Las organizaciones gubernamentales son particularmente susceptibles a este tipo de ataque. De hecho, el 49% de los ataques en el gobierno estatal/local y el 47% en el gobierno central/federal son originados por el uso de credenciales robadas.



2.4 CIBERCRIMEN ORGANIZADO

Los grupos de Ransomware y APT encabezan el crimen organizado, pues cuentan con los recursos para desarrollar herramientas de ciberespionaje o secuestro de datos, muchas veces gracias al financiamiento de gobiernos.

LockBit

Primera detección

Última versión

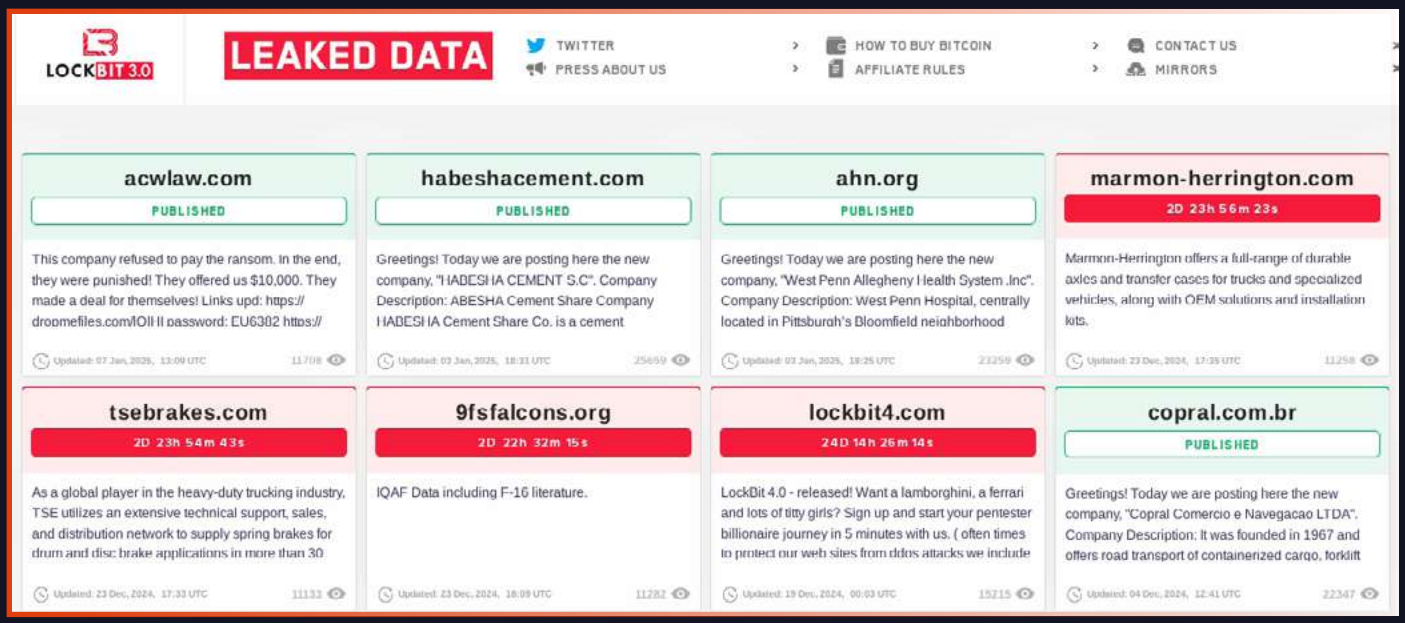
Singularidad

LockBit 3.0, lanzada en junio de 2022, introdujo mejoras clave como cifrado más robusto, tácticas avanzadas de exfiltración de datos y un modelo Ransomware-as-a-Service (RaaS) que ha atraído a numerosos afiliados, aumentando su alcance global.

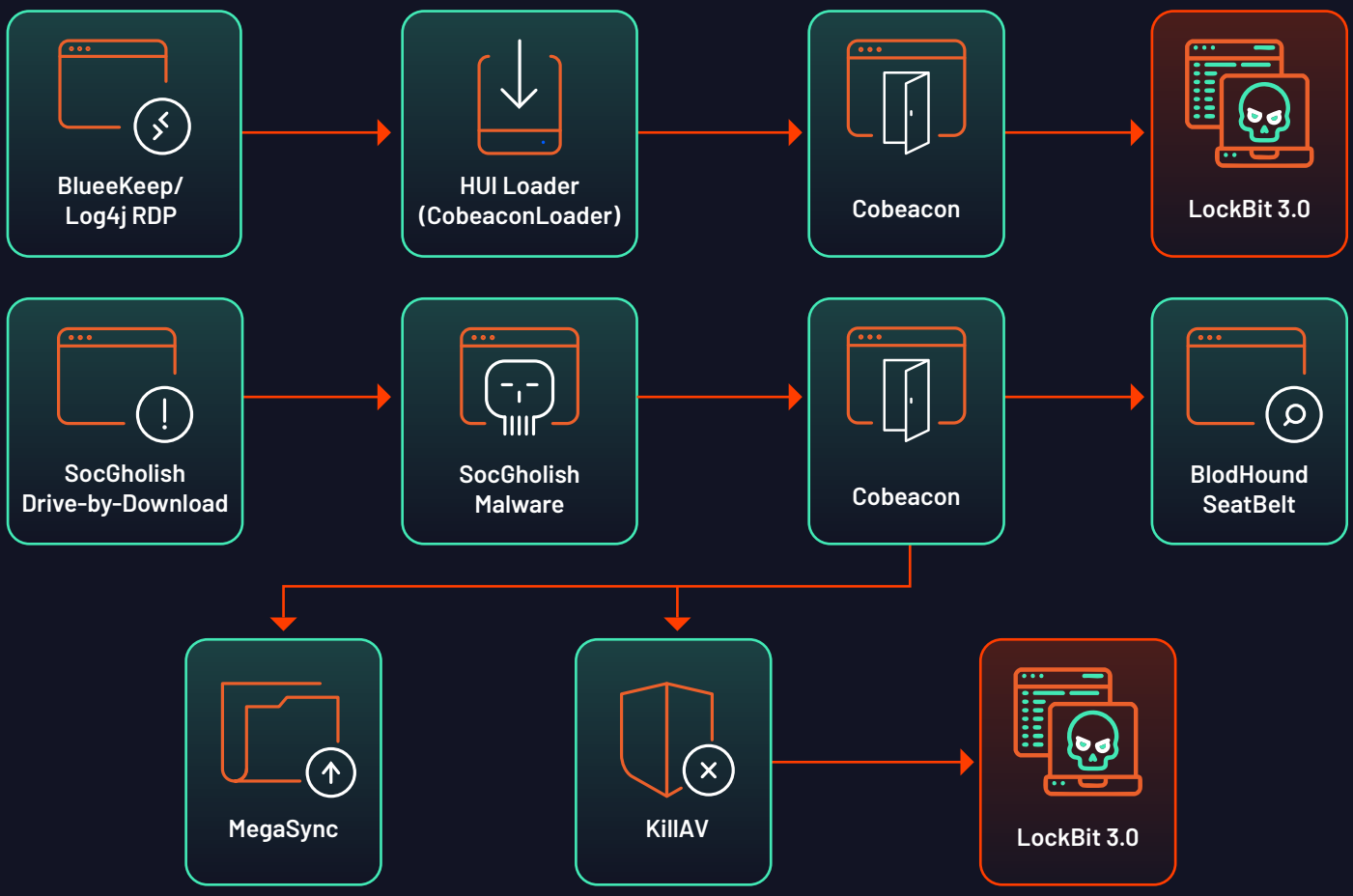
Hechos importantes: Operación Cronos

Fue una operación conjunta llevada a cabo por agencias policiales de 10 países, con el objetivo de interrumpir y desmantelar LockBit.

- **Coordinada por:** la Agencia Nacional contra el Crimen del R.U., el FBI y el grupo de trabajo internacional de aplicación de la ley de la Operación Cronos
- **Objetivo:** tomar el control de los activos y la infraestructura utilizada por los operadores de LockBit, así como recopilar información vital
- **Participación:** Australia, Canadá, Finlandia, Francia, Alemania, Japón, Países Bajos, Suecia, Suiza, Reino Unido y Estados Unidos, junto con Europol



Cadena de ataque de LockBit



Estos son los pasos de la cadena de ataque de Lockbit:

1 Acceso Inicial

- Obtienen acceso principalmente a través de servidores comprometidos, cuentas RDP adquiridas de afiliados o vulnerabilidades como CVE-2018-13379 en VPNs de Fortinet.
- También se han identificado vectores como correos no deseados y fuerza bruta de credenciales RDP o VPN.

2 Ejecución

- Se ejecuta generalmente mediante línea de comandos, tareas programadas o herramientas de post-explotación como PowerShell Empire.
- Puede especificar rutas específicas para cifrar archivos.

3 Acceso a Credenciales

- Utiliza herramientas como Mimikatz para recopilar credenciales.
- Aprovecha las credenciales obtenidas por afiliados.

4 Evasión de Defensa

- Desactiva soluciones de seguridad usando herramientas como GMER, PC Hunter o Process Hacker.
- Desactiva políticas de grupo para inhabilitar Windows Defender.

5 Descubrimiento

- Utiliza escáneres como Network Scanner, Advanced Port Scanner y AdFind.
- Mapea redes y localiza controladores de dominio o servidores de Active Directory.

6 Movimiento Lateral

- Propaga el ransomware mediante SMB.
- Utiliza credenciales robadas, políticas de grupo, PsExec o Cobalt Strike.

7 Exfiltración

- Roba datos utilizando herramientas como MEGA, FreeFileSync o el Malware StealBit.
- Transfiere archivos a servidores externos.

8 Impacto

- Realiza cifrado local y de red utilizando AES combinado con RSA, y optimiza cifrando solo los primeros 4KB de cada archivo.
- Reemplaza fondos de pantalla con notas de rescate, envía paquetes WoL para activar unidades de red y utiliza impresoras para imprimir las notas.

PLAY

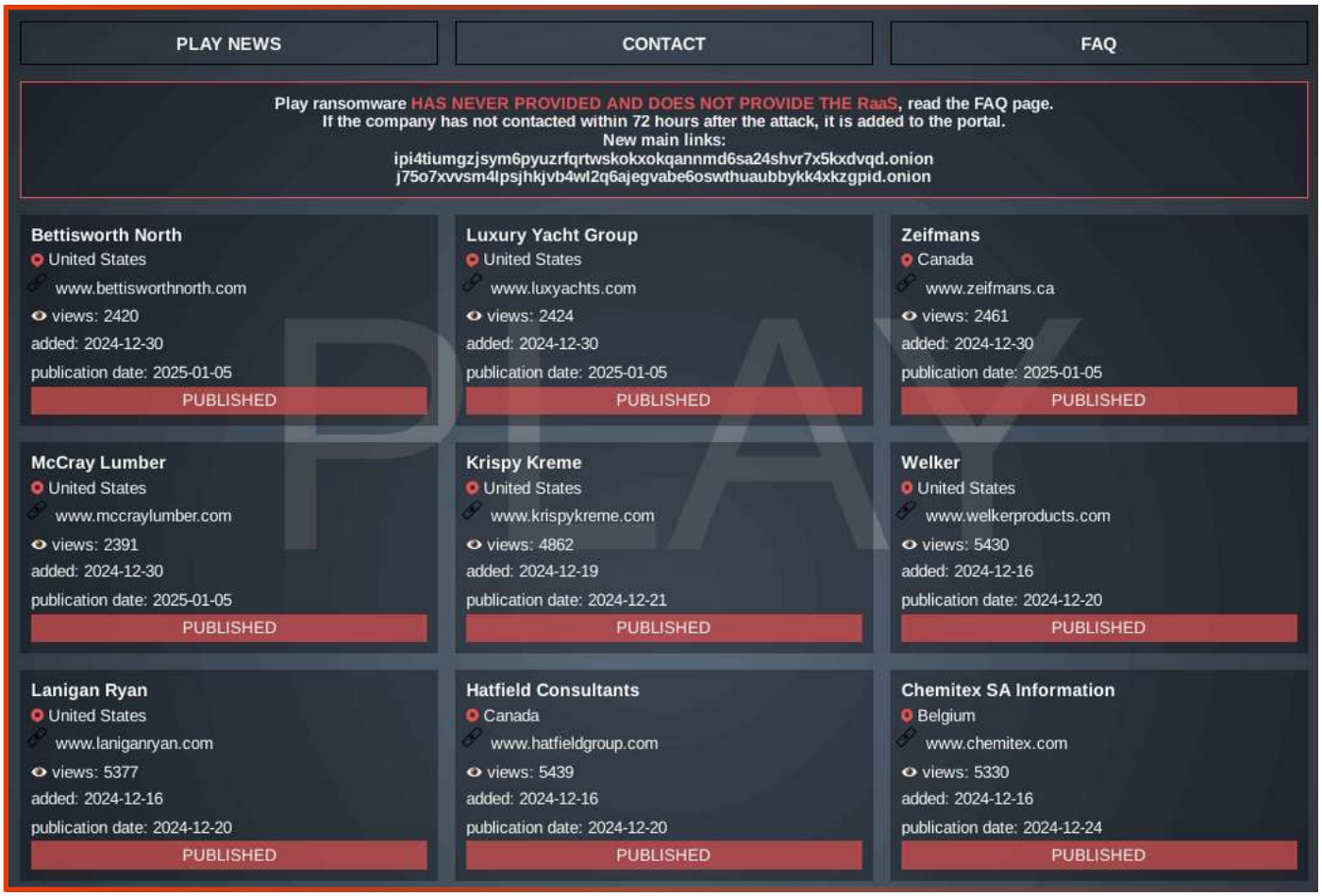
2022
Primera detección

PlayCrypt
AKA

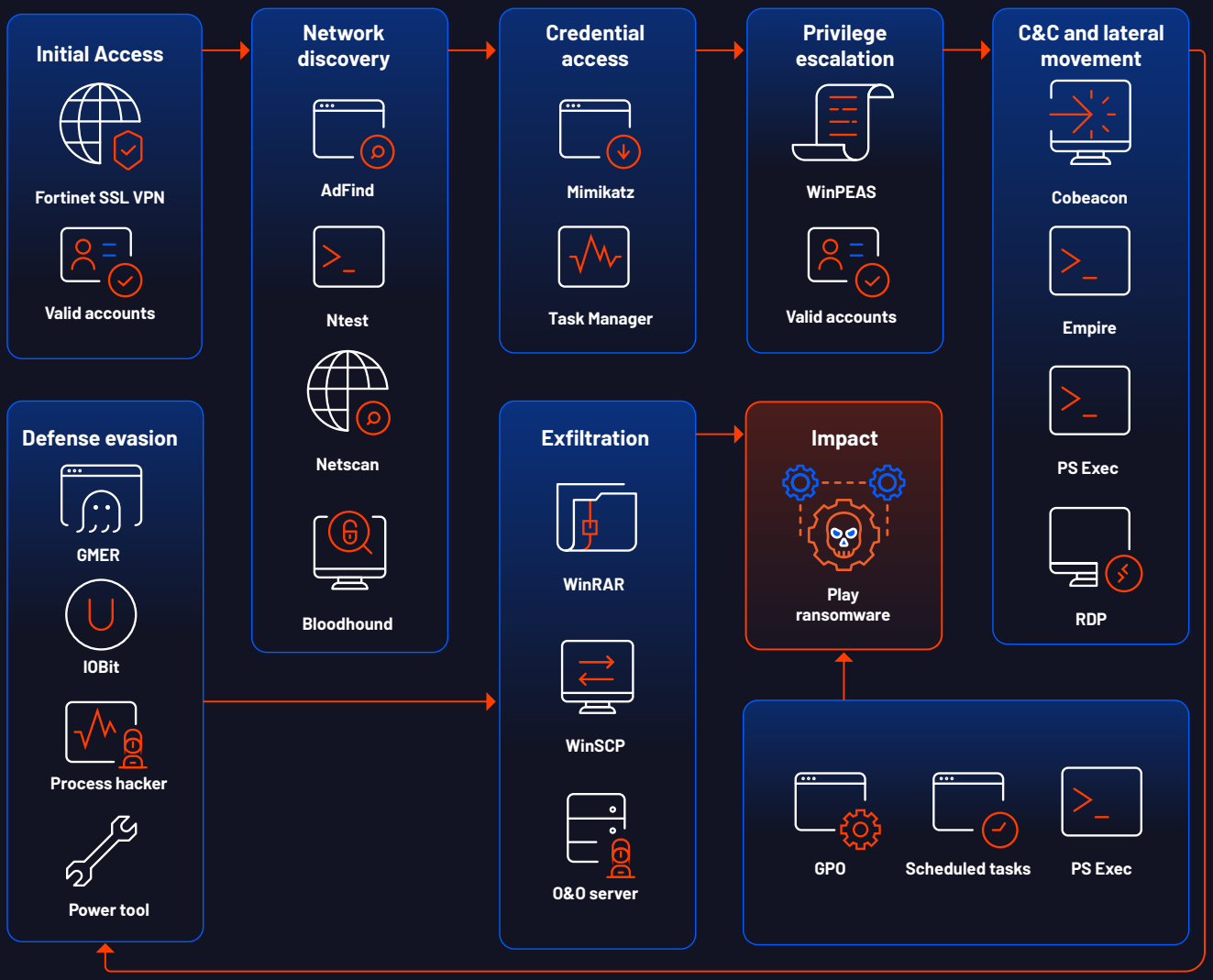
Modelo doble extorsión
Singularidad

Este grupo opera con un modelo de doble extorsión, generalmente explotando vulnerabilidades en dispositivos Fortinet SSL VPN o Microsoft Exchange.

Igualmente, consigue credenciales legítimas en mercados ilegales para obtener el acceso inicial.



Cadena de ataque de PLAY



Estos son los pasos en la cadena de infección de PLAY:

1 Acceso Inicial

- Usan cuentas reutilizadas, expuestas o adquiridas en mercados ilegales, incluyendo credenciales de VPN, cuentas locales y de dominio.
- Aprovechan servidores con Protocolo de Escritorio Remoto (RDP) accesibles públicamente para establecer un punto de entrada.

2 Explotación de Vulnerabilidades

- Explotan vulnerabilidades como Fortinet SSL VPN, CVE-2018-13379 y CVE-2020-12812.
- Igualmente, se valen de ProxyNotShell (CVE-2022-41040) y CVE-2022-41082, así como de OWASSRF (CVE-2022-41080).

3 Reconocimiento

- Usa herramientas como ADFind, NItest, BloodHound y Grixba.
- Recopila nombres de hosts, recursos compartidos e información de dominio.

4 Acceso a Credenciales

- Uso de Mimikatz para extraer credenciales y LSASS dump mediante el Administrador de Tareas de Windows.
- Grixba para obtener información adicional sobre archivos y procesos críticos.

5 Escalada de Privilegios

- Uso de Mimikatz para extraer credenciales de memoria y añadir cuentas a grupos privilegiados como Administradores de Dominio.
- Empleo de WinPEAS para identificar posibles caminos de escalamiento local.

6 Movimiento Lateral

- Utiliza herramientas como Cobalt Strike SMB Beacon, SystemBC y Empire.
- Uso de Mimikatz para obtener acceso administrativo y moverse lateralmente.

7 Evasión de Defensas

- Desactivación de seguridad con herramientas como Process Hacker, GMER, IOBit, PowerTool y PowerShell.
- Ocultación de rastros y eliminación de logs con wevtutil o scripts batch.
- Scripts en PowerShell (codificados en Base64) para ejecutar herramientas como Cobalt Strike y Empire.

8 Exfiltración

- Fragmentación de datos para evitar detecciones y uso de WinSCP (cliente SFTP) para transferir datos.
- Compresión de archivos con WinRAR en formato .RAR y transferencia de archivos mediante una página web PHP personalizada.

9 Impacto

- Los archivos cifrados reciben la extensión ".play" y se envía una nota de rescate con un archivo ReadMe.txt.
- Uso de AlphaVSS para borrar copias sombra, deshabilitando la restauración del sistema.

RansomHub

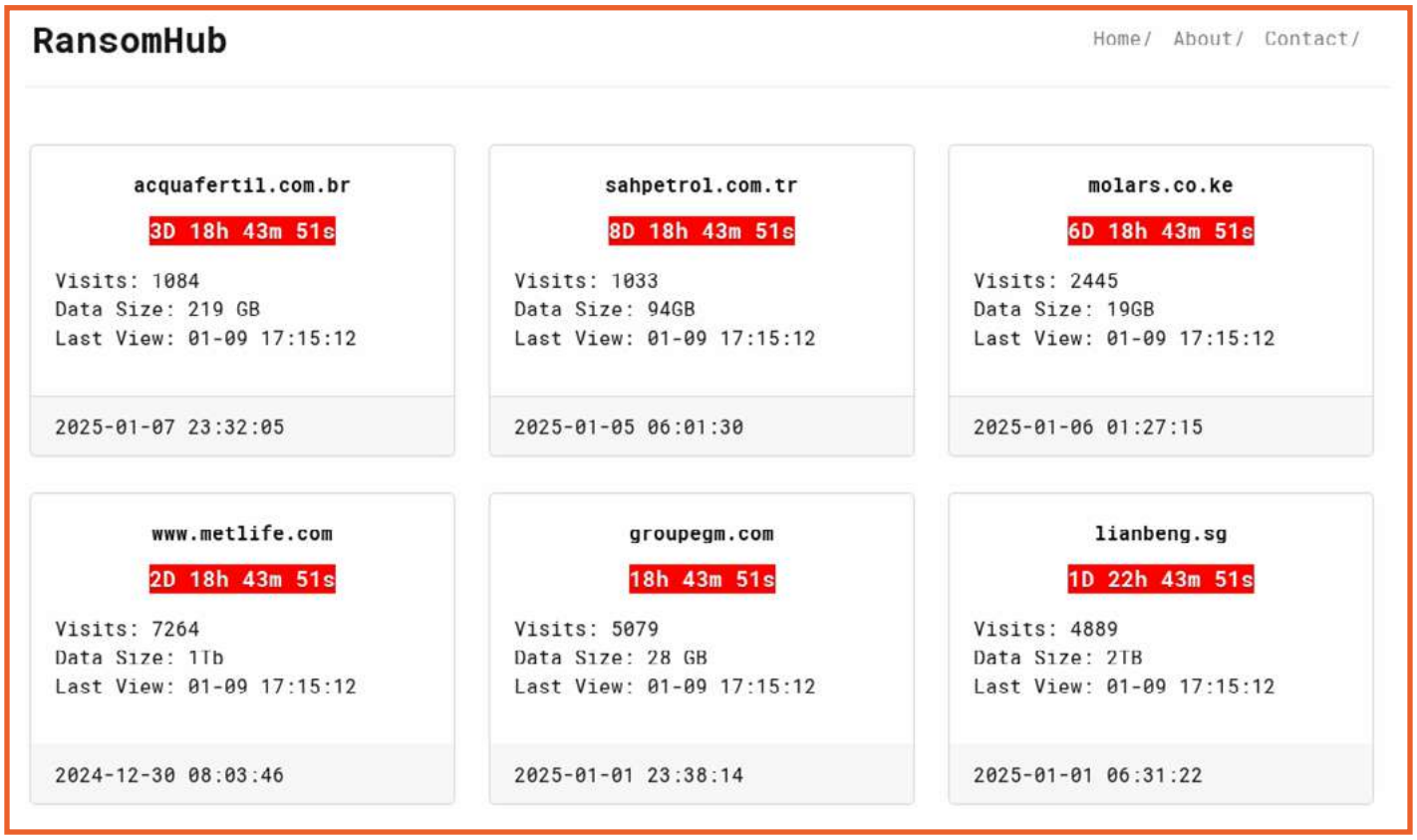
Primera detección

Método

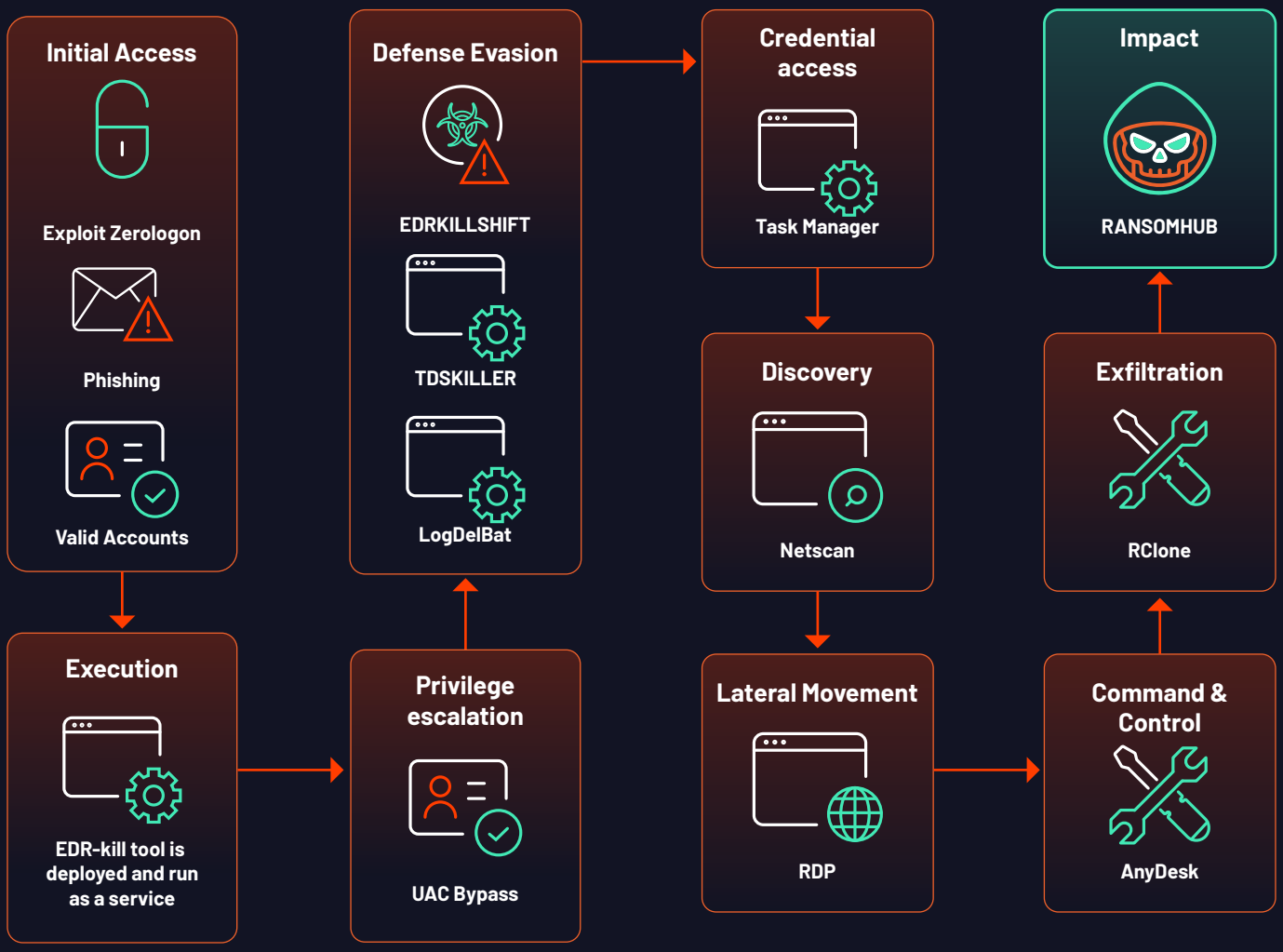
Singularidad

Este grupo de Ransomware opera a través de la doble extorsión, es decir, cifrar los sistemas de la organización e impedir que se publique la información exfiltrada en el ataque. Por otro lado, el grupo opera como RaaS, donde los afiliados se encargan del acceso inicial y realizar la entrega del Ransomware en la organización objetivo.

Son conocidos por desactivar las protecciones de EDR y antivirus de sus objetivos. Utilizan herramientas como EDRKILLSHIFTER para explotar controladores vulnerables dentro del objetivo, interrumpir los procesos de seguridad y ayudar a la evasión de detección en la cadena de ataque.



Cadena de ataque de RansomHub



Estos son los pasos en la cadena de ataque de RansomHub:

1 Acceso Inicial

- Obtienen credenciales a través de Phishing.
- Explotación de vulnerabilidades y hacen ataques tipo Password Spraying.

2 Evasión

- Utilización de lotes de archivos .bat
- Los detectados durante la investigación de Trendmicro fueron "232.bat", "tdsskiller.bat", "killdeff.bat" y "LogDel.bat".

3 Acceso a Credenciales

- Obtención de credenciales a través del proceso LSASS.
- Dump a la memoria para extraer las credenciales.

4 Descubrimiento

- Utilización de Netscan a través de entrega por buffer RDP.
- Reconocimiento de la red de la víctima.

5 Movimiento Lateral

- Windows/SMB para utilizar los recursos compartidos y ejecutar comandos.
- AnyDesk para ejecutar comandos y extraer información.

6 Exfiltración

- Ejecución del comando rclone para extraer la información de la red.
- Copia de la información y envío al servidor remoto.

7 Impacto

- Ejecución del binario con el parámetro -pass.
- Creación de la nota de rescate y cifrado de los archivos.

CLOP

Primera detección

Origen

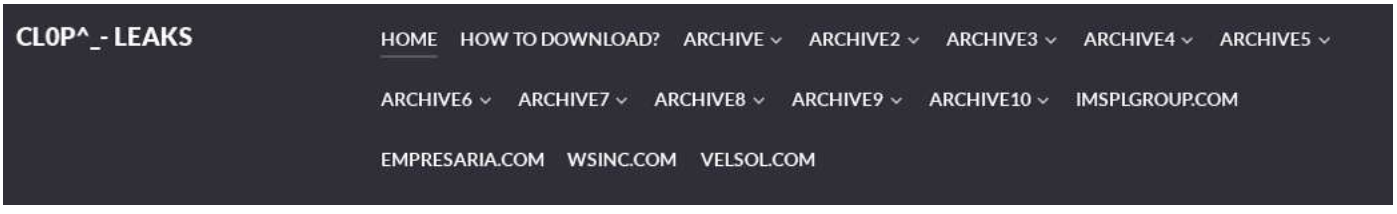
Capacidades

Se trata de una variante del Ransomware CryptoMix, que cifra los archivos de la víctima y los renombra añadiendo la extensión [.]clop.

Esta variante se entregó como la carga útil final en una campaña de Phishing en 2019, por los actores de amenazas TA505, con motivación únicamente financiera.

Es capaz de desactivar Windows Defender y eliminar Microsoft Security Essentials, lo que le permite operar de manera encubierta dentro del sistema afectado, facilitando su infiltración sin ser detectado.

Su nombre deriva de la palabra rusa “klop”, que significa insecto (bug).



Estos son los pasos en la cadena de ataque de Clop:

1 Acceso Inicial

- Campañas masivas de Phishing.
- Explotación de RDP comprometidos.
- Explotación de vulnerabilidades específicas (Zero-Day), como CVE-2021-27101, CVE-2021-27102 o CVE-2021-27103.

2 Descubrimiento

- Uso de herramientas maliciosas para recopilar información y preparar el ataque.
- Se vale de FlawedAmmyy RAT, Cobalt Strike o SDBOT RAT.

3 Movimiento Lateral, Reconocimiento y Evasión de Defensa

- Identifica si la máquina es personal o corporativa, mediante el análisis del grupo de trabajo.
- Distingue entre grupo de trabajo predeterminado y dominio del servidor AD, continuando con el ataque solo en el segundo caso.
- Utiliza herramientas como Cobalt Strike, TinyMet y SDBOT.

4 Exfiltración

- Uso de la herramienta DEWMODE para exfiltrar datos robados antes de la fase de cifrado.

5 Impacto

- Finaliza múltiples servicios y procesos de Windows.
- Realiza el cifrado de los datos en el sistema comprometido, dejando a la organización paralizada.

Akira

2023	Storm-1567, Punk Spider, GOLD SAHARA	Phishing y RDP
Primera detección	AKA	Método

Ha sido reconocido fácilmente por la extensión que agrega a los archivos que encripta " [.]akira ". Tiene operaciones recientes en Latinoamérica y Chile, siendo uno de los Ransomware actuales más preocupantes en la región.

Akira presenta un sitio web inspirado en la estética cyberpunk y su nombre se basa en el anime "Akira" de Katsuhiro Otomo. Además, el sitio incluye un mensaje para las víctimas y una lista de 5 comandos:

- **Leaks:** Para visualizar las compañías hackeadas y descargar su información.
- **News:** Apartado donde se mencionan las nuevas víctimas.
- **Contact:** Un chat para establecer negociaciones con el grupo.
- **Help:** Comando de ayuda.
- **Clear:** Limpia la pantalla de comando anterior.

Una vez dentro de la red afectada, Akira utiliza el protocolo de escritorio remoto (RDP) para moverse lateralmente dentro de la red, y PowerShell para ejecutar comandos y scripts que facilitan el despliegue del Ransomware y la extracción de datos.

Estos son los pasos en la cadena de ataque de Akira:

1 Acceso Inicial

- Utilizan mayormente credenciales robadas de conexiones vpn.
- También han utilizado el CVE-2023-20296 para acceso a productos Cisco.

2 Persistencia

- Crean cuentas de dominio (AD) en los controladores de objetivo.
- Así logran la creación o apropiación de cuentas con permisos de administrador.

3 Descubrimiento

- Utilizan herramientas como son los comandos de red del sistema operativo Windows y Advanced ip Scanner.

4 Movimiento Lateral

- Usan herramientas como Windows RDP y Anydesk para gestionar el control remoto de los equipos.
- Ocupan programas como Filezilla o Winscp para la distribución de la información de la víctima.

5 Impacto

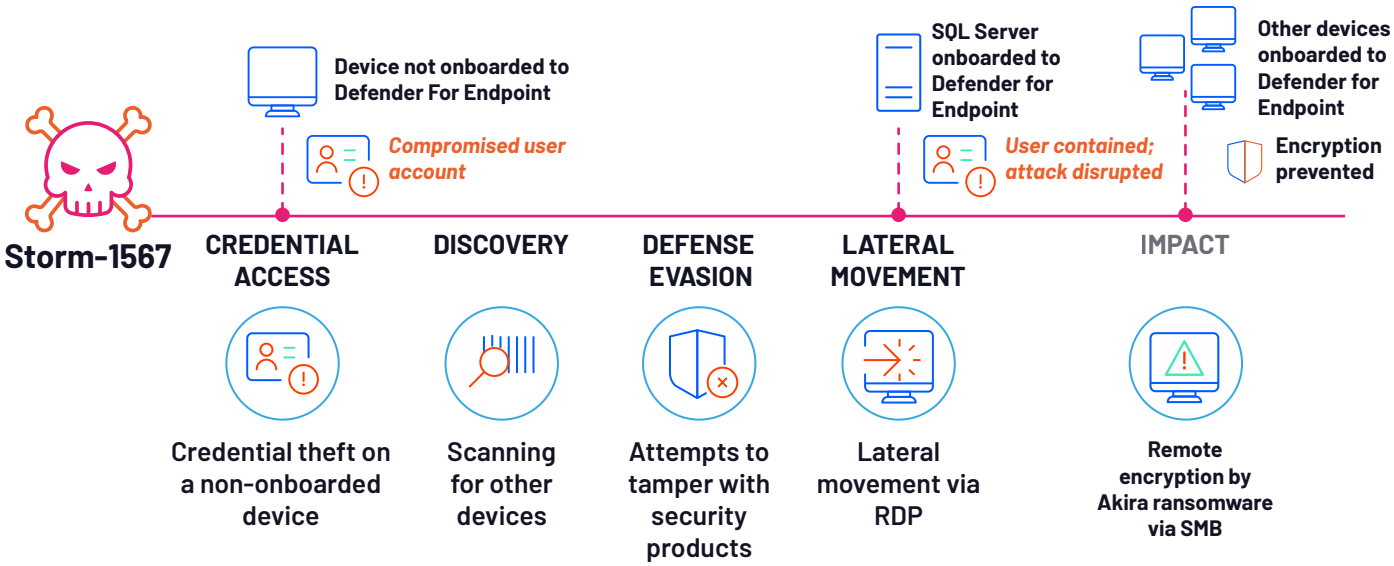
- Cifrado Chacha para la información del objetivo.
- Piden un rescate por los datos, amenazando con su filtración pública.

6 Proceso de Encriptado

- Excluyen una lista de directorios, los cuales podrían corromper el funcionamiento del sistema operativo.
- Estos son: tmp, winnt, temp, thumb, $Recycle.Bin, $RECYCLE.BIN, System Volume Information, Boot Windows y Trend Micro ProgramData.

Un caso de ataque

En la siguiente figura, podemos apreciar la cadena de ataque que realizó Akira a una empresa de ingeniería.



2.5 AMENAZAS EN CLOUD Y SaaS

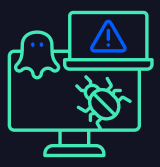
El panorama de amenazas en la nube está en constante evolución, pues los atacantes adaptan rápidamente sus técnicas para explotar las vulnerabilidades de las infraestructuras de SaaS y los entornos de nube.

Crecimiento exponencial de los incidentes de seguridad en la nube

61% de las organizaciones reportó haber experimentado incidentes de seguridad en la nube durante los últimos 12 meses. Esto representa un aumento significativo en comparación con el 24% del año anterior.

Tendencias claves en las amenazas a la nube y SaaS

Estas son las tendencias más notables de amenazas en la nube y SaaS:



1. Aprovechamiento de Vulnerabilidades

Los actores de amenazas están utilizando vulnerabilidades en los servicios de SaaS, como la vulnerabilidad de SugarCRM (CVE-2023-22952), para obtener acceso a las cuentas de la nube.

2. Ataques de Ingeniería Social

La ingeniería social sigue siendo una táctica eficaz, y los atacantes utilizan cada vez más IA para crear correos electrónicos de Phishing convincentes a gran escala.

3. Movimiento Lateral

Los atacantes pueden moverse lateralmente utilizando herramientas de administración de sistemas y explotando cuentas con privilegios excesivos.

4. Exfiltración de Datos

Los atacantes están automatizando los procesos de exfiltración de datos, lo que les permite robar grandes cantidades de información en poco tiempo.

5. Aumento de la Velocidad

El tiempo entre el compromiso inicial y la exfiltración de datos se ha reducido drásticamente, obligando a responder con mayor rapidez.

Vulnerabilidades de nube más explotadas en 2024

Las vulnerabilidades más explotadas en la nube están cambiando. Si bien las configuraciones erróneas han sido un problema importante en el pasado, el panorama actual de amenazas ha evolucionado.

Top 3 de vulnerabilidades más explotadas durante 2024:

21%

1. Brechas de seguridad de datos

Los atacantes están apuntando y explotando vulnerabilidades que les permiten acceder a datos confidenciales almacenados en la nube.

17%

2. Uso indebido de los servicios en la nube

Los atacantes están utilizando servicios legítimos en la nube para fines maliciosos, como el lanzamiento de ataques o el alojamiento de contenido infectado.

12%

3. Errores de configuración y administración

Si bien las organizaciones están mejorando en la gestión, los atacantes aún pueden encontrar y explotar errores que conducen a brechas de seguridad.

Es importante tener en cuenta que estas estadísticas solo representan los incidentes informados. Es probable que haya muchos más incidentes que no se detectan o no se informan, lo que subraya la necesidad de una mayor visibilidad y control sobre la seguridad de la nube.

Por otra parte, las amenazas de día cero, como Log4j/Log4Shell, también representan un riesgo significativo. Estas aprovechan las vulnerabilidades que son desconocidas para los desarrolladores de software, lo que las hace extremadamente difíciles de detectar y prevenir.

Para mitigar estas vulnerabilidades, las organizaciones deben adoptar un enfoque de seguridad más proactivo que priorice la prevención en lugar de la detección y respuesta.

Medidas de seguridad para la nube y SaaS

Implementar firewalls de aplicaciones web (WAF)

Con tecnología de IA para protegerse contra amenazas web sofisticadas, incluidos los exploits de día cero.

Implementar soluciones avanzadas de seguridad de red

Que escalen con la infraestructura de la nube y brinden protección integral en todas las plataformas de la nube.

Adoptar una plataforma de protección de aplicaciones nativas de la nube (CNAPP)

Que combine CSPM, CWP, CIEM, CDR y seguridad de código para una mejor automatización y eficiencia.

Aprovechar las tecnologías de IA para la prevención proactiva de amenazas

Para abordar la escasez de habilidades de ciberseguridad.

Capítulo

03.

CIBER AMENAZAS EN LATINOAMÉRICA Y EL CARIBE

Según el seguimiento de CCI Entel Digital, Chile se posicionó como el cuarto país más afectado por Ransomware en LATAM.

Reporte Ciberseguridad 2025

La amenaza de Ransomware continúa constantemente evolucionando a nivel global y regional, a la vez que nuevos actores se suman a la escena. **Esto se debe principalmente a 3 factores:**

1. Las grandes retribuciones monetarias que **es posible obtener a partir de los ataques.**
2. La reutilización de **Builders de Ransomware filtrados en internet.**
3. La generación de **nuevas cepas de Builders en internet.**

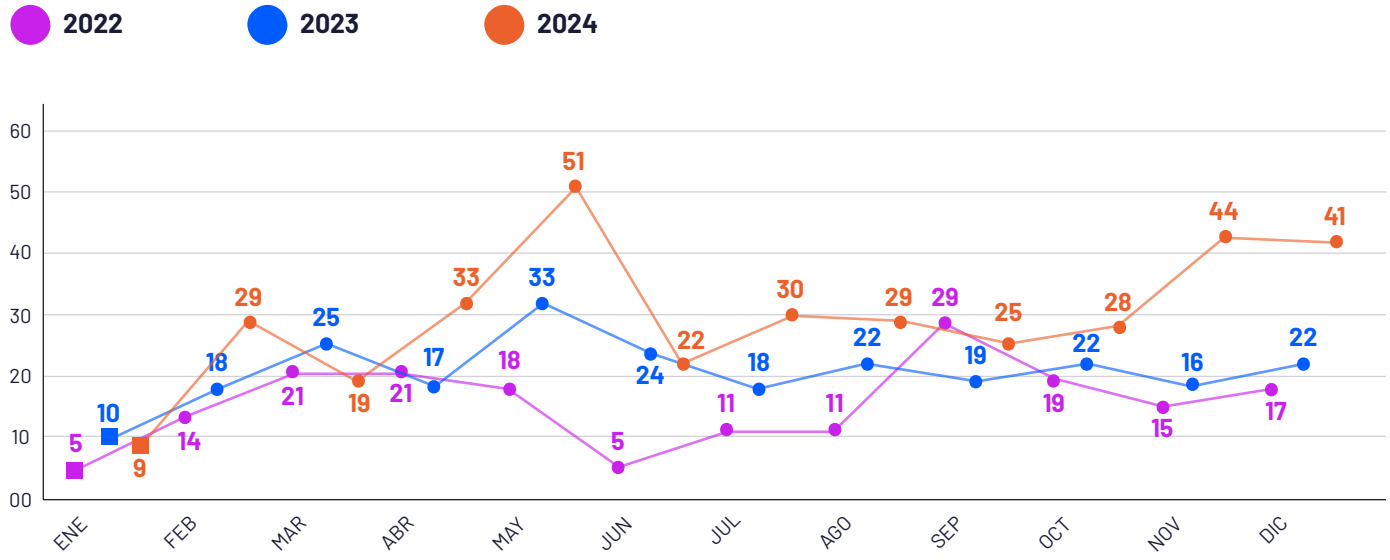
Esta evolución se manifiesta en un aumento en los ataques. De hecho, en el año 2024 se vio un total de 360 organizaciones comprometidas, lo que supera en 114 el anterior récord de actividad en 2023

> **El año 2024 superó por 114 víctimas el récord de actividad establecido en 2023.**

Actividad de Ransomware en Latinoamérica y el Caribe entre 2021 y 2024

2021	2022	2023	2024
13	186	246	360

Cantidad de ataques de Ransomware por mes en Latinoamerica y el Caribe entre 2022 y 2024



Data Breach en LATINOAMÉRICA Y EL CARIBE

Es importante mencionar que pueden existir diferencias en los números que posea cada investigador, debido a la amplitud y profundidad de cada monitoreo. Sin embargo, desde CCI, tomamos revisiones propias sumadas a otros proveedores de fuentes abiertas y cerradas, para aumentar la visibilidad de la operación e intentar reunir la mayor cantidad de datos posibles relacionados con nuestra región de enfoque.

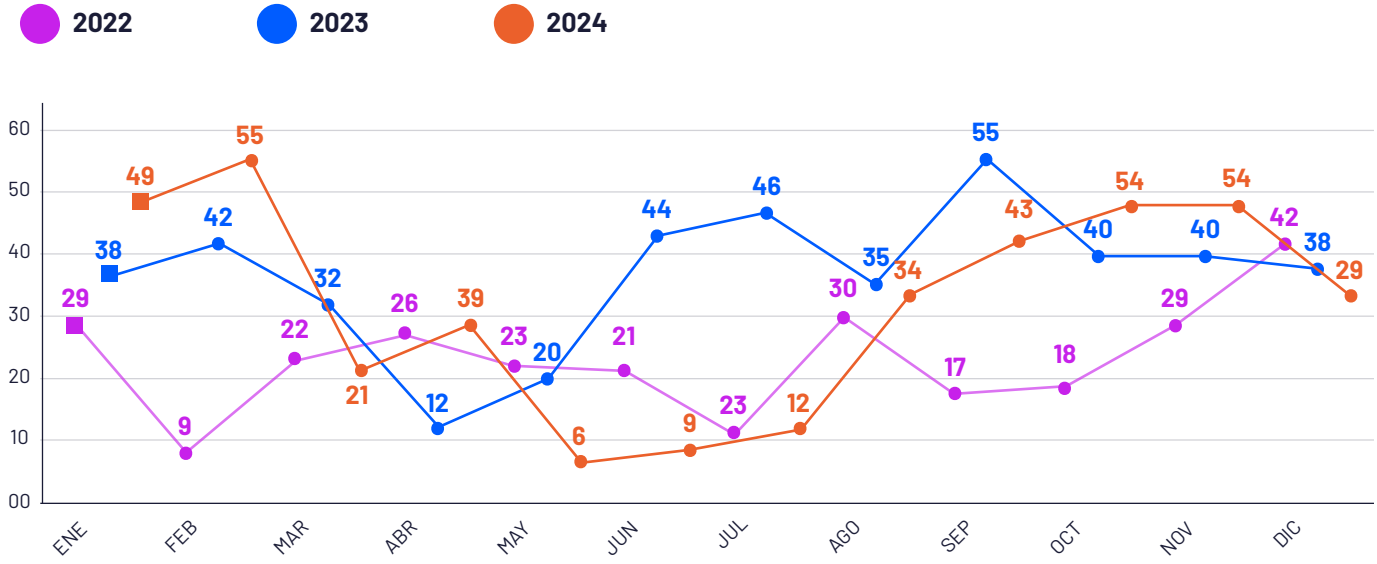
Las actividades de Data Breach y Data Leaks, aunque no se han detenido, sí han disminuido en la región durante el 2024, sin una razón particular. Sin embargo, a medida que la digitalización y el manejo de grandes volúmenes de datos continúen expandiéndose, aumentará el riesgo de que estos incidentes vuelvan a crecer, tanto en frecuencia como en intensidad.

> **A medida que la digitalización avance, el riesgo de incidentes de Data Breach seguirá creciendo.**

Actividad de Data Breach en Latinoamérica y el Caribe entre 2021 y 2024

2021	2022	2023	2024
178	289	442	405

Cantidad de ataques de Data Breach por mes en Latinoamerica y el Caribe entre 2022 y 2024



Principales actores en LATINOAMÉRICA Y EL CARIBE

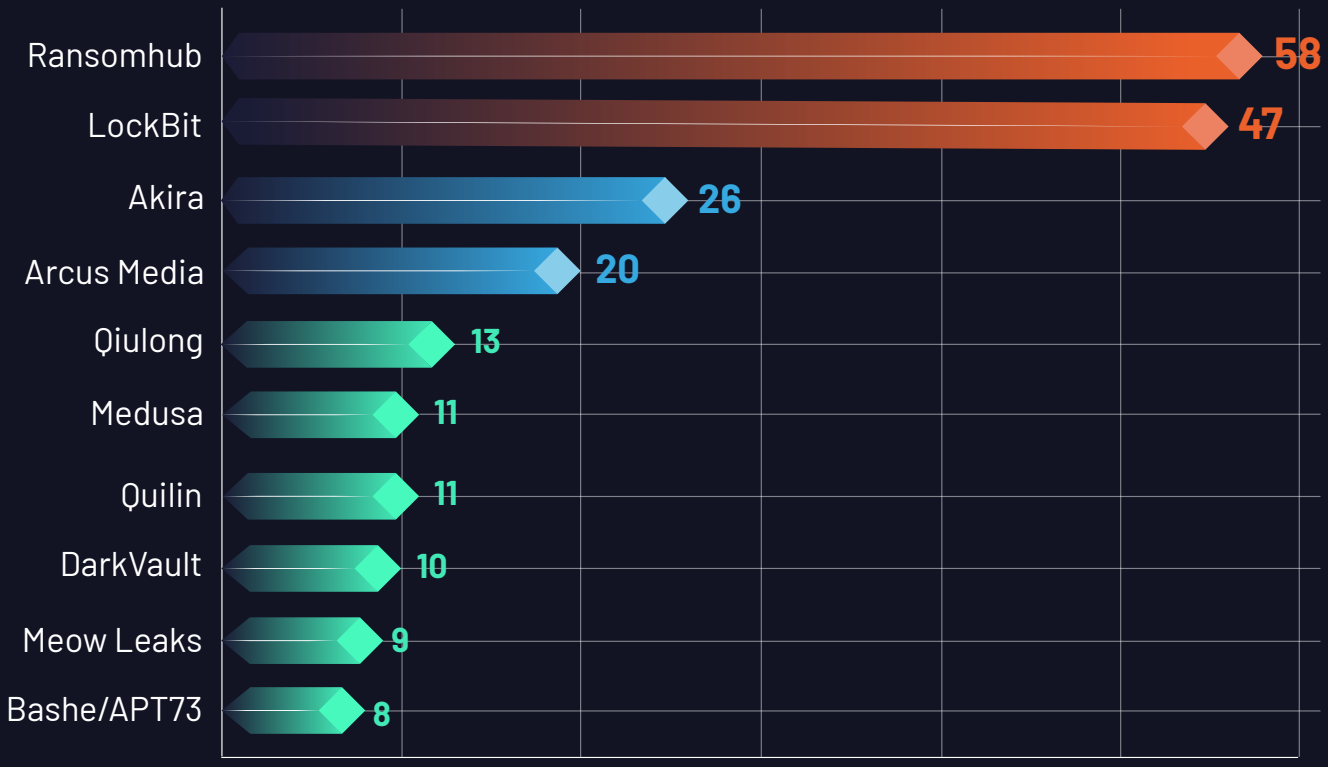
Cabe destacar que no todos los actores continúan sus operaciones indefinidamente. Muchos cumplen ciertos objetivos monetarios para posteriormente cambiar de nombre o darse de baja, evitando persecuciones y seguimiento de fuerzas de orden.

Actores de Ransomware

Grupos como Ransomhub, LockBit y Akira han tenido actividad creciente en el entorno latinoamericano. Aunque sus ataques no se limitan únicamente a una región, existen algunos factores que hacen del continente un sector atractivo:

- **Falta de recursos y cultura de ciberseguridad.**
- **La presencia de algunos países activos económicamente.**
- **La tramitación tardía de legislaciones de ciberseguridad.**

Actores de Ransomware con mayor presencia en Latinoamerica y el Caribe durante 2024



> **La falta de recursos y cultura de ciberseguridad hacen de Latinoamérica y el Caribe un terreno atractivo para los actores de Ransomware.**

Este es el TOP 3 de actores de Ransomware más activos en la región

Ransomhub

Origen: Desconocido

544 Víctimas Globales

2021 Año de surgimiento

Singularidades

- Ofrece un informe de pentesting en el que se detallan las vulnerabilidades explotadas.
- Promete borrar de sus servidores para siempre los datos tras el rescate.
- Los métodos de exfiltración de datos dependen de la filial que lleve a cabo el ataque.
- La nota de rescate proporciona a las víctimas un ID de cliente y les indica que se pongan en contacto con una URL [.]onion única.

LockBit

Origen: Rusia

2933 Víctimas Globales

2019 Año de surgimiento

Singularidades

- Mayor actividad histórica, superando con creces al anterior líder Conti [Offline].
- FBI ha intentado desbaratarlo, pero solo han capturado una parte (cerca de 7000 claves de descifrado).
- FBI ofrece en total 15 M USD (10+5) en recompensas por antecedentes.
- Si bien disminuyó su actividad tras ese incidente, sigue activo y en pie.

Akira

Origen: Desconocido

415 Víctimas Globales

2023 Año de surgimiento

Singularidades

- Amplia gama de objetivos, con preferencia a industria tecnológica y banca.
- Constante actualización de la herramienta y alto nivel de sofisticación de operaciones.
- Pasaron de utilizar herramientas de terceros a desarrollar su propia variante.
- Capaz de infectar múltiples sistemas operativos, desplegando ataques específicos.

Actores de Data Breach

Hay una constante renovación en el mundo de los actores de Data Breach, ya que muchos de los Alias son desechables, parte de SecOps o de campañas específicas de corta duración. Solo una pequeña minoría de usuarios se repite y estos suelen contar con gran reputación en línea y en portales DDW.

Igualmente, no todos los leaks se hacen públicos, debido a compartimentaje interno entre actores específicos o mediante canales cerrados. Sin embargo, la forma en que se libera o se hace conocer va a depender netamente de las motivaciones del actor.

Motivaciones de Data Breach:

Top Actores de Data Leak en Latinoamérica y el Caribe durante 2024

Prapra123

Surgimiento: octubre 2023

Motivación: reputacional y financiera

Características

- Mantiene actividad fuera de Latinoamérica, pero su foco está en Argentina, Perú y Ecuador.
- Objetivos relacionados a entidades públicas, gubernamentales y educativas.
- Cuenta con gran reputación en foros de mercado negro.
- No registra nueva actividad desde marzo de 2024.

InjectionInferno

Surgimiento: mayo 2024

Motivación: reputacional y financiera

Características

- Grandes capacidades y leaks de todo el mundo, principalmente de Latinoamérica y el Caribe.
- Se especializa en obtención de información personal para ofrecer como Leads para ventas y Marketing.
- Se perfila como un usuario único y no como un grupo.
- Cuenta con gran reputación en foros de mercado negro.

CiberinteligenciaSV

Surgimiento: abril 2024

Motivación: hacktivismo y daño reputacional

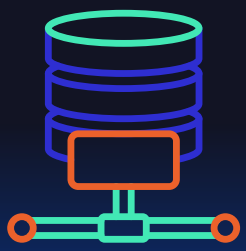
Características

- Libera información de El Salvador, bajo la premisa de liberar información de actos de corrupción por parte de su presidente y organizaciones públicas.
- Actividad en su canal de Telegram, originalmente llamado "Guacamaya", muy probablemente relacionado con ataques hacktivistas del grupo Guacamaya (2022).
- Es altamente probable que este perfil corresponda a un grupo de actores y no a un solo usuario.
- Cuenta con gran reputación en foros de mercado negro.

Sectores y países afectados en Latinoamérica y el Caribe

Sectores y países afectados por Ransomware

Los grupos de Ransomware comparten un gran interés por organizaciones de Banca y Finanzas, debido a la alta retribución económica que pueden obtener. Sin embargo, la industria Tecnológica permanece como la más codiciada, por factores como:



Alta cantidad de infraestructura susceptible a ser comprometida.

Muchas de estas empresas son proveedores de servicios.

Por esto, pueden impactar a cientos de personas y organizaciones con un solo ataque y poner en riesgo su percepción social, ejerciendo mayor presión a las víctimas para pagar el rescate.

Los actores de Ransomware estudian a sus víctimas, de forma que el cobro de rescate, a pesar de ser alto, resulte más económico que el impacto de la indisponibilidad de servicios y la vulneración de datos sensibles.

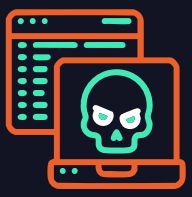
A la vez, el TOP 3 de actores ha enfocado su actividad en Banca y Finanzas e Infraestructura tecnológica, coincidiendo completamente con la mirada histórica.

Akira

Top países

Top 3 industrias

- **8** Infraestructura tecnológica
- **5** Banca y finanzas
- **3** Transporte



LockBit

- **9** Banca y finanzas
- **5** Transporte
- **4** Agricultura/ Entretenimiento/ Manufactura/ Infraestructura tecnológica/ Servicios de salud

Ransomhub

- **9** Banca y finanzas
- **7** Servicios de salud
- **5** Agricultura consumo/ Servicios legales

Al considerar el total de los ataques de Ransomware en 2024, Brasil, México y Argentina se mantienen como los países más afectados, mientras Chile se ubica en el 4° lugar.

Brasil se mantiene como el más afectado, mientras que casos como Argentina han bajado su incidencia tras condiciones económicas desfavorables. En ese sentido, el atractivo para el cibercrimen podría estar relacionado a factores como:

- El volumen de infraestructura tecnológica
- La densidad poblacional
- La prosperidad económica

Muchas veces estos ataques tienen repercusiones directas para los ciudadanos en su día a día, generando indisponibilidades de acceso a internet o de trámites de gran relevancia, en:

- Entidades públicas
- Entidades privadas

Sectores y países afectados por Data Breach

Entre el TOP 3 de actores más prolíficos en Data Breach, los sectores que más frecuentemente han sufrido ataques o filtraciones son:

- Gobierno
- Banca y finanzas
- Educación

De entre la gran cantidad de datos que se extrae de estas organizaciones, los que generan mayor valor e interés en los mercados negros son los relacionados con información personal de clientes o colaboradores, como:

- Identificación
- Número de teléfono
- Correo corporativo
- Contraseñas

> **Esto sirve para generar listados de perfilamiento de usuarios y ataques direccionados a usuarios VIP y VAP.**

Estos son los sectores más afectados por el TOP 3 de actores de Data Breach:

prapra123

Top países

24 Argentina

2 Perú

1 Ecuador

Top 3 industrias

- 13 Gobierno
- 6 Educación/ Seguros
- 2 Servicios Legales

Injectioninferno

7 Argentina

4 Brasil

4 Perú

- 10 Banca y finanzas
- 3 Telecomunicación
- 2 Gobierno

CiberinteligenciaSV

11 El Salvador

1 Brasil

1 México

- 8 Gobierno
- 2 Banca y finanzas
- 1 Telecomunicación/ Defensa y orden público/ Transporte / Servicios de Salud

Similar al caso del Ransomware, Argentina, Brasil y México se posicionaron como los países más afectados por Data Breach en la región durante 2024, mientras que **Chile quedó en el 7 lugar.**

Top 10 países más afectados por DataBreach en Latam y el Caribe en 2024

Nuevamente, los países afectados suelen ser principalmente los más activos económicamente, lo cual representa dos principales atractivos:

1. Mayores retribuciones económicas para los atacantes.
2. Despliegue de infraestructura con grandes capacidades.

A nivel regional, las industrias que más han sufrido estos incidentes son:

- **Telecomunicaciones.**
- **Tecnología.**
- **Transporte.**
- **Gobierno.**
- **Seguros.**
- **Banca y finanzas.**

Cabe destacar que los Data Leak más grandes corresponden a filtraciones ocurridas mediante Ransomware, aunque sus motivación varían y no son catalogables dentro del mismo origen.

digital

Capítulo

04.

EVOLUCIÓN DE LAS TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTP´s)

La popularización de los modelos de IA ha precipitado la creación de nuevas TTP's, entre las que se destacan el compromiso de la cadena de suministro de ML y la evasión del modelo de ML.

> **MITRE ATT&CK es uno de los principales marcos de referencia globales respecto a inteligencia de amenazas y operaciones de ciberseguridad**

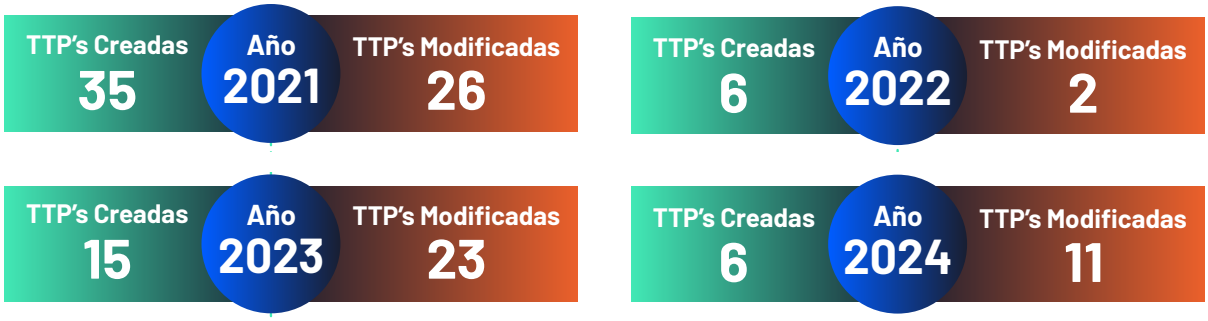
Uso de IA y automatización en ciberataques

Desde su creación, la cantidad de tácticas, técnicas y procedimientos ha experimentado numerosos cambios. Sin embargo, no fue hasta mediados del 2021 que la matriz Mitre publicó nuevas TTP's, a partir de la creciente adopción de modelos de IA en la mayoría de los procesos y actividades.

Por corresponder a una tecnología emergente, las nuevas TTP´s no fueron agregadas en la matriz ya existente, sino que se creó una bifurcación de la matriz especialmente orientada a ellas: Mitre ATLAS, mencionada en nuestro panorama de Inteligencia Artificial.

Tomando como referencia la Mitre ATLAS, se describe la evolución de las TTP's, considerando la bifurcación ocasionada por la creciente integración de los modelos de IA en procesos y operaciones cotidianas.

Este el número de TTP's creadas y modificadas por cada año.



TTP's que representan el mayor número de casos asociados al abuso de modelos de IA.

Top 10 Técnicas

1. **Compromiso de la cadena de suministro de ML** (ML Supply Chain Compromise)
2. **Evadir el modelo de ML** (Evade ML Model)
3. **Elaborar datos contradictorios** (Craft Adversarial Data)
4. **Daños externos** (External Harms)
5. **Búsqueda de material de investigación de las víctimas a disposición del público** (Search for Victim's Publicly Available Research Materials)
6. **Verificación del ataque** (Verify Attack)
7. **Producto o servicio basado en ML** (ML-Enabled Product or Service)
8. **Acceso a la API de inferencia de modelos de IA** (AI Model Inference API Access)
9. **Erosionar la integridad del modelo de ML** (Erode ML Model Integrity)
10. **Inyección rápida de LLM** (LLM Prompt Injection)

> **Una de las técnicas más relevantes y con mayor número de casos de uso registrados hasta la publicación de este informe es el "Compromiso de la cadena de suministro de ML".**

Esta técnica, junto con aquellas que explotan o abusan de los ecosistemas de desarrollo vinculados a los modelos de IA y aprendizaje automático, son especialmente atractivas para los actores de amenaza, porque:

- Los vectores de ataque permiten aprovechar la confianza depositada en los proveedores del ecosistema de software basado en IA y ML legítimos.
- Se puede reducir las probabilidades de detección, logrando un mayor alcance, además de una expansión significativa de la superficie de ataque.

Caso de uso

Víctima:
Hugging Face

Fecha:
Marzo 2024

La popular plataforma de ecosistemas IA/ML "Hugging Face" registró entre sus repositorios por lo menos 100 modelos de IA/ML maliciosos. Estos afectaron directamente a la librería de serialización Pickle de Python, con un formato predeterminado para compartir datos de manera eficiente entre partes con PyTorch.

Al importar los módulos asociados a la librería, Pickle permitía a los actores de amenaza:

- Ejecutar código arbitrario a través de la incorporación de funciones integradas como eval o exec.
- Llamar al constructor al crear instancias de objetos para insertar código arbitrario.

Una gran cantidad de usuarios del ecosistema de IA/ML de Hugging Face resultaron afectados, con puertas traseras que permitirían a los atacantes obtener control total de sus máquinas. Por lo tanto, **Hugging Face tuvo que implementar mecanismos de protección a este tipo de vulnerabilidades de los archivos de serialización.**

Los actores de amenazas siguen mejorando sus TTP's para sumar otras librerías asociadas al ecosistema de IA/ML, como parte del vector de ataque de la cadena de suministros del software. Estas librerías se asocian a las siguientes extensiones de archivos IA/ML:

- .keras
- .mar
- .pb
- .pth
- .bin
- .npy
- .pt
- .h5
- .pt2
- .ckpt
- .tflite
- .safetensors
- .npz
- .onnx

Todas estas son extensiones de archivos usados en contextos específicos de aprendizaje automático, que facilitan el almacenamiento, intercambio o despliegue de modelos y datos relacionados. Lo anterior implica que la cadena de suministro del software es y seguirá siendo un vector relevante y prevalente dentro de las TTP's de los actores de amenaza para el 2025.

Esto resulta especialmente cierto para la cadena de suministro de software libre, en donde el foco está orientado especialmente a los marcos de desarrollo PyTorch y Tensorflow:

95% **De los modelos maliciosos en Hugging Face corresponde a Pytorch**

5% **De los modelos maliciosos en Hugging face corresponde a Tensorflow**

Códigos maliciosos ocultos en modelos IA/ML

Para ocultar código malicioso en modelos IA/ML, los actores de amenaza se valen de la serialización.

- **Serialización**

  La traducción de un modelo de IA/ML a un formato de flujo de bytes que se pueda usar para el almacenamiento, la transmisión y la carga.

A partir de este proceso, los actores de amenaza pueden:

1. Usar la manipulación de los valores de coma flotante de 32 bits de la serialización.
2. Reemplazar los bits menos significativos de la mantisa por datos arbitrarios.
3. Sobreescribir los bits menos significativos de la mantisa para coincidir con el peso dado.
4. Hacer que el modelo funcione con normalidad.

Por ser el formato de pickling una forma de serialización extensiva en la mayoría de modelos ML, los atacantes abusan de esta característica para insertar troyanos activos y efectuar ataques de envenenamiento de pesos en los tensores de los modelos.

La serialización es un procedimiento común que se puede aplicar a todo tipo de estructuras y objetos de datos, utilizando formatos como:

- **CSV**
- **JSON**
- **XML**
- **Google Protobuf**

Aunque algunos de estos se pueden usar para almacenar modelos de ML, existen muchos formatos específicos que pueden ser abusados por los actores de amenaza en sus operaciones maliciosas.

Aunque algunos de estos se pueden usar para almacenar modelos de ML, existen muchos formatos específicos que pueden ser abusados por los actores de amenaza en sus operaciones maliciosas.

Framework con RCE	Formato
PyTorch, Pandas, scikit-learn	Pickle - dill
PyTorch	TorchScript
Python-based frameworks	Numpy
Keras	H5
-	ONNX
PyTorch, scikit-learn	Joblib
TensorFlow	TensorFlow TFLite/FlatBuffers
H2O	POJO - MOJO

Framework sin RCE	Formato
Python-based frameworks	SafeTensors
TensorFlow	SavedModel
Flax	MsgPack
Spark	Arrow
-	PMML
-	JSON

> **El 62.5% de los Frameworks puede ser abusado por actores de amenaza para la ejecución remota de código.**

Vulnerabilidades registradas en base de datos públicas asociadas al ecosistema de IA/ML 2023 al 2024

Por otra parte, hemos rastreado un promedio de 255 vulnerabilidades asociadas al ecosistema IA/ML, entre finales de septiembre del año 2023 y principios de noviembre de 2024.

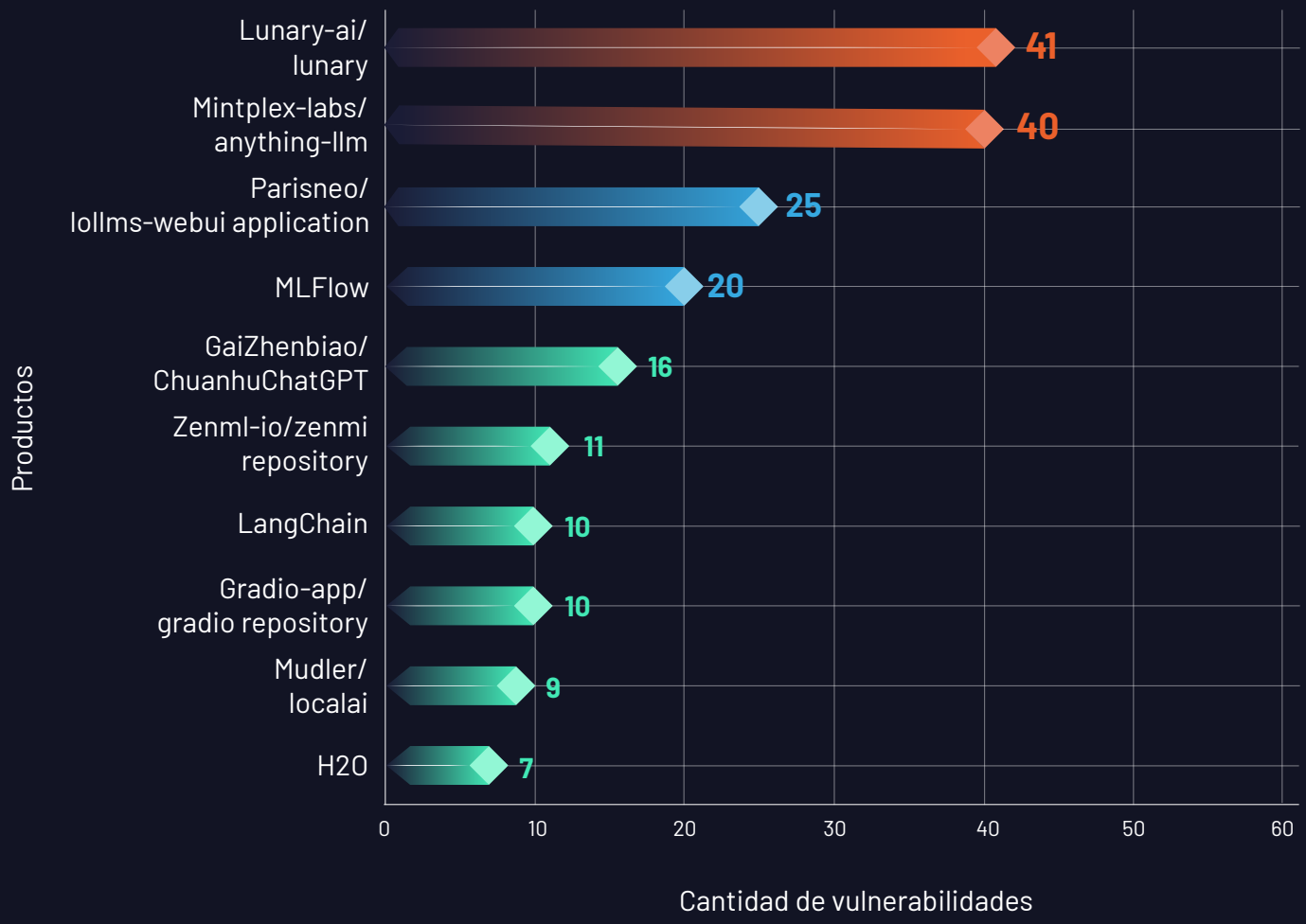
71	114	61	9
Vulnerabilidades: **severidad crítica**	Vulnerabilidades: **severidad alta**	Vulnerabilidades: **severidad media**	Vulnerabilidades: **severidad baja**

Productos de ecosistemas IA/ML más afectados con vulnerabilidades en el 2023 - 2024

De entre las 255 vulnerabilidades observadas en el periodo:

16%	15,7%	9,8%	6%
Corresponde a Lunary-ai/lunary	Corresponde a Mintplex-labs/ anything-llm	Corresponde a Parisneo/ lollms-webui application	Corresponde a MLFlow

El resto de las vulnerabilidades corresponde a otros productos del ecosistema de IA/ML:



Actores de amenaza afiliados al estado y el uso de la IA

Entre los actores de amenaza más prolíficos en dirigir recursos y capacidades en talento humano para desarrollar y optimizar el uso de tecnologías emergentes son sin dudas las Amenazas Persistentes Avanzadas (APT), sin embargo, ¿hasta qué punto son capaces de llegar?, Desde nuestra perspectiva, no hay límite, ya que los recursos son abundantes y los resultados a perseguir son tan lucrativos y beneficiosos para los gobiernos afiliados.

De hecho, existen al menos cinco APT descubiertas usando uno de los modelos de IA más populares hasta el momento. Hablamos de ChatGPT de OpenAI, que, a principios de febrero de 2024, dio a conocer a la comunidad de usuarios, a través de su sitio web, los actores de amenaza que están haciendo uso de sus plataformas para sus operaciones maliciosas.

APTs que han utilizado ChatGPT para sus operaciones:

APT Charcoal Typhoon

Afiliación: China

Uso

- Obtención de información de empresas.
- Depuración de códigos y generación de scripts.
- Creación de contenido para campañas de Phishing.

APT Salmon Typhoon

Afiliación: China

Uso

- Traducción de documentos técnicos.
- Recuperación de información de agencias de inteligencia.
- Recolección de información de actores regionales.
- Generación de scripts.

APT Crimson Sandstorm

Afiliación: Irán

Uso

- Desarrollo de aplicaciones y sitios web.
- Generación de contenido para Phishing.
- Obtención de formas comunes de evadir detecciones.

APT Forest Blizzard

Afiliación: China

Uso

- Investigación de código abierto sobre protocolos de comunicación satelital.
- Investigación de tecnologías de imágenes de radar.
- Tareas de scripting.

APT Emerald Sleet

Afiliación: Corea del norte

Uso

- Identificación de expertos y organizaciones centradas en defensa de la región Asia-Pacífico.
- Comprensión de vulnerabilidades disponibles públicamente.
- Generación de scripts y contenido para Phishing.

Para qué usan la plataforma las APTs descubiertas por OpenAI

100%	80%	60%	40%	20%
Generación de scripts	Contenido para Phishing	Investigación (código abierto e investigación de vulnerabilidades)	Traducción técnica o recopilación de datos	Evasión de detección

> **100% de las APTs descubiertas utilizan ChatGPT para automatizar las operaciones de scripting.**

Automatización de ataques con el uso de IA

No solo las ATPs organizadas emplean IA para sus ataques, cualquier actor malicioso puede:

- Acceder a diversas herramientas a través de foros clandestinos y sitios malintencionados.
- Descargar modelos Open Source preentrenados de IA/ML disponible públicamente para abusar de ellos.

Este riesgo se ve amplificado por la rápida y generalizada adopción de modelos de IA, tanto en organizaciones como en un amplio espectro de la actividad humana.

Las aplicaciones de la automatización de operaciones maliciosas con IA pueden dividirse en 4 grandes grupos:

1. **Ingeniería social**
2. **Generación de código malicioso**
3. **Ataques coordinados**
4. **Ataque o manipulación de modelos IA/ML**

Cada uno de estos tiene sus propias características.

1 Ingeniería social

Esta estrategia explota la manipulación psicológica y emocional de las personas para obtener información, acceso o beneficios ilícitos. Suele configurarse como un vector de ataque inicial debido a su naturaleza estratégica: es más sencillo superar las restricciones de una persona (a menudo el eslabón más débil en la cadena de seguridad) que superar las restricciones y protecciones implementadas en los sistemas de una organización.

En entornos IA, abarca ámbitos como:

Recopilación y procesamiento de datos masivos de las víctimas (Doxing):

- Análisis masivo de datos públicos y redes sociales
- Detección de patrones específicos sobre las víctimas
- Generación de campañas de ataque altamente dirigidas

Phishing y Spear Phishing a gran escala:

- Generación de correos electrónicos, mensajes o publicaciones
- Diseño de textos más persuasivos y personalizados de forma masiva
- Aumento en las probabilidades de éxito en este tipo de ataques

Fraude:

- Generación de identidades falsas con manipulación de imágenes, video, voz y texto
- Réplica de comportamiento, aspecto o voz, para lograr mayor persuasión

Puede desplegarse desde:

- **Chatbots maliciosos**
  Interactuar con víctimas en tiempo real
- **Perfiles falsos**
  Fotos de perfil IA realistas que parecen legítimas
- **Deepfakes y humanos sintéticos**
  Extorsión y manipulación de la opinión pública
- **Identidades falsas**
  Imágenes realistas para manipular o extorsionar víctimas
- **Falsificación de documentos**
  Documentos de identidad para suplantación
- **Clonación de la voz**
  Sintetizar voces falsas de alta fidelidad
- **Anuncios Falsos**
  Identificar objetivos y ajustar el contenido
- **Astroturfing a gran escala**
  Bots y publicaciones masivas que apoyen ideas y movimientos sociales o políticos
- **Fake news multilingües**
  Generación masiva de noticias falsas en distintos idiomas

2 Generación de código malicioso

Un actor malicioso puede entrenar un modelo para generar código malicioso de forma automatizada en tiempos más reducidos y orientado a cualquier arquitectura, que sea adaptativo a explotar vulnerabilidades específicas de los sistemas.

Esto puede incluso extenderse a otros escenarios:

Ofuscación automática:

- Dificulta la identificación del Malware por parte de los analistas
- Ofuscación automatizada de acuerdo a las herramientas de detección

Generación de Malware polimórfico y metamórfico:

- Efectuar modificaciones del código o la firma del Malware en tiempo récord
- Modificaciones cada vez que se ejecuta o distribuye
- No altera su funcionalidad u objetivo

Integración de aprendizaje automático:

- Identificar entornos desfavorables para su ejecución como honeypots o sandboxs
- Adaptar su comportamiento para pasar desapercibido hasta detectar sistemas reales
- Evita desencadenar alertas de sistemas de monitoreo basados en comportamiento

Exploits automáticos:

- Identificar las vulnerabilidades del sistema huésped
- Desplegar exploits adaptados a las vulnerabilidades
- Mejorar la velocidad y efectividad de sus ataques

Ransomware inteligente:

- Identifica los datos críticos de un sistema y prioriza su encriptación
- Maximiza el impacto del ataque a los datos críticos
- Cálculos automáticos del rescate basado en el análisis

Malware-as-a-Service (MaaS):

- Generar plataformas de servicios maliciosos con kits personalizados
- Personalizar Malware para expandir su alcance de forma exponencial
- Facilita el acceso a los actores de amenaza menos experimentados

3 Ataques coordinados

Los ataques coordinados con el uso de IA pueden adquirir nuevas proporciones, permitiendo a los actores de amenaza:

Campañas coordinadas:

- Coordinar bots, deepfakes y contenido falso en campañas sincronizadas
- Conseguir impacto simultáneo en diferentes plataformas
- Optimizar tiempos de propagación en momentos clave

4 Manipulación de modelos IA/ML

Los actores de amenazas pueden desarrollar sus propios modelos ofensivos, a partir de modelos pre entrenados Open Source. Estos son descargados en repositorios públicos y adaptados a sus necesidades, optimizando ataques automatizados a otros modelos de IA/LM.

Ya existen herramientas para éste propósito como:

- WolfGPT
- DarkBARD
- FraudGPT
- WormGPT

Sirven de apoyo para automatizar operaciones maliciosas, sobre todo en contra de modelos licenciados como ChatGPT de OpenAI. Sin embargo, esto podría igualmente ser adaptado o replicado para comprometer otros modelos, como:

- Gemini
- Claude
- Llama

Según los datos obtenidos durante nuestra investigación, este es su flujo inicial de ataque:

Entorno Open Source:

- **Acceso inicial**
  Obtenido a través del abuso de las plataformas o Frameworks usados para el desarrollo, entrenamiento, colaboración y despliegue del ecosistema IA/ML.
- **Intervención por etapa**
  Cada etapa asociada a la puesta en marcha de un modelo de IA es susceptible a ser intervenida por los actores de amenaza, a través de sus distintas TTP's.
- **TTP's**
  Robo de credenciales, creación y manipulación de librerías, inserción de código malicioso en partes específicas de los modelos.

Entornos de IA/ML licenciados:

- **Credenciales de acceso**
  Para lograr las credenciales emplean stealers específicamente diseñados.
- **Stealers**
  Entre junio 2022 y mayo 2023, al menos 101.134 dispositivos han sido infectados con stealers dirigidos a obtener credenciales de ChatGPT.

Medidas a considerar sobre el uso de los modelos de IA/ML

La autenticación de doble factor es una de las medidas de protección más efectivas asociadas a los modelos de IA/ML. Esto agrega una capa adicional de seguridad a las plataformas, reduciendo su utilidad para los stealers.

Ya que los stealers siguen siendo uno de los métodos más usados por los actores de amenaza para conseguir acceso inicial, es importante tomar medidas para protegerse de enlaces maliciosos, correos o descargas en sitios poco confiables.

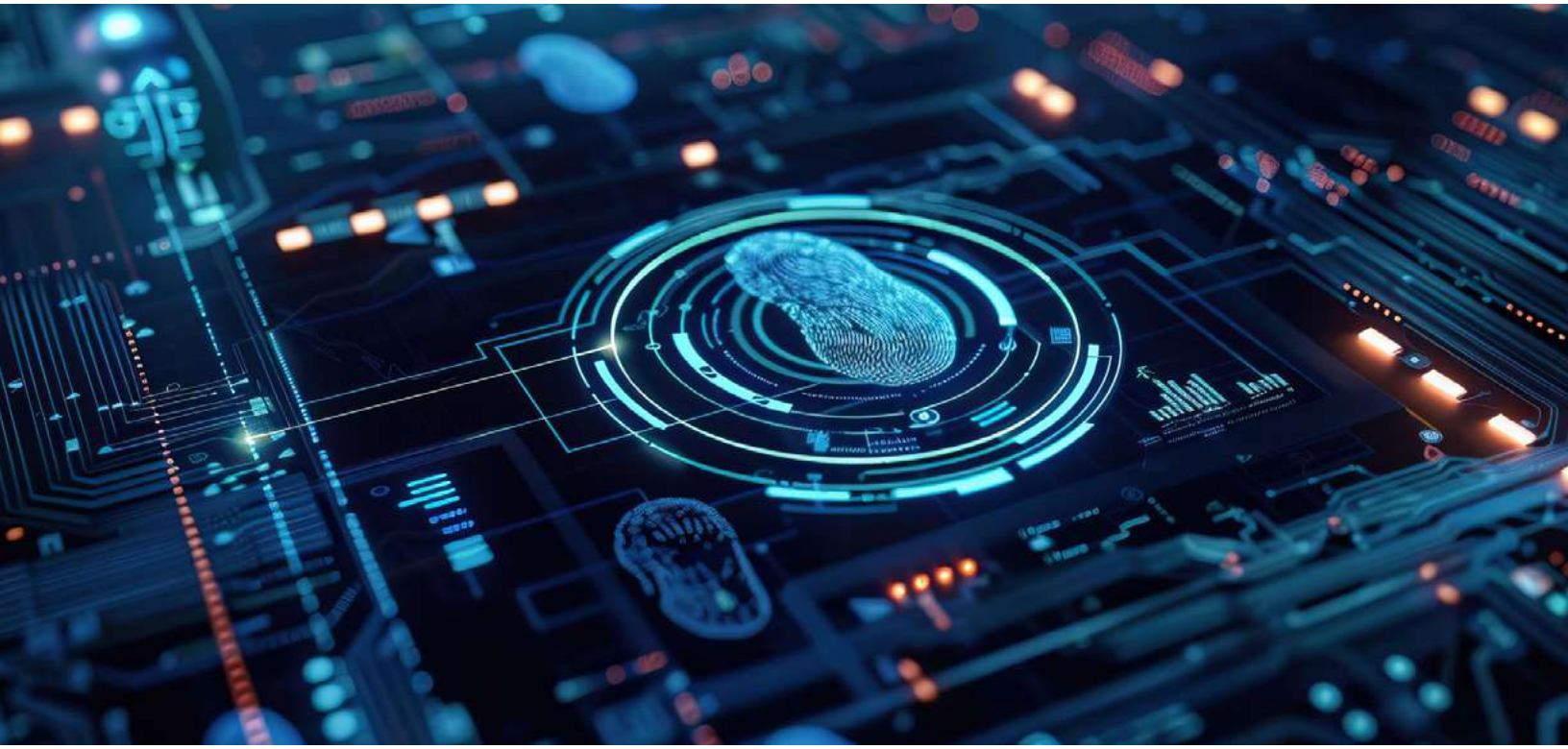
Por otro lado, para el uso responsable y seguro del ecosistema de IA/ML, estas son algunas medidas valiosas:

Medidas para entornos Open Source

- **Sitios confiables**
  Si desea descargar modelos de IA/ML preentrenados Open Source, procure hacerlo desde sitios confiables.
- **Prueba de modelos en entornos aislados**
  Evalúe el código en busca de conexiones sospechosas o redes con código ofuscado.
- **Control de versiones**
  Procure entornos de desarrollo que utilicen control de versiones y evaluación de vulnerabilidades conocidas.
- **Verificar vulnerabilidades**
  Procure usar herramientas como pip-audit o npm-audit para verificar vulnerabilidades.
- **Protección de datos confidenciales**
  Use las mejores prácticas de seguridad para proteger los accesos (tokens, APIs) de los modelos.
- **Examinar pesos del modelo**
  Revise en busca de datos codificados o comportamientos anómalos, con herramientas como TensorBoard.
- **Limitar los accesos**
  Limite el acceso en entornos de desarrollo del ecosistema IA/ML.
- **Validación de modelo**
  Compruebe el modelo y asegure su integridad con firmas digitales, utilizando ModelDB, MosaicML o Google Cloud AI Model Verification.

Medidas para entornos licenciados

- **No guardar historial**
  Es recomendable no guardar el historial de las conversaciones del modelo, pues la información puede revelar datos interesantes.
- **Resguardar acceso**
  Resguarde el acceso a las API de los modelos en caso de que aplique, utilizando las mejores prácticas de seguridad y desarrollo de aplicaciones.
- **Monitoreo de comportamiento del modelo**
  Asegúrese de monitorear el comportamiento del modelo de forma constante evaluando sesgos o información errónea.
- **No entregar información confidencial**
  Los modelos de IA/ML son solo herramientas de apoyo en las operaciones. No les entregue decisiones ni datos importantes.



Proyecciones en el ecosistema de IA/ML para el 2025

Estas son algunas tendencias a tener en cuenta para el año 2025:

- **Cadena de suministros del software**
  Seguirá siendo un vector prevalente y en constante aumento. Las plataformas de desarrollo del ecosistema IA/ML, los científicos de datos, desarrolladores, etc., seguirán aumentando en número como objetivos de los actores de amenaza.
- **Aumento de stealers**
  Se multiplicará el número de stelears orientados a capturar actividad asociada a ecosistemas de IA/ML.
- **Desarrollo de modelos ofensivos**
  Desarrollo de modelos ofensivos automatizados. Surgirán herramientas ofensivas más potentes asociadas a **Agentes de IA** para ejecutar cada etapa en la explotación de vulnerabilidades de forma autónoma y adaptativa.

Por lo mismo, resulta fundamental estar atentos e informados de la evolución de las amenazas asociadas al ecosistema de IA/ML, y seguir reforzando las medidas y políticas de seguridad que permitan adaptarse a esta amenaza creciente.

digital

Capítulo

05.

CIBER AMENAZAS EN IoT Y DISPOSITIVOS MÓVILES

Según nuestro seguimiento de Amenazas en Entel Digital, Brasil (46%), México (18%), Argentina (11%) y Chile (7%) lideraron el Top 10 de países más afectados por Ransomware en Latinoamérica y el Caribe durante 2024.

Perspectiva de amenazas en IoT y dispositivos móviles

Los dispositivos IoT transforman empresas e industrias por medio de la automatización, al:

- Optimizar procesos.
- Reducir costos.
- Mejorar la eficiencia operativa.
- Permitir recopilación en tiempo real de datos cruciales.
- Facilitar toma de decisiones basada en análisis precisos.

> **La IoT impulsa la innovación y la competitividad en un mercado cada vez más digitalizado, pero también presenta importantes amenazas de seguridad.**

La conexión constante de los dispositivos IoT a las redes de datos, amplía la superficie de ataque de las organizaciones, quedando expuestas a:

- Vulnerabilidades por acceso no autorizado.
- Robo de datos sensibles.
- Interrupciones operativas mediante Ransomware o DDoS.
- Propagación rápida por interconexión de dispositivos.
- Afectación de múltiples áreas de la operación.

Además, la falta de estándares de seguridad robustos, combinada con configuraciones débiles o dispositivos sin actualizaciones, facilita que los atacantes comprometan sistemas críticos. Por ello, es crucial implementar medidas de ciberseguridad específicas para mitigar estos riesgos.

Amenazas que afectan a los dispositivos IoT

Malwares y Botnets

Los atacantes pueden comprometer aquellos dispositivos que se encuentren mal protegidos, como cámaras de seguridad, routers, sensores u otros artefactos que, al agruparlos en botnets, pueden ser utilizados para realizar ataques como:

1. Ataques distribuidos de denegación de servicio (DDoS):

- Pueden sobrecargar servidores y redes con tráfico, causando interrupciones masivas.
- La botnet Mirai comprometió millones de dispositivos IoT para ejecutar un ataque DDoS a gran escala.

Botnets asociadas a dispositivos IoT presentes en los últimos años a nivel mundial

Ngioweb

Origen: Rusia

Fecha de detección: 2022

Objetivo

- Crear una red global de proxys (NSOCKS), con dispositivos de IoT comprometidos, para realizar trabajos de DDoS

Raptor Train

Origen: China

Fecha de detección: 2020

Objetivo

- Comprometer dispositivos SOHO e IoT afectados, incluidos módems, routers, cámaras IP, dispositivos NVR/DVR y dispositivos NAS

Medusa

Origen: Desconocido

Fecha de detección: 2020

Objetivo

- Ataques DDoS utilizando múltiples navegadores en dispositivos infectados

LokiBot

Origen: Desconocido

Fecha de detección: 2021

Objetivo

- Minería de criptomonedas y robo de credenciales

Mozi

Origen: China

Fecha de detección: 2019

Objetivo

- Ataques DDoS y persistencia en redes IoT

Mirai

Origen: Japón

Fecha de detección: 2020

Objetivo

- Ataques DDoS, principalmente en routers y cámaras IP

2. Ransomware en IoT:

- Dirigido a dispositivos IoT como cámaras de seguridad e incluso equipos industriales con configuraciones débiles.
- Secuestra el control del dispositivo o cifra datos almacenados, exigiendo un pago para devolver el acceso.
- La falta de actualizaciones, estándares de seguridad inconsistentes y la creciente interconexión aumentan el riesgo.

Secuestro y acceso no autorizado

Muchos dispositivos IoT se entregan con contraseñas por defecto o utilizan credenciales débiles que no son modificadas por los usuarios. Esto facilita que los atacantes puedan acceder a los dispositivos sin mucha dificultad, tanto para llevar a cabo actividades de espionaje o como puntos de entrada a redes más amplias.

Estas amenazas se ejecutan a través de los siguientes ataques:

Ataques de fuerza bruta

Pueden automatizar intentos para adivinar las contraseñas de los dispositivos IoT.

Ataques de diccionario

Utilizan listas de contraseñas comunes o por defecto para acceder rápidamente a dispositivos.

Casos más emblemáticos relacionados con la explotación de IoT

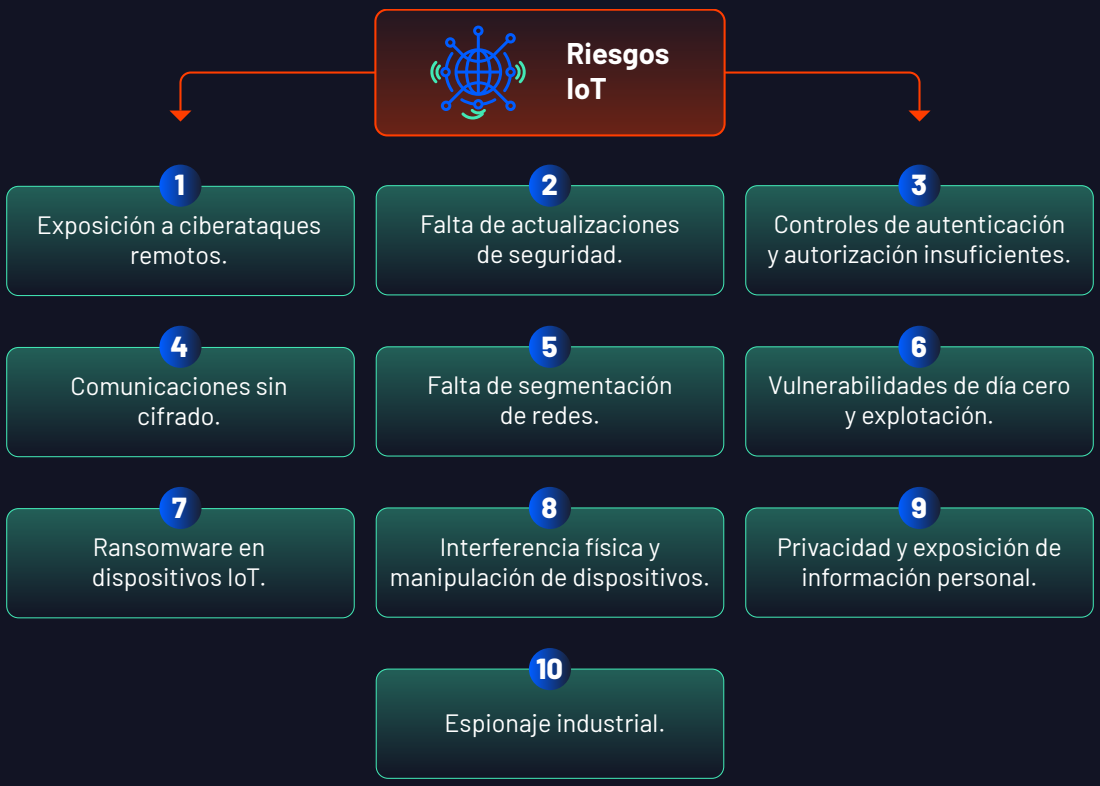
	Descripción	Dispositivos afectados
Mirai Botnet Año 2016	Ataque de DDoS masivo utilizando miles de dispositivos IoT comprometidos.	Cámaras IP, routers, DVRs
Reaper (IoTroop) Año 2017	Botnet que explotó vulnerabilidades en múltiples dispositivos IoT.	Cámaras IP, DVRs, routers
Cámaras de seguridad Hikvision Año 2017	Hackers explotaron vulnerabilidades en cámaras de seguridad para espiar y acceder a redes internas.	Cámaras de seguridad
Hackeo a casino con termómetro Año 2018	Un termómetro inteligente de un acuario fue utilizado para acceder a la red interna y robar datos de clientes.	Termómetro inteligente
Botnet "VPNFilter" Año 2018	Malware infectó routers y dispositivos IoT para espionaje y control remoto, afectando redes globalmente.	Routers y dispositivos IoT
Operación "Zebrocy" Año 2019	Grupo vinculado al espionaje estatal utilizó IoT para infliltrarse en redes corporativas y gubernamentales.	Routers, cámaras conectadas
Industroyer 2 Año 2022	Ataque dirigido a infraestructuras críticas usando IoT como punto de entrada.	Dispositivos industriales conectados
Malware TR-064 (Mirai) Año 2023	Uso de vulnerabilidades en TR-064 para propagar malware Mirai en redes domésticas.	Routers y dispositivos domésticos
Roku Credential Stuffing Año 2024	Compromiso con cuentas mediante reutilización de credenciales en dispositivos IoT.	Smart TVs (Roku)

Estos casos demuestran cómo la falta de seguridad en dispositivos conectados puede tener consecuencias significativas, desde el robo de datos sensibles hasta la infiltración en redes corporativas y gubernamentales.

Seguridad en redes de IoT industrial y personal

La seguridad en redes de IoT es un desafío creciente, pues crea nuevas superficies de ataque para los ciberdelincuentes, quienes aprovechan vulnerabilidades en dispositivos IoT para comprometer datos y operaciones críticas.

Los riesgos se asemejan mucho a los que suceden a diario en dispositivos computacionales comunes, donde destacan:



Impacto IoT

Operativo

En entornos IoT, las interrupciones de servicios causadas por ciberataques puden paralizar operaciones críticas, afectando industrias, servicios públicos y cadenas de suministro.

Financiero

Las brechas de seguridad en IoT, generan altos costos de recuperación, incluyendo la restauración de sistemas, inversiones en mejoras de seguridad y gestión de daños reputacionales.

Reputacional

Los ataques a dispositivos IoT dañan la confianza del cliente al exponer vulnerabilidades en sistemas conectados, estos incidentes pueden desencadenar sanciones regulatorias y perjudicar la competitividad en mercados que valoran la seguridad.

Seguridad y privacidad

El robo de datos personales o corporativos es una consecuencia frecuente de ataques a entornos IoT. Los dispositivos comprometidos pueden ser utilizados para espionaje o vigilancia no autorizada, en redes empresariales y gubernamentales.

Principales amenazas en dispositivos móviles

Dispositivos móviles como smartphones y tablets resultan atractivos porque:

- Almacenan información personal y laboral.
- Permiten realizar transacciones financieras.
- Dan acceso a redes corporativas y otros dispositivos.

Por eso, los atacantes se enfocan cada vez más en los sistemas operativos móviles, desarrollando amenazas que van desde spyware y troyanos bancarios, hasta aplicaciones de suplantación de identidad (Phishing).

¿Qué es el Malware móvil?

- Es cualquier software malicioso diseñado específicamente para atacar dispositivos móviles, como smartphones y tablets.
- Suele tener como objetivo robar información personal, espiar al usuario o entregar el control sobre el dispositivo afectado.

Tipos de malware móvil

Rootkits

Spyware

Ransomware

Adware y fraudes Click

Troyanos Bancarios

Métodos de distribución

Phishing

APK maliciosas en sitios no oficiales

Explotación de vulnerabilidades

La adopción de buenas prácticas de seguridad y la concientización sobre los riesgos son claves para mitigar el impacto del Malware en dispositivos móviles. A medida que los atacantes continúan desarrollando técnicas más sofisticadas, es fundamental que los usuarios estén atentos y utilicen soluciones de seguridad adecuadas para proteger sus dispositivos y su información personal.

Phishing móvil y Smishing

El Phishing móvil y el Smishing son dos de las tácticas más comunes utilizadas por ciberdelincuentes para engañar a los usuarios de dispositivos móviles y obtener acceso a información personal o financiera.

Phishing móvil

- Creación de enlaces maliciosos y sitios web falsos, que imitan a plataformas legítimas.
- El tamaño de las pantallas móviles y la facilidad de distracción promueven el click irresponsable.

Smishing

- Utiliza mensajes de texto fraudulentos que parecen provenir de fuentes confiables.
- Suelen incluir enlaces a sitios falsos, enlaces infectados o solicitar datos personales.

Explotación de vulnerabilidades móviles

Es una técnica para aprovechar fallos o errores de seguridad en los sistemas operativos y aplicaciones de dispositivos móviles.

Estas vulnerabilidades permiten:

- Obtener acceso no autorizado a datos.
- Controlar el dispositivo de la víctima.
- Instalar Malware sin que el usuario se percate.

Afectan tanto a sistemas operativos como Android e iOS, y abarcan desde problemas en el propio sistema hasta fallos en aplicaciones de terceros.

Algunas de las vulnerabilidades más explotadas son:

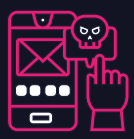
- Vulnerabilidades del sistema operativo.
- Vulnerabilidades de aplicaciones.
- Fallos en protocolos de comunicación.
- Ataques de día cero (Zero-Day).

Vulnerabilidades que han afectado a dispositivos móviles

Stagefright

Sistema: Android

Descripción
Ejecución de código malicioso mediante archivo de vídeo manipulado
Impacto
Ejecución de código sin interacción del usuario al recibir MMS
Mitigación
Google lanzó parches de seguridad y fabricantes actualizaron dispositivos



Pegasus

Sistema: iOS, Android

Descripción
Spyware de NSO Group que explota vulnerabilidades de día cero
Impacto
Ejecución de código sin interacción del usuario al recibir MMS
Mitigación
Google lanzó parches de seguridad y fabricantes actualizaron dispositivos

BlueBorne

Sistema: Android, iOS, Windows, Linux

Descripción
Vulnerabilidad en protocolo Bluetooth sin necesidad de emparejamiento
Impacto
Compromiso de dispositivos sin interacción ni conexión a internet
Mitigación
Actualizaciones de seguridad por Google, Apple, Microsoft y distribuciones Linux

QuadRooter

Sistema: Android (Qualcomm)

Descripción
Serie de cuatro vulnerabilidades en procesadores Qualcomm
Impacto
Control total del dispositivo mediante acceso root
Mitigación
Qualcomm y Google lanzaron parches, fabricantes actualizaron sistemas

JailbreakMe

Sistema: iOS

Descripción
Exploit basado en navegador activado al visitar página web
Impacto
Instalación de software no autorizado y posible malware
Mitigación
Apple lanzó parches específicos

Towelroot

Sistema: Android

Descripción
Exploit diseñado por George Hotz para vulnerabilidad en kernel Linux
Impacto
Acceso root y compromiso total del dispositivo
Mitigación
Google cerró vulnerabilidad en versiones posteriores

Dirty COW

Sistema:
Copy-On-WriteAndroid, Linux

Descripción
Vulnerabilidad en manejo de memoria del kernel Linux
Impacto
Elevación de privilegios y facilitación de malware
Mitigación
Google y Linux lanzaron parches de seguridad

StrandHogg

Sistema: Android

Descripción
Suplantación de aplicaciones en el dispositivo
Impacto
Interceptación de credenciales y acceso a datos sensibles sin detección
Mitigación
Google lanzó parche para versiones recientes

Broadpwn

Sistema: iOS, Android

Descripción
Vulnerabilidad en chipset Wi-Fi Broadcom
Impacto
Compromiso de dispositivos en la misma red Wi-Fi
Mitigación
Google y Apple lanzaron parches de seguridad

KrØØk

Sistema:
Android, iOS, Dispositivos Wi-Fi con chips Broadcom y Cypress

Descripción
Vulnerabilidad en chips Broadcom y Cypress para Wi-Fi
Impacto
Interceptación de datos protegidos por WPA2
Mitigación
Fabricantes corrigieron vulnerabilidad en chips Wi-Fi

Estrategias de defensa para IoT y dispositivos móviles

1 Segmentación de redes y gestión de dispositivos IoT

- **Ubicar dispositivos IoT en una red separada** de otros sistemas críticos o redes empresariales para reducir el riesgo de propagación de amenazas.
- **Implementar VLANs (Redes de Área Local Virtual)** para separar dispositivos IoT según su función o nivel de seguridad.
- **Configurar ACL para gestionar el tráfico entre redes** y definir qué dispositivos o redes pueden comunicarse entre sí.
- **Colocar firewalls entre las redes de IoT y otras redes internas**, para filtrar y supervisar el tráfico de IoT y bloquear conexiones no autorizadas.
- **Adoptar un enfoque de Confianza Cero**, donde ningún dispositivo se considera seguro a menos que se autentique y autorice explícitamente.
- **Implementar soluciones de monitoreo de red**, que permitan detectar comportamientos anómalos o intentos de acceso no autorizado en la red IoT.
- **Colocar dispositivos que manejan datos sensibles o críticos en subredes** con acceso restringido y monitoreado para minimizar la exposición.

2 Recomendaciones en políticas de administración de dispositivos móviles

- **Requerir autenticación multifactor (MFA)** en dispositivos móviles para asegurar el acceso.
- **Establecer políticas de control de acceso** que limiten el acceso a aplicaciones y datos sensibles según el rol del usuario.
- **Habilitar el cifrado de datos en dispositivos móviles** para proteger la información almacenada.
- **Implementar una lista de aplicaciones autorizadas** para limitar el uso de software que no cumpla con las políticas de seguridad.
- **Evitar el uso de aplicaciones no autorizadas** que puedan poner en riesgo la información corporativa.
- **Establecer políticas de contraseñas seguras**, que incluyan longitud mínima y requisitos de complejidad.
- **Forzar el cambio de contraseñas regularmente** y establecer límites para intentos fallidos de inicio de sesión.
- **Implementar soluciones de administración de dispositivos móviles (MDM)** que permitan supervisar, actualizar y, en caso necesario, borrar remotamente los datos del dispositivo.
- **Utilizar redes de acceso Wi-Fi separadas** para dispositivos móviles de empleados y visitantes, para evitar riesgos en la red interna y proteger recursos sensibles.
- **Establecer políticas para mantener actualizados el sistema operativo y las aplicaciones** en los dispositivos móviles, aplicando los parches de seguridad apenas estén disponibles.
- **Restringir el acceso de las aplicaciones a datos sensibles**, como contactos, ubicación o información corporativa, solo a lo necesario para sus funciones.
- **Desactivar funciones como Bluetooth o GPS** en dispositivos móviles cuando no se necesiten, ya que pueden aumentar la superficie de ataque.
- **Realizar programas de capacitación y concientización** en seguridad móvil, para que los usuarios comprendan los riesgos y sigan las políticas.

3 Autenticación multifactor y cifrado

El uso de autenticación y cifrado en dispositivos IoT y móviles son medidas fundamentales para proteger la transmisión de datos y garantizar que la información que se intercambia entre dispositivos, aplicaciones y redes sea segura y accesible solo para usuarios y sistemas autorizados.

- **Autenticación**
  Asegura que solo los dispositivos legítimos puedan comunicarse en la red.
- **Cifrado**
  Protege los datos almacenados y en tránsito frente a intercepción o manipulación.

Sin estas medidas, el riesgo de comprometer datos críticos (como información de sensores o comandos de dispositivos industriales) es alto.

Es importante considerar lo siguiente para cada dispositivo:

- **Dispositivos IoT**
  Debido a las limitaciones de procesamiento, los métodos de autenticación y cifrado deben ser ligeros y eficientes, sin sacrificar seguridad.
- **Dispositivos móviles**
  El cifrado y la autenticación avanzada, como la autenticación multifactor (MFA), son cruciales para proteger la integridad y confidencialidad de los datos.

4 Monitoreo continuo y parcheo regular

La gestión efectiva de dispositivos IoT conectados requiere un enfoque integral que combine monitoreo continuo, buenas prácticas de seguridad e implementación de tecnologías avanzadas.

- **Monitoreo con soluciones en tiempo real**

  Para analizar el tráfico y detectar anomalías, con herramientas como IDS y plataformas de análisis de comportamiento. Escanear regularmente dispositivos para identificar Firmware desactualizado o brechas.

- **Aplicar parches y actualizaciones de manera oportuna**

  Seguir las recomendaciones del fabricante para mitigar riesgos derivados de vulnerabilidades descubiertas. Asimismo, implementar autenticación robusta.

- **Segmentación de la red**

  Separar los dispositivos IoT de los sistemas críticos minimiza el alcance de un ataque en caso de una intrusión.

- **Visibilidad y el control son fundamentales**

  Centralizar la gestión de los dispositivos IoT mediante plataformas que permitan inventariarlos, monitorearlos y gestionar configuraciones de forma remota.

- **Capacitación del personal**

  Buenas prácticas de ciberseguridad, auditorías regulares y un plan de respuesta ante incidentes que permita actuar rápidamente.

Estos pasos, en conjunto, fortalecen la seguridad de los dispositivos IoT y reducen significativamente los riesgos asociados.

digital

Capítulo

06.

CASOS DE ESTUDIO INCIDENTES SIGNIFICATIVOS DURANTE EL 2024

Según CCI Entel Digital, los incidentes de Data Breach en LATAM disminuyeron un 15% en 2024, respecto del peak histórico de 442 casos alcanzado en 2023.

6.1 Ransomware en Latinoamérica: una empresa de Telecomunicaciones

Objetivo
Empresa proveedora de servicios de telecomunicaciones

Fecha: abril 2024

Una empresa con presencia en América Latina sufrió un devastador ataque de Ransomware dirigido específicamente a su infraestructura basada en servidores VMware ESXi, una tecnología clave en la virtualización de recursos esenciales.

Este incidente se suma a una creciente lista de ciberataques que destacan la vulnerabilidad de los sistemas críticos en una era de digitalización acelerada y amenazas cada vez más sofisticadas.

Estas fueron algunas de las consecuencias del ataque:

- Expuso fallas estructurales en las defensas cibernéticas de la organización
- Afectó sectores clave como la salud, la educación y los servicios públicos
- Interrupciones de servicios esenciales afectaron a múltiples organizaciones
- Puso en riesgo la continuidad operativa de servicios fundamentales

La naturaleza de este ataque, que explota vulnerabilidades conocidas en entornos virtualizados, es representativa de tendencias globales:

- Los ciberdelincuentes están apuntando cada vez más a Infraestructuras Críticas con herramientas avanzadas de extorsión y tácticas de infiltración complejas.
- El uso de Ransomware no solo busca beneficios financieros, sino también maximizar el daño operativo y reputacional.

Este caso sirve como una advertencia para otras organizaciones en América Latina y en todo el mundo, enfatizando la urgencia de reforzar la resiliencia frente a amenazas que no muestran signos de desaceleración.

Vector de ataque

- El Ransomware SEXi aprovechó vulnerabilidades críticas en servidores VMware ESXi, una plataforma utilizada en entornos industriales y de Infraestructura Crítica por su capacidad para gestionar múltiples servidores virtuales en un único hardware físico.
- Esta tecnología es clave en sectores donde la alta disponibilidad y el uso eficiente de recursos son fundamentales, como Salud, Energía, Transporte y Servicios públicos.

Técnicas utilizadas por los atacantes

1. Cifrado y exfiltración de datos:

- Además de cifrar los sistemas afectados, los atacantes exfiltraron datos sensibles.
- Los utilizaron como segunda capa de extorsión, aumentando la presión para pagar el rescate.

2. Explotación de vulnerabilidades conocidas:

- Explotaron vulnerabilidades conocidas en VMware ESXi que no fueron corregidas, algo especialmente riesgoso en Infraestructura Crítica por su baja frecuencia de actualización.
- **49% de los ataques de Ransomware** a Infraestructuras Críticas explotan vulnerabilidades sin parchear.

3. Configuraciones inseguras:

- Utilizaron configuraciones predeterminadas o mal configuradas, como credenciales por defecto, para ganar acceso inicial a los sistemas.
- Estos errores de configuración son comunes en entornos con una gestión inadecuada de activos y redes.

4. Movimiento lateral y propagación:

- Una vez dentro, SEXi utilizó técnicas de movimiento lateral, propagándose a través de redes interconectadas que carecían de segmentación adecuada.
- Esto permitió comprometer servidores adicionales y cifrar datos en múltiples nodos simultáneamente, amplificando el impacto del ataque.

Impacto del ataque

1. Infraestructura afectada

89 VPS (Virtual Private Servers) comprometidos

38% de la infraestructura operativa afectada

Servidores vinculados a redes de respaldo

2. Sectores afectados

Salud
Paralización de servicios médicos

Educación
Sistemas de gestión y registro inaccesibles

Servicios Esenciales
Interrupciones en servicios de agua y electricidad

3. Compromiso de copias de seguridad

79% de los respaldos fueron cifrados

Se eliminaron opciones inmediatas de recuperación

4. Impacto operacional

Servicios esenciales paralizados por más de 15 días

Sistemas de respaldo inhabilitados en medicina y transporte

5. Impacto económico

140M USD en rescates potenciales (2 bitcoins por víctima)

50M USD por sistemas, sanciones y pérdida de confianza

6. Impacto en seguridad

Exposición de datos sensibles para posible Phishing

Introducción de backdoors para futuros ataques

> **El ataque escaló rápidamente debido a la reutilización de credenciales comprometidas y la falta de segmentación de red, lo que permitió a los atacantes moverse lateralmente dentro de la infraestructura.**

Apreciación

La combinación de amenazas avanzadas y una dependencia tecnológica cada vez mayor exige un enfoque estratégico que integre:

- La resiliencia operativa
- La colaboración interinstitucional
- El uso de tecnologías avanzadas

Para organizaciones similares, este análisis destaca que la preparación no es opcional: **es imperativo adoptar una mentalidad proactiva y estratégica para anticiparse a amenazas** dinámicas y garantizar la continuidad operativa en un panorama global cada vez más hostil.

6.2 Ciberespionaje en el sector gubernamental

El ciberespionaje en 2024 ha evolucionado hacia un enfoque más dirigido y sofisticado, priorizando:

- La explotación de identidades
- El abuso de credenciales válidas
- La adopción de herramientas avanzadas

Este análisis integra datos de múltiples informes recientes, destacando los desafíos técnicos y estratégicos que enfrenta el sector público en un entorno cada vez más dinámico y hostil.

Escalamiento de amenazas

Las tácticas de los actores de ciberamenazas han evolucionado hacia la optimización de ataques dirigidos, con un fuerte enfoque en vulnerabilidades activas y credenciales comprometidas:

1. Explotación de identidades

30% En el uso de credenciales válidas para acceder a sistemas gubernamentales.

2. Automatización e IA Generativa

Utilizan IA para crear contenido de Phishing avanzado y acelerar las campañas de explotación de vulnerabilidades.

Objetivos principales

1. Infraestructuras Críticas

La explotación de herramientas de transferencia de datos como MOVEit Transfer ha comprometido millones de registros sensibles.

2. Sistemas de Gobierno y Defensa

APTs patrocinados por estados priorizan datos diplomáticos y estratégicos, empleando herramientas avanzadas para evadir detecciones.

Vectores de ataque principales

1. Abuso de credenciales:

266% en 2024▲ En el aumento del uso de Infostealers en 2024, con nuevas variantes como Rhadamanthys y LummaC2.

Los accesos iniciales mediante credenciales válidas se han combinado con Kerberoasting para burlar la autenticación MFA.

2. Explotación de vulnerabilidades activas:

Vulnerabilidades como CVE-2023-34362 en MOVEit Transfer han sido explotadas para acceso remoto.

La explotación de herramientas de administración como Active Directory ha permitido movimientos laterales rápidos en redes gubernamentales.

3. Ataques basados en IA y automatización:

IA generativa para automatizar la creación de señuelos en Phishing y personalización de Malware para objetivos específicos.

4. Ransomware y filtración de datos:

54% De los ataques gubernamentales en 2024 han incluido la filtración de datos en sus ataques de Ransomware.

Impacto en el sector gubernamental

1. Pérdida de confidencialidad:

Los datos filtrados incluyen información estratégica que compromete tanto la soberanía nacional como la seguridad operativa.

En un caso destacado en 2024, se expusieron 7 GB de registros sensibles de un portal gubernamental.

94% De los ataques intentaron vulnerar copias de seguridad para maximizar el daño, siendo las entidades gubernamentales un blanco prioritario.

2. Interrupciones operacionales:

Ataques como los de Rhysida y LockBit 3.0 han causado interrupciones prolongadas en servicios públicos esenciales.

Un ataque en Latinoamérica en 2024 dejó a los sistemas judiciales fuera de línea por días.

3. Impacto económico:

Los costos de los ataques exitosos en Infraestructuras Críticas se han incrementado por la complejidad de las remediaciones y la dependencia creciente de sistemas conectados.

Las organizaciones gubernamentales con mayor infraestructura TI presentan costos hasta cuatro veces mayores que los de sectores menos conectados, con tiempos de recuperación promedio superiores a un mes.

4. Impacto geopolítico:

Los ataques cibernéticos se han convertido en una herramienta clave en conflictos internacionales, con ejemplos en Ucrania, Taiwán y el Medio Oriente.

En 2024, fueron empleados para manipular narrativas y paralizar infraestructuras estratégicas, desestabilizando gobiernos y afectando la opinión pública.

Lecciones aprendidas

Las tácticas de los actores de ciberamenazas han evolucionado hacia la optimización de ataques dirigidos, con un fuerte enfoque en vulnerabilidades activas y credenciales comprometidas:

1. Gestión de accesos e identidades:

- **Estrategias avanzadas de autenticación**

  En 2024, el abuso de credenciales válidas se ha consolidado como el principal vector de ataque en el sector gubernamental (47% de los incidentes). Esto refuerza la necesidad de implementar autenticación multifactor adaptativa y políticas de acceso basadas en el contexto.

- **Inteligencia Artificial aplicada**

  Soluciones de IA permiten detectar anomalías en el acceso en tiempo real, identificando patrones sospechosos antes de que se materialicen compromisos mayores.

2. Modernización tecnológica:

- **Segmentación de Redes**

  Separar redes críticas mediante tecnologías como microsegmentación dificulta los movimientos laterales de los atacantes. En 2024, esta estrategia redujo los incidentes en un 30%.

- **Actualización continua**

  La explotación de vulnerabilidades activas, como CVE-2023-34362, resalta la importancia de mantener un ciclo continuo de parches en sistemas y aplicaciones críticas.

3. Ciber resiliencia operacional:

- **Simulaciones de incidentes**

  Ensayos regulares en redes gubernamentales han demostrado reducir los tiempos de respuesta en hasta un 25%.

- **Planes de recuperación y redundancia**

  Los sistemas redundantes han sido clave para minimizar el impacto de interrupciones críticas.

Estrategias de colaboración

La colaboración entre gobiernos y el sector privado es crucial para abordar las amenazas cibernéticas de manera integral, dado que ambos sectores tienen activos interdependientes.

Los modelos de colaboración en tiempo real, que incluyen intercambio de inteligencia de amenazas, simulacros conjuntos y el desarrollo de estándares de seguridad, han reducido los tiempos de detección en un 20% en entornos críticos durante 2024.

Apreciación

La ciberseguridad actualmente **requiere un enfoque holístico que integre:**

- Tecnologías avanzadas
- Colaboración entre entidades
- Una gestión proactiva de riesgos

La adopción de herramientas innovadoras y la modernización de infraestructuras no solo mitigan riesgos, sino que también pueden convertirse en ventajas estratégicas.

> **Los gobiernos que logren integrar estas estrategias estarán mejor posicionados para resistir ataques y mantener la confianza pública.**

Beneficios clave

- Reducción de tiempos de respuesta
- Fortalecimiento de la soberanía digital
- Estímulo a la innovación local

Los gobiernos enfrentan el desafío de adaptarse rápidamente al panorama cibernético de 2025. Las estrategias combinadas de innovación tecnológica, capacitación y colaboración multisectorial son esenciales para superar estos retos y garantizar la protección de los activos más valiosos frente al ciberespionaje global.

6.3 Fraude financiero y cibercrimen

El 14 de mayo de 2024, una importante institución financiera informó sobre un acceso no autorizado a una base de datos alojada en un proveedor externo. Este incidente comprometió información personal de clientes, empleados y exempleados en Chile, España y Uruguay.

Aunque no se accedió a datos transaccionales ni a credenciales bancarias, la filtración de información aumentó el riesgo de fraudes mediante Phishing y robo de identidad.

La institución activó inmediatamente sus protocolos de respuesta:

- Bloquear el acceso a la base de datos afectada
- Notificar a reguladores y clientes
- Reforzar medidas de prevención de fraudes

Sin embargo, el impacto del ataque fue significativo, con efectos en diferentes niveles.

Impacto del incidente

1. Operacional

- Las operaciones y sistemas centrales de la institución financiera no fueron afectados, garantizando la continuidad del servicio.
- Se implementaron medidas inmediatas de mitigación, incluyendo la monitorización activa de posibles intentos de fraude relacionados.

2. Reputacional

- El incidente recibió cobertura mediática internacional, impactando negativamente la confianza de clientes, inversionistas y empleados.
- Se identificaron posibles consecuencias a largo plazo, como la dificultad para retener clientes y el desprestigio de la marca.

3. Financiero

- Se incurrió en costos operativos como reforzamiento de medidas de seguridad y campañas de comunicación.
- Riesgo de litigios en múltiples jurisdicciones, especialmente en países con legislaciones estrictas en protección de datos.
- Aumento en las primas de seguros de ciberseguridad, reflejando la percepción de mayor exposición al riesgo.

4. Legal y Regulador

- Investigación en curso por parte de autoridades regulatorias y policiales en Chile, España y Uruguay.
- Potenciales sanciones por incumplimientos en la protección de datos según normativas locales e internacionales, como el GDPR en Europa.

5. Social

- 4.1 millones de clientes expuestos en Chile y un número indeterminado en España y Uruguay.
- Sensibilización de la sociedad sobre los riesgos asociados a la protección de datos en la banca digital.

Estrategias de mejora

Auditorías y controles de proveedores

Realizar evaluaciones continuas y establecer estándares estrictos para proveedores de servicios externos, priorizando la seguridad de datos.

Mejoras en resiliencia cibernética

Implementar sistemas de monitoreo proactivo y fortalecer la infraestructura tecnológica para identificar amenazas en tiempo real.

Almacenamiento inmutable

Adoptar tecnologías que aseguren que los datos almacenados no puedan ser modificados, cifrados ni eliminados en caso de un ataque.

Programas de concientización

Desarrollar campañas educativas para clientes y empleados, enfocadas en identificar intentos de fraude y adoptar buenas prácticas de seguridad digital.

Refuerzo de políticas de seguridad

Incluir la adopción de tecnologías emergentes y la implementación de estrategias de defensa basadas en Inteligencia Artificial.

Simulaciones regulares de incidentes

Realizar simulacros de ataques cibernéticos y ejercicios de respuesta para evaluar y mejorar la capacidad de la institución frente a posibles incidentes futuros.

Apreciación

Este ciberataque a una institución financiera destaca los riesgos inherentes a la digitalización y la creciente sofisticación de los ciberdelincuentes. Aunque las medidas inmediatas adoptadas limitaron el impacto, el incidente evidencia la necesidad de reforzar la seguridad cibernética, especialmente en un entorno financiero globalizado y dependiente de la tecnología.

Estas medidas no solo protegerán a las instituciones, sino también a los millones de usuarios que confían en ellas para gestionar su patrimonio.

Capítulo

07.

TENDENCIAS Y PROYECCIONES PARA EL 2025

Las medianas y grandes empresas serán un blanco prioritario para los ciberataques, impulsados por un incremento en intrusiones en la nube y el uso de credenciales comprometidas.

Proyección de amenazas emergentes

Por los constantes avances tecnológicos y el ingenio de los actores maliciosos, se proyecta un incremento significativo en la sofisticación y alcance de las ciberamenazas para el año 2025.

Este año puede marcar un punto de inflexión en cómo las organizaciones abordan la seguridad digital. Para ello, la integración de tecnologías emergentes como la Inteligencia Artificial plantea tanto oportunidades como desafíos.

La única manera de enfrentarse a las diversas y sofisticadas estrategias de los ciberdelincuentes es comprender en profundidad las amenazas emergentes y prepararse de forma proactiva en dos áreas clave:

- El uso de tecnologías avanzadas en ciberataques
- Las nuevas tendencias en Ransomware y Exploit Kits

1. Uso de nuevas tecnologías en ciberataques

Ataques impulsados por Inteligencia Artificial (IA):

Automatización avanzada

Los cibercriminales están utilizando IA para automatizar la creación de ataques adaptables y personalizados, con herramientas que imitan patrones de lenguaje humano.

Deepfakes y engaños visuales

Los modelos generativos permiten generar deepfakes convincentes, que pueden utilizarse para fraudes financieros, campañas de desinformación y espionaje.

Ataques predictivos

Los modelos de lenguaje de gran tamaño (LLM) permiten prever vulnerabilidades en sistemas de defensa, optimizando la efectividad de los ataques.

Manipulación de datos con IA:

Sabotaje de IA operativa

Pueden entrenar modelos con datos maliciosos, alterando decisiones críticas en sistemas autónomos como vehículos o aplicaciones médicas.

2. Nuevas tendencias en Ransomware y Exploit Kits

Ransomware evolucionado y ataques selectivos:

Segmentación precisa

Los ataques de Ransomware están migrando hacia modelos más dirigidos, investigando exhaustivamente a sus objetivos.

Nuevas tácticas de extorsión

Además de cifrar datos, algunos filtran información sensible para presionar a las víctimas.

Ransomware-as-a-Service (RaaS):

Accesibilidad democratizada

Plataformas de RaaS están permitiendo que atacantes con habilidades limitadas ejecuten campañas complejas.

Automatización y velocidad

La integración de IA en estas plataformas facilita la creación de exploits más sofisticados en menor tiempo.

Exploit Kits más avanzados:

Ataques adaptativos

Incorporan capacidades de Machine Learning para adaptar ataques a las vulnerabilidades detectadas en tiempo real.

Vulnerabilidades persistentes

81% de los ataques explotan vulnerabilidades no parcheadas, a menudo en software antiguo.

Impacto en la cadena de suministro:

Ransomware dirigido a proveedores

Las cadenas de suministro son un objetivo cada vez más común, afectando a varias empresas a la vez.

Cambios en el marco legal y normativo

El nuevo panorama de la seguridad digital ha exigido cambios profundos en el marco normativo a nivel global, regional y local. En este contexto, Chile y Latinoamérica se encuentran en una fase crucial de adaptación regulatoria, con iniciativas legislativas que buscan:

- Proteger Infraestructuras Críticas y datos personales
- Establecer estándares que fomenten la resiliencia digital y la cooperación entre el sector público y privado

Ley Marco de Ciberseguridad N° 21.663 (Chile)

Objetivo

Establecer la institucionalidad y normativa general para estructurar y coordinar las acciones de ciberseguridad en organismos del Estado y sectores críticos.

Impacto clave

- Creación de la Agencia Nacional de Ciberseguridad (ANCI) como entidad reguladora central.
- Regulación de servicios esenciales para implementar estándares de ciberseguridad mínimos.
- Colaboración público-privada, cooperación entre empresas y el Estado.
- Resiliencia digital, obliga a desarrollar planes de respuesta y recuperación.

Reforma a la Ley N° 19.628 sobre Protección de Datos Personales

Objetivo

Actualización del enfoque hacia los derechos digitales, aplicando principios como consentimiento informado y derecho a la portabilidad de datos.

Impacto clave

- Aumento en la inversión de empresas para cumplir con medidas de seguridad de datos.
- Fortalecimiento de sanciones para el incumplimiento de estándares de protección.

Análisis de regulaciones en Latinoamérica

Latinoamérica ha intensificado sus esfuerzos por fortalecer el marco normativo en ciberseguridad y protección de datos personales. Esto responde al incremento de ciberamenazas que afectan tanto a Infraestructuras Críticas como a los derechos de los ciudadanos en un entorno digital interconectado.

1. Ciberseguridad como prioridad estratégica

Enfoque en Infraestructuras Críticas

- Las nuevas normativas están centradas en **proteger sectores estratégicos como Energía, Salud, Telecomunicaciones y Servicios financieros.**
- **Buscan garantizar estándares mínimos de seguridad** y fomentar la resiliencia operativa en caso de ciberataques.

Gestión de incidentes

- Se promueve la creación de **equipos nacionales de respuesta a incidentes** (CSIRTs).
- **Protocolos para el reporte obligatorio de incidentes cibernéticos,** con esfuerzos públicos y privados.

2. Protección de datos personales: hacia un enfoque regional unificado

Ampliación de derechos

- Reformas para garantizar derechos como el **acceso, rectificación, oposición y portabilidad de datos personales.**
- Buscan establecer principios como **la seguridad desde el diseño y la privacidad por defecto.**

Impacto en las empresas

- **Las regulaciones están generando un aumento en la inversión tecnológica** para cumplir con estándares más altos de protección.
- Se fomenta una **cultura organizacional de ciberseguridad.**

3. Impacto regional e interoperabilidad normativa

Fomento de la cooperación regional

- **Regulaciones similares a estándares internacionales,** como el Reglamento General de Protección de Datos (GDPR) europeo.
- Esto promueve la interoperabilidad normativa en la región, **facilitando el comercio transfronterizo y la colaboración.**

Centroamérica como modelo

- Países como El Salvador están implementando leyes que **sirven como referencia para otras naciones vecinas.**
- **Demuestran cómo un enfoque regulatorio sólido puede ser adoptado** de manera progresiva en toda la región.

4. Desafíos y oportunidades hacia 2025

Desafíos:

- La diversidad en el desarrollo regulatorio entre países **representa un desafío para la coordinación regional.**
- Se observan **disparidades en la implementación y cumplimiento de leyes.**

Oportunidades:

- Estas regulaciones incentivan la **creación de ecosistemas de ciberseguridad más sólidos.**
- Promueven un **enfoque en la colaboración intersectorial e internacional para proteger datos y servicios críticos.**

Impacto global

1. Estandarización internacional y colaboración

Adopción de estándares internacionales como el GDPR y el NIST Cybersecurity Framework, asegurando compatibilidad para transacciones transfronterizas.

La armonización de normativas facilita la cooperación internacional en la lucha contra ciberataques.

2. Infraestructura crítica como prioridad

Las legislaciones emergentes priorizan la **protección de sectores estratégicos como Energía, Banca y Telecomunicaciones.**

Siguen modelos como la Directiva de Seguridad de Redes e Información (NIS) en la Unión Europea.

Proyecciones hacia 2025

El nuevo panorama de la seguridad digital ha exigido cambios profundos en el marco normativo a nivel global, regional y local. En este contexto, Chile y Latinoamérica se encuentran en una fase crucial de adaptación regulatoria, con iniciativas legislativas que buscan:

1. Mayor responsabilidad corporativa

- Las regulaciones exigirán auditorías de seguridad frecuentes y reportes obligatorios de incidentes.
- Las sanciones por incumplimiento serán más altas, incentivando que las empresas prioricen inversiones en ciberseguridad.

2. Expansión de derechos digitales

- Regulaciones más estrictas sobre el uso de datos sensibles y biométricos.
- Enfoque en la anonimización y seudonimización para proteger identidades en entornos digitales.

3. Nuevas entidades regulatorias

- Fortalecimiento de agencias nacionales de ciberseguridad en países como Chile.
- Tener un enfoque unificado frente a ciberamenazas globales.

4. Crecimiento en la cooperación internacional

- Acuerdos entre países para compartir información sobre amenazas cibernéticas y mejores prácticas.
- Esto permitirá mitigar riesgos en infraestructuras globales.

Latinoamérica está experimentando una transformación normativa sin precedentes en ciberseguridad y protección de datos personales, impulsada por la urgencia de enfrentar las amenazas crecientes en un entorno digital interconectado. Esto demuestra un compromiso claro por parte de los gobiernos para proteger tanto a las Infraestructuras Críticas como a los ciudadanos.

Hacia 2025, se proyecta un fortalecimiento de estas regulaciones, con un enfoque en la interoperabilidad regional y la alineación con estándares internacionales.

A pesar de desafíos como las disparidades regulatorias entre países, las oportunidades son significativas. La implementación de estándares unificados y la creación de agencias nacionales de ciberseguridad prometen un avance hacia un ecosistema más resiliente y preparado para mitigar los riesgos cibernéticos. Además, promueven la competitividad y la cooperación internacional.

Capítulo

08.

RECOMENDACIONES PARA EMPRESAS Y GOBIERNOS

Durante el 2024, los ataques de Ransomware evolucionaron significativamente, con un aumento del 90% en las víctimas extorsionadas públicamente y representando el 10% de todo el Malware detectado.

Mejores prácticas en ciberseguridad

1. Implementar normas y marcos de referencia de la familia ISO 27000

Estas proporcionan directrices para gestionar la seguridad de la información. Aunque cada una de ellas brinda sus propias capacidades, se potencian especialmente en conjunto. Entre estas normas se encuentran:

ISO 27001

Define los requisitos para un sistema de gestión de seguridad de la información (SGSI), permitiendo a las organizaciones gestionar adecuadamente los riesgos asociados a la seguridad de los datos.

ISO 27002

Ofrece una guía detallada sobre los controles de seguridad a implementar, proporcionando mejores prácticas para proteger la información.

ISO 27005

Proporciona un marco para identificar, evaluar y tratar riesgos específicos de seguridad de la información.

ISO 27701

Extiende los requisitos de ISO 27001 para incluir la gestión de la privacidad, lo cual es esencial para cumplir con normativas de protección de datos como el GDPR.

2. Adoptar un enfoque Zero-Trust

Zero-Trust se basa en la premisa "nunca confiar, siempre verificar". Esto implica la verificación constante y la autenticación continua para todos los accesos, tanto internos como externos. La verificación incluye la autenticación multifactor (MFA), el uso de microsegmentación y la aplicación de políticas de acceso condicional.

- **Implementar segmentación de redes** para limitar la propagación de amenazas, junto con autenticación constante de usuarios/dispositivos.
- **Crear zonas seguras dentro de la infraestructura de TI,** para minimizar el movimiento lateral de un atacante en caso de una violación de seguridad.
- **Definir políticas de seguridad por zona,** para implementar restricciones adecuadas y habilitar únicamente el tráfico necesario.

3. Autenticación de múltiples factores (MFA)

La autenticación multifactor combina factores como autenticación biométrica (algo que eres), tokens físicos (algo que tienes) y contraseñas seguras (algo que sabes) para lograr una seguridad proporcional al riesgo de cada nivel de acceso.

Asegura una mayor protección frente a ataques como el Phishing, la fuerza bruta o uso de credenciales filtradas conocidas.

- **Debe ser obligatoria para el acceso a todos los sistemas críticos,** incluyendo servicios en la nube, aplicaciones empresariales y cuentas administrativas.
- **Realizar auditorías periódicas** para asegurar que los mecanismos de autenticación funcionen correctamente y no presenten vulnerabilidades.
- **Monitorear continuamente los intentos de acceso y la detección de eventos anómalos** para evitar compromiso de mecanismos.

4. Hardenizado básico y segmentación de redes

Las medidas de endurecimiento (hardening) básico incluyen eliminar configuraciones por defecto, desactivar servicios innecesarios y restringir el acceso a puertos abiertos. Igualmente, deben integrar parches de seguridad de forma regular y listas blancas para aplicaciones autorizadas.

- **Implementar herramientas como CIS Benchmarks** como guía de buenas prácticas específicas para cada tipo de sistema operativo y aplicación.
- **Segmentar redes según importancia,** relevancia y sensibilidad de los datos, para establecer entornos seguros.
- **Implementar barreras lógicas y físicas para proteger datos críticos,** así como utilizar VLANs y NAC para control de acceso basado en roles.

5. Fortalecimiento de la ciber resiliencia y respuesta a incidentes

Es necesario aplicar protocolos y ejercicios de fortalecimiento de resiliencia, identificando debilidades en los procesos de respuesta y ajustando los sistemas de comunicación interna y externa.

- **Desarrollar e implementar planes de respuesta a incidentes** con roles y responsabilidades claramente definidos, realizando simulacros tipo Table Top y ejercicios de Ransomware. Deben incluir validación de protocolos de comunicación.
- **Alinear planes de respuesta con la estrategia organizacional,** asegurando coordinación entre departamentos, continuidad operativa y comunicación con stakeholders externos.
- **Integrar sistema SIEM configurado con reglas de correlación específicas** para la infraestructura, permitiendo detección y gestión de incidentes en tiempo real. Las reglas deben adaptarse a las necesidades y contexto único de la organización.

Seguridad en la nube y en Infraestructuras Críticas

1. Seguridad perimetral y configuraciones seguras

Utilizar firewalls y sistemas de detección de intrusos (IDS/IPS) para monitorear el tráfico hacia y desde las instancias en la nube y bloquear accesos no autorizados.

- **Asegurarse de que los buckets y otros recursos estén correctamente configurados** para evitar la exposición de información sensible.
- **Las configuraciones incorrectas, como permisos excesivos o falta de cifrado,** están entre las principales causas de incidentes en la nube.

2. Gestión de Identidad y Acceso (IAM) en la nube

Definir grupos y roles, para que la administración de identidades y accesos (IAM) garantice a cada usuario los permisos adecuados para sus responsabilidades.

- **Monitorear el uso de recursos y auditar configuraciones regularmente** para evitar desviaciones y detectar posibles amenazas.
- **Aplicar principios de mínimo privilegio y políticas Just-In-Time (JIT)** para reducir riesgos en la asignación de permisos temporales.

3. Convergencia IT/OT y estrategias de seguridad

Las redes segmentadas y controles de acceso estrictos protegen las tecnologías operativas (OT) y el monitoreo permite detectar comportamientos anómalos.

- **La coordinación entre los equipos de IT y OT es esencial** para implementar controles de seguridad adecuados sin afectar la operatividad de los sistemas industriales.
- **Implementar protocolos seguros como OPC UA y gateways** diferenciados para segmentar el tráfico entre IT y OT, reduciendo la exposición a ataques.

4. Redundancia y Resiliencia de Infraestructuras Críticas

Implementar mecanismos de redundancia en Infraestructuras Críticas, con sistemas de respaldo a nivel de hardware y software, así como configuración de failover.

- **La resiliencia debe ser un aspecto clave en el diseño de Infraestructuras Críticas,** incorporando capacidades de recuperación rápida y continuidad del negocio.

5. Monitoreo y Evaluación Continua

Establecer un monitoreo constante de las infraestructuras y servicios en la nube para identificar configuraciones inseguras y actividades sospechosas.

- **Utilizar herramientas de seguridad específicas para la nube, como CSPM,** para asegurar configuraciones y estándares de seguridad.
- **Más del 60% de los incidentes en la nube se deben a errores de configuración,** lo que resalta la importancia del monitoreo y la evaluación.

6. Vigilancia y seguridad de aplicaciones y sistemas operativos obsoletos

Supervisar de cerca y asegurar aplicaciones y sistemas operativos obsoletos que aún sustentan el núcleo de negocio de las organizaciones.

- **Tomar precauciones en sectores como el bancario o gubernamental,** donde sistemas core están escritos en lenguajes de programación que se vuelven obsoletos.
- **Aunque estos sistemas son críticos, su falta de soporte y actualizaciones** los hace vulnerables a ciberataques y se les debe prestar especial atención.

Capacitación y conciencia en ciberseguridad

1. Concientización y protección del entorno personal y profesional

Separar identidades profesional/personal y proteger usuarios VIP/VAP con capacitación específica contra ingeniería social y exposición en redes.

- **Implementar Application Whitelisting y prohibir el uso de software no confiable que pueda contener tanto Malware como Infostealer.** Eliminar credenciales codificadas expuestas en repositorios.
- **Establecer programas de concientización sobre ingeniería social e implementar MFA,** especialmente en entornos cloud, para prevenir ataques de fuerza bruta.

2. Capacitación continua y simulaciones de ataques

Realizar simulaciones y ejercicios de respuesta a incidentes para mejorar la reacción ante ataques reales, de forma periódica.

- **Además, se debe medir la efectividad de las respuestas** y proporcionar retroalimentación personalizada a los empleados.
- **Es necesario hacer simulaciones efectivas de Phishing,** que sigue siendo una de las principales amenazas a la que se enfrentan las organizaciones.

3. Seguridad física y digital combinada

Conectarse únicamente a redes confiables e implementar normativas y estándares que garanticen la seguridad, incluyendo VPN.

- **Implementar autenticación multifactor que combine biometría,** tarjetas de acceso y contraseñas robustas, así como tokens de hardware.
- **Crear redes aisladas para dispositivos externos y controlar conexiones** con Network Access Control (NAC).
- **Definir políticas y estándares de seguridad para el uso de dispositivos externos.** Evaluarlos con MDM antes de conectarse a la red.
- **Evitar que se conecten equipos con la función compartir internet de dispositivos móviles,** pues puede saltarse medidas de seguridad.

4. Fomento de una cultura de seguridad

Capacitación continua, con simulaciones y escenarios prácticos, en temas como gestión segura de contraseñas, protección de datos sensibles y detección de amenazas comunes.

- **Promover que cada empleado entienda su responsabilidad en la seguridad digital** y el manejo de datos sensibles, mediante capacitación y guías claras.

Capítulo

09.

CONCLUSIONES

Transcurrido el 2024, el cibercrimen organizado creció un 30%, impulsado por el uso de IA y plataformas automatizadas de Ransomware-as-a-Service (RaaS).

Los hallazgos más críticos

El panorama de ciberseguridad en 2024 evidenció un aumento en la sofisticación y frecuencia de los ciberataques, afectando sectores críticos en todo el mundo y particularmente en Latinoamérica. Las principales amenazas incluyeron:

El Ransomware

Los ataques a infraestructuras en la nube

El uso de inteligencia artificial (IA) para automatizar y perfeccionar estrategias maliciosas

Estas continúan evolucionando a nivel global, impulsadas por la creciente digitalización e interconectividad, integrando ataques sofisticados y hasta campañas de ciberespionaje respaldadas por estados. Esto subraya la creciente profesionalización del cibercrimen, que se apoya en mercados de la Deep y Dark Web para adquirir herramientas y datos sensibles.

En Latinoamérica, el panorama es igualmente alarmante, ya que los cibercriminales aprovechan brechas de seguridad en Infraestructuras Críticas y una baja madurez en ciberseguridad en algunos sectores. La región ha visto un aumento en ataques dirigidos a entidades financieras, gubernamentales, medianas y pequeñas empresas, que suelen carecer de recursos para implementar medidas robustas de defensa.

El Ransomware impactó especialmente a sectores como Gobierno, Salud y Energía, evidenciando la vulnerabilidad en la región. Además, los Grupos de Amenaza Persistente Avanzada (APT), respaldados por estados o financiados por redes criminales, se enfocaron en infiltraciones sigilosas para realizar espionaje o sabotaje estratégico.

Por otro lado, la infraestructura en la nube y los servicios SaaS fueron objetivos frecuentes, debido a configuraciones deficientes y al uso inadecuado de credenciales. La dependencia de estas tecnologías y los avances de estas amenazas hacen necesario un enfoque integral en ciberseguridad.

La evolución de las Tácticas, Técnicas y Procedimientos (TTPs) refleja un nivel creciente de profesionalización entre los atacantes. Las campañas actuales combinan ingeniería social avanzada, el uso de IA para personalizar ataques y herramientas automatizadas que explotan vulnerabilidades a una velocidad sin precedentes.

En este contexto, los dispositivos IoT y móviles representan un desafío particular, ampliando la superficie de ataque y exponiendo redes críticas a vulnerabilidades que pueden ser explotadas masivamente. Ataques como botnets IoT, infecciones en dispositivos y el uso de aplicaciones falsas están en aumento.

Proyecciones para 2025 y futuro

Estas son algunas de las aristas a tener en cuenta para el futuro:

Aumento en ataques avanzados y personalizados:

- **El acceso a datos masivos y herramientas de IA** impulsarán ataques a sectores como Energía, Transporte y Salud.
- **Las redes 5G y las aplicaciones basadas en IA** podrían ser vectores de nuevos tipos de ataques.

Evolución de los ataques:

- **Se espera el crecimiento de ataques** que cifran datos y destruyan sistemas críticos.
- **Con ello, logran ejercer mayor presión** sobre las víctimas.

Ataques políticos:

- **En un mundo políticamente polarizado,** se proyecta un incremento en ataques dirigidos por motivos ideológicos o geopolíticos.
- Estos ataques pondrán especial foco **en sectores gubernamentales y estratégicos.**

Uso de IA:

- Atacantes la utilizarán para **diseñar ataques personalizados y automatizados.**
- Las empresas la adoptarán para **identificar patrones anómalos y responder proactivamente.**

Dispositivos IoT:

- **Su proliferación impulsará ataques más sofisticados,** aprovechando la conectividad interdependiente.
- Las industrias deberán invertir en **estándares de seguridad más estrictos.**

Políticas de seguridad:

- **Los países con mayores recursos implementarán políticas y alianzas** internacionales para resguardarse.
- Las regiones con menos capacidad **seguirán siendo blanco fácil.**

Marcos unificados:

- **Gobiernos y organismos internacionales** priorizarán la creación de marcos legales unificados.
- **Así podrán enfrentar amenazas transnacionales,** con medidas más severas.

Organizaciones y gobiernos deben priorizar inversiones en tecnologías avanzadas, promover la educación en ciberseguridad y fomentar colaboraciones internacionales para proteger Infraestructuras Críticas y datos sensibles. Las empresas que integren prácticas proactivas de ciberdefensa no solo minimizarán riesgos, sino que se posicionarán como líderes en un mercado cada vez más digital y competitivo.

Recomendaciones generales de ciberseguridad

Para no permitir que las amenazas se fortalezcan, se proponen las siguientes medidas:

1. Educar a los usuarios

- Buenas prácticas de ciberseguridad y cómo identificar ataques de ingeniería social.

2. Priorizar la protección de activos críticos

- Mediante la evaluación constante de vulnerabilidades.

3. Integrar soluciones de Inteligencia Artificial

- Para detectar y responder a amenazas en tiempo real.

4. Configurar correctamente dispositivos IoT

- Deshabilitar funciones innecesarias y usar herramientas de gestión de seguridad en dispositivos móviles.

5. Utilizar dispositivos de seguridad

- Firewalls, sistemas de detección y prevención de intrusos (IDS/IPS), herramientas de monitoreo de red y soluciones de endpoint.

6. Actualizar todo el software y hardware

- Poner al día, con los últimos parches de seguridad.

7. Fomentar alianzas entre países y organizaciones

- Para compartir información de inteligencia sobre amenazas en LATAM.

Es crucial reconocer que ningún sistema o dispositivo de seguridad puede garantizar una protección completa contra todos los ataques. Las sofisticadas tácticas de los atacantes están en constante evolución y pueden pasar desapercibidas incluso para las tecnologías más modernas.

Lo más efectivo será generar un sistema holístico de protección, con foco tanto en las herramientas como en los usuarios.

Palabras finales del Director del Centro de Ciberinteligencia

La ciberseguridad en Latinoamérica enfrenta retos sin precedentes debido a la creciente sofisticación y volumen de amenazas cibernéticas. En 2024, fuimos testigos de un alarmante aumento en los ataques de ransomware, la explotación de vulnerabilidades y el uso de inteligencia artificial (IA) por parte de actores maliciosos.

Este panorama exige que las organizaciones, los gobiernos y los sectores críticos adopten un enfoque proactivo, fundamentado en inteligencia de amenazas, gestión eficiente de vulnerabilidades e inversión estratégica en tecnologías de protección.

Es crucial pasar de un enfoque reactivo a uno preventivo, destacando la necesidad de adaptarse rápidamente al acelerado crecimiento de las amenazas cibernéticas. Las caídas de servicios y los ciberataques representan un riesgo creciente para todo tipo de organizaciones. Aunque la tecnología digital ha ampliado su alcance y complejidad, también las ha hecho más vulnerables.

Diferentes sectores son víctimas de los ataques dirigidos por ciberdelincuentes. Infraestructuras críticas y la cadena de suministro, como sus principales objetivos, deben trabajar en mejorar su madurez respecto a la ciberresiliencia. Este reto es especialmente difícil para las pequeñas y medianas empresas (PYMES), que carecen de los recursos necesarios para defenderse, lo que las convierte en objetivos atractivos para los ciberdelincuentes.

La adopción de la inteligencia artificial sigue en aumento, tanto para las empresas como para los actores maliciosos. En 2024, las campañas de phishing fueron dirigidas contra varias empresas, centrándose en sectores críticos como telecomunicaciones y tecnología. Esto resalta la importancia de implementar procesos seguros para la adopción de IA, con el objetivo de proteger la información confidencial y mitigar los riesgos asociados con su uso.

En nuestra quinta edición del informe anual de ciberinteligencia, hemos trabajado para ofrecer un análisis exhaustivo de las tendencias y amenazas actuales en la región.

Algunos hallazgos destacados incluyen:

Ransomware en aumento: Los ataques crecieron un 38% a nivel LATAM en 2024, alcanzando 4,429 incidentes. Variantes como LockBit 3.0 y CLOP continúan dominando este panorama.

Explotación de vulnerabilidades: En 2023 se documentaron 28,831 vulnerabilidades, incluyendo 88 casos de día cero explotados, un aumento del 43% respecto al año anterior.

Uso de malware: Los ladrones de información representaron el 21% de las ofertas relacionadas con malware, seguidos por los troyanos de acceso remoto (RAT).

La ciberseguridad ya no puede ser tratada como un esfuerzo reactivo. Es vital invertir en inteligencia de amenazas, fomentar una cultura organizacional que priorice la seguridad digital y adoptar una gestión proactiva de vulnerabilidades. La construcción de una ciberresiliencia efectiva no solo protege a las grandes empresas, sino que también asegura la estabilidad operativa de las PYMES y la confianza de los ciudadanos en un mundo digital cada vez más interconectado.

El conocimiento, como enfatizamos en nuestro equipo del Centro de Ciberinteligencia, es nuestra mejor defensa. Al enfrentar los desafíos del futuro digital, debemos actuar de manera conjunta y decidida para proteger nuestro presente y construir un futuro más seguro.

Sobre los autores

Autores

Cyril Delaere
Gerente Servicios
Ciberseguridad Entel Digital

Eduardo Bouillet Carroza
Director del Centro de
Ciberinteligencia

Jonathan Armijo Catalán
Especialista Senior Operación
Ciberinteligencia

Equipo Ciberinteligencia 2024-2025

- **Juan P. Domínguez González**
  Jefe de Área Ciberinteligencia
- **Joaquín Miranda Gajardo**
  Especialista Operación
  Ciberinteligencia
- **Ernesto Lavanderos Saavedra**
  Especialista Operación
  Ciberinteligencia
- **Marco Arancibia Ocampo**
  Ingeniero Operación
  Ciberinteligencia
- **Lorena Pérez Contreras**
  Ingeniero Operación
  Ciberinteligencia
- **Esteban Andrade Andrade**
  Ingeniero Operación
  Ciberinteligencia

Juntos, tu empresa evoluciona