Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Marzo - 2025

Sobre Axus

Axus es una empresa especializada en ciberseguridad, con presencia en el Perú y Latinoamérica. Asesora a clientes en la protección de su información e infraestructura tanto en ámbitos industriales (OT) como en ámbitos corporativos (IT) y viene registrando una creciente participación en el ámbito de Internet de las Cosas (IoT) y en la protección de entornos Cloud e Híbridos.

En base a su reputación como especialista con los principales fabricantes de la industria y su equipo profesional en permanente capacitación, Axus genera valor a través de una visión consultiva que busca definir soluciones a la medida de las necesidades de cada cliente.

Alertas de Ciberseguridad

A continuación, compartimos con ustedes algunas de las alertas más relevantes de Marzo.

Alertas de Seguridad IT:

- El ransomware Albabat ataca Windows, Linux y macOS mediante GitHub Abuse.
- Hackers de Blind Eagle ataca organizaciones con archivos .url armados.
- Hackean los datos de El Corte Inglés, Legálitas y CCOO: filtran 570GB de información a la dark web.
- Hospital Madroños sufre ciberataque de la banda de ransomware Qilin.

Alertas de Seguridad OT/ICS:

- Hackers chinos de Volt Typhoon permanecieron en la red eléctrica de EE.UU. durante 300 días.
- Vulnerabilidades permiten el hackeo remoto de cámaras de monitoreo de plantas de Inaba.
- Vulnerabilidades críticas encontradas en el 99% de las redes de atención médica.

El ransomware Albabat ataca Windows, Linux y macOS mediante GitHub Abuse

Tipo de Ataque: Ransomware

Medio de Propagación: Correo electrónico, redes sociales, entre otros.

1. **PRODUCTOS AFECTADOS:**
   - Sistemas operativos Windows, Linux y macOS

2. **RESUMEN:**

Una investigación reciente de Trend Micro ha descubierto una evolución significativa en el ransomware Albabat, que ahora ataca no solo a sistemas Windows sino también Linux y macOS. Esta expansión resalta la creciente sofisticación de los grupos de ransomware a la hora de explotar múltiples sistemas operativos para maximizar su impacto. El grupo Albabat ha estado aprovechando GitHub para optimizar sus operaciones, utilizando la plataforma para administrar archivos de configuración y componentes esenciales del ransomware.

3. **DETALLE:**

Las últimas versiones del ransomware Albabat, específicamente las versiones 2.0.0 y 2.5, han sido diseñadas para recopilar información del sistema y del hardware de dispositivos Linux y macOS, además de Windows. Estas versiones recuperan sus datos de configuración a través de la API REST de GitHub, utilizando una cadena "User-Agent" denominada "Awesome App". Según el informe de Trend Micro, esta configuración proporciona detalles cruciales sobre el comportamiento y los parámetros operativos del ransomware, lo que indica un enfoque sofisticado para gestionar y actualizar el malware. El uso de GitHub permite a los atacantes mantener un control centralizado sobre la configuración del ransomware, lo que facilita la actualización y adaptación de sus tácticas. El ransomware cifra una amplia gama de extensiones de archivos, incluidos formatos comunes como .exe, .lnk, .dll, y .mp3, mientras omite carpetas y archivos específicos para evitar la detección o interferencia con las operaciones del sistema. También finaliza varios procesos, como administradores de tareas y software de productividad, para evitar que los usuarios interfieran con sus actividades. Los atacantes almacenan los datos robados en una base de datos PostgreSQL, lo que les ayuda a rastrear infecciones, monitorear pagos y potencialmente vender información confidencial. La capacidad del ransomware Albabat de atacar múltiples sistemas operativos y su uso de GitHub para lograr eficiencia operativa subrayan la necesidad de contar con medidas sólidas de ciberseguridad.

4. **RECOMENDACIONES:**
   - Priorizar controles de acceso sólidos, actualizaciones periódicas del sistema y copias de seguridad seguras para mitigar el riesgo de este tipo de ataques.
   - Configurar la segmentación de la red para limitar la propagación de ransomware, mientras que los programas de capacitación y concientización de los usuarios pueden ayudar a prevenir infecciones iniciales.

- Implementar soluciones de seguridad proactiva, como las plataformas impulsadas por IA, para brindar protección integral al predecir y prevenir amenazas, reduciendo así el riesgo de ataques de ransomware.
- Mantenerse informado sobre los indicadores de compromiso (IoC) y aprovechar la inteligencia sobre amenazas son cruciales para mantener defensas de ciberseguridad efectivas contra amenazas emergentes como Albabat.

5. REFERENCIAS:

- https://cdn.www.gob.pe/uploads/document/file/7814612/6594607-alerta-integrada-de-seguridad-digital-067-2025-cnsd.pdf?v=1742598645

Hackers de Blind Eagle ataca organizaciones con archivos .url armados

Tipo de Ataque: **Robo de credenciales (NTLM Relay)**

Medio de Propagación: **Correo electrónico, redes sociales, entre otros.**

1. **PRODUCTOS AFECTADOS:**
   - Organizaciones en América del Sur (instituciones financieras, agencias gubernamentales, organizaciones de manufactura)
2. **RESUMEN:**

El grupo de hackers conocido como Blind Eagle (también rastreado como APT-C-36) ha lanzado una campaña sofisticada que utiliza archivos .url armados para extraer hashes de autenticación de usuarios. Este método combina ingeniería social con explotación técnica para comprometer redes corporativas y acceder a información sensible. Los ataques comienzan con correos electrónicos de spear-phishing que contienen archivos .url aparentemente inocuo

3. **DETALLE**

Cuando se abre el archivo .url, se inicia una conexión a un servidor remoto controlado por los atacantes, forzando al sistema de la víctima a autenticar y transmitir hashes de autenticación NTLM. Este ataque ha sido refinado por Blind Eagle para evadir las medidas de seguridad comunes y evitar la detección por herramientas de seguridad convencionales. Los archivos .url armados contienen código diseñado para asegurar que el sistema de la víctima intente autenticarse con un servidor SMB controlado por los atacantes. Los atacantes capturan estos hashes utilizando herramientas como “Responder”.

4. **RECOMENDACIONES:**
   - Priorizar controles de acceso sólidos, actualizaciones periódicas del sistema y copias de seguridad seguras para mitigar el riesgo de este tipo de ataques.
   - Configurar la segmentación de la red para limitar la propagación de ransomware, mientras que los programas de capacitación y concientización de los usuarios pueden ayudar a prevenir infecciones iniciales.
   - Implementar soluciones de seguridad proactiva, como las plataformas impulsadas por IA, para brindar protección integral al predecir y prevenir amenazas, reduciendo así el riesgo de ataques de ransomware.
   - Mantenerse informado sobre los indicadores de compromiso (IoC) y aprovechar la inteligencia sobre amenazas son cruciales para mantener defensas de ciberseguridad efectivas contra amenazas emergentes como Blind Eagle.

5. **REFERENCIAS:**
   - https://cybersecuritynews.com/blind-eagle-attacking-organizations-with-weaponized-url-files/

Hackean los datos de El Corte Inglés, Legálitas y CCOO: filtran 570GB de información a la dark web

Tipo de Ataque: **Exposición de Datos**

Medio de Propagación: **Explotación de vulnerabilidades en servidores o credenciales comprometidas.**

1. **PRODUCTOS AFECTADOS:**
   - Sistemas de gestión de datos de El Corte Inglés
   - Plataformas de asesoramiento jurídico de Legálitas
   - Sistemas de gestión de información de Comisiones Obreras (CCOO)

2. **RESUMEN:**

El grupo de ciberdelincuentes Hunters International ha llevado a cabo una serie de ataques dirigidos a entidades españolas, incluyendo El Corte Inglés, Legálitas y el sindicato Comisiones Obreras (CCOO). En el caso de CCOO, lograron acceder a 570 GB de información sensible, amenazando con su publicación si no se cumplían sus demandas. Al no recibir el rescate solicitado, los atacantes filtraron la información en la dark web el 3 de marzo de 2025.

3. **DETALLE**

El ataque a CCOO resultó en el acceso a 689,764 archivos que abarcan diversas áreas, como personal, finanzas, gabinete jurídico y negociación colectiva. Aunque no se especificaron los métodos exactos de intrusión, se sabe que Hunters International se especializa en la exfiltración de datos antes de cifrarlos, lo que les permite extorsionar a las víctimas bajo la amenaza de divulgar la información robada. Al no recibir el dinero reclamado, el grupo publicó toda la información extraída el 3 de marzo. Este ataque no es el primero sufrido por CCOO, ya que en 2023 también fueron víctimas de una filtración de credenciales de 6,000 usuarios.

4. **RECOMENDACIONES:**
   - Priorizar controles de acceso sólidos, actualizaciones periódicas del sistema y copias de seguridad seguras para mitigar el riesgo de este tipo de ataques.
   - Configurar la segmentación de la red para limitar la propagación de ransomware, mientras que los programas de capacitación y concientización de los usuarios pueden ayudar a prevenir infecciones iniciales.
   - Implementar soluciones de seguridad proactiva, como las plataformas impulsadas por IA, para brindar protección integral al predecir y prevenir amenazas, reduciendo así el riesgo de ataques de ransomware.
   - Mantenerse informado sobre los indicadores de compromiso (IoC) y aprovechar la inteligencia sobre amenazas son cruciales para mantener defensas de ciberseguridad efectivas contra amenazas emergentes como Hunters International.

5. **REFERENCIAS:**
   - https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiH0q-

92bSMAxXXmbAFHZtMBQIQFnoECBkQAQ&url=https%3A%2F%2Fwww.infobae.com%2Fespana%2F2025%2F03%2F03%2Fhackean-los-datos-de-el-corte-ingles-legalitas-y-ccoo-filtran-570gb-de-informacion-a-la-dark-web%2F&usg=AOvVaw3Gm3zrlmm0RlV-8YIRGPyO&opi=89978449

Hospital Madroños sufre ciberataque de la banda de ransomware Qilin

Tipo de Ataque: Ransomware

Medio de Propagación: Acceso remoto no seguro

1. **PRODUCTOS AFECTADOS:**
   - Sistemas de gestión hospitalaria del Hospital Madroños
2. **RESUMEN:**

El Hospital Los Madroños, especializado en neurorrehabilitación, sufrió un ciberataque perpetrado por la banda de ransomware Qilin. Los atacantes afirman haber obtenido 540 GB de datos y más de 21,000 archivos del centro. Tras intentar negociar sin éxito con la institución, publicaron la información en la dark web el 17 de marzo de 2025.

3. **DETALLE**

El 7 de marzo de 2025, el hospital detectó una violación de seguridad en sus sistemas, resultando en el cifrado de datos y la extracción no autorizada de información sensible. Los datos comprometidos incluyen:

- **Empleados:** DNI, datos académicos y de formación, información laboral y números de cuenta bancaria.
- **Proveedores:** Datos identificativos (nombre, apellidos, contacto), en algunos casos DNI/NIF, y detalles bancarios.
- **Pacientes:** Nombre, documento de identidad, fecha de nacimiento, domicilio, contacto y datos del historial clínico.

El hospital activó su protocolo de respuesta, desconectó los sistemas afectados y notificó a las autoridades pertinentes, incluyendo la Agencia Española de Protección de Datos y las Fuerzas y Cuerpos de Seguridad del Estado.

4. **RECOMENDACIONES:**
   - Priorizar controles de acceso sólidos, actualizaciones periódicas del sistema y copias de seguridad seguras para mitigar el riesgo de este tipo de ataques.
   - Configurar la segmentación de la red para limitar la propagación de ransomware, mientras que los programas de capacitación y concientización de los usuarios pueden ayudar a prevenir infecciones iniciales.
   - Implementar soluciones de seguridad proactiva para brindar protección integral al predecir y prevenir amenazas, reduciendo así el riesgo de ataques de ransomware.
   - Mantenerse informado sobre los indicadores de compromiso (IoC) y aprovechar la inteligencia sobre amenazas son cruciales para mantener defensas de ciberseguridad efectivas contra amenazas emergentes como Qilin.

5. REFERENCIAS:

- https://www.lavanguardia.com/sociedad/20250320/10502272/hospital-madronos-sufre-ciberataque-banda-ransomware-qilin-agenciaslv20250320.html

Hackers chinos de Volt Typhoon permanecieron en la red eléctrica de EE.UU. durante 300 días

Tipo de Ataque: Ciberespionaje

Medio de Propagación: Explotación de vulnerabilidades en sistemas de control industrial (ICS)

1. **PRODUCTOS AFECTADOS:**
   - Red eléctrica de la Littleton ElectricLigh and Water Department (LELWD)
2. **RESUMEN:**

El grupo de hackers chinos conocido como Volt Typhoon logró infiltrarse y permanecer sin ser detectado en la red eléctrica de la Littleton Electric Light and Water Department (LELWD) en Massachusetts durante más de 300 días. Este ataque ha puesto de manifiesto las vulnerabilidades en la infraestructura crítica de EE.UU. y ha generado preocupación entre los expertos en ciberseguridad.

3. **DETALLE:**

La intrusión fue descubierta en noviembre de 2023 mientras LELWD implementaba soluciones de seguridad para tecnología operativa (OT). Se determinó que los hackers habían tenido acceso a la red desde febrero de 2023, recopilando datos críticos de los sistemas de control industrial (ICS) sin ser detectados. La investigación reveló que el grupo Volt Typhoon, también conocido como VOLTZITE, utilizó técnicas avanzadas para evadir las medidas de seguridad y mantener su presencia en la red1. Este incidente ha acelerado la implementación de soluciones de ciberseguridad en LELWD y ha resaltado la necesidad de mejorar la seguridad en la infraestructura crítica nacional.

4. **RECOMENDACIONES:**
   - Priorizar controles de acceso sólidos, actualizaciones periódicas del sistema y copias de seguridad seguras para mitigar el riesgo de este tipo de ataques.
   - Configurar la segmentación de la red para limitar la propagación de malware, mientras que los programas de capacitación y concientización de los usuarios pueden ayudar a prevenir infecciones iniciales.
   - Implementar soluciones de seguridad proactiva, como las plataformas impulsadas por IA, para brindar protección integral al predecir y prevenir amenazas, reduciendo así el riesgo de ciberespionaje.
   - Mantenerse informado sobre los indicadores de compromiso (IoC) y aprovechar la inteligencia sobre amenazas son cruciales para mantener defensas de ciberseguridad efectivas contra amenazas emergentes como Volt Typhoon.

5. **REFERENCIAS:**

- https://www.securityweek.com/chinas-volt-typhoon-hackers-dwelled-in-us-electric-grid-for-300-days/

Vulnerabilidades permiten el hackeo remoto de cámaras de monitoreo de plantas de Inaba

Tipo de Ataque: Exposición de Vulnerabilidades

Medio de Propagación: Explotación de vulnerabilidades en cámaras de monitoreo de plantas de Inaba.

1. PRODUCTOS AFECTADOS:

- Cámaras de monitoreo de plantas de Inaba

2. RESUMEN:

Se han descubierto múltiples vulnerabilidades en las cámaras de monitoreo de plantas fabricadas por Inaba, que permiten a los atacantes remotos acceder y controlar estas cámaras sin autorización. Estas vulnerabilidades exponen a las plantas industriales a riesgos significativos de espionaje y sabotaje

3. DETALLE:

Las vulnerabilidades fueron identificadas por investigadores de seguridad y permiten a los atacantes ejecutar código de forma remota, acceder a las transmisiones de video en tiempo real y manipular las configuraciones de las cámaras. Los atacantes pueden explotar estas fallas para obtener acceso no autorizado a las redes de las plantas industriales, lo que podría resultar en la interrupción de operaciones críticas y la exposición de información sensible. Aunque no se especificaron los métodos exactos de explotación, se sabe que las vulnerabilidades afectan a varias versiones de las cámaras de monitoreo de Inaba. La empresa ha sido notificada y se espera que emita parches de seguridad para mitigar estos riesgos.

4. RECOMENDACIONES:

- Priorizar la actualización de firmware y la aplicación de parches de seguridad proporcionados por el fabricante para mitigar el riesgo de explotación de estas vulnerabilidades.
- Implementar controles de acceso sólidos y segmentación de la red para limitar el acceso no autorizado a las cámaras de monitoreo.
- Configurar alertas de seguridad para detectar actividades sospechosas y responder rápidamente a posibles incidentes.
- Realizar auditorías de seguridad periódicas para identificar y corregir posibles vulnerabilidades en los sistemas de monitoreo.

5. REFERENCIAS:

- https://www.securityweek.com/vulnerabilities-allow-remote-hacking-of-inaba-plant-monitoring-cameras/

Vulnerabilidades críticas encontradas en el 99% de las redes de atención médica

Tipo de Ataque: Exposición de Vulnerabilidades

Medio de Propagación: Acceso no autorizado a través de conexiones inseguras a Internet y explotación de vulnerabilidades conocidas en dispositivos IoMT y OT.

1. **PRODUCTOS AFECTADOS:**
   - Dispositivos IoMT (Internet de las Cosas Médicas)
   - Dispositivos OT (Tecnología Operativa)
2. **RESUMEN:**

Un informe de Claroty ha revelado que el 99% de las redes de atención médica contienen vulnerabilidades críticas que pueden ser explotadas por atacantes. Estas vulnerabilidades afectan tanto a dispositivos IoMT como OT, exponiendo a los hospitales y otras organizaciones de salud a riesgos significativos de ciberataques.

3. **DETALLE:**

Claroty analizó más de 2.25 millones de dispositivos IoMT y más de 647,000 dispositivos OT en 351 organizaciones de atención médica. Las vulnerabilidades detectadas incluyen:

- Requisitos débiles de contraseña: Permiten accesos no autorizados debido a la facilidad para adivinar o forzar las credenciales.
- Navegación forzada (Forced browsing): Posibilita que atacantes accedan a partes restringidas del sistema sin autenticación.
- Autenticación en el lado del cliente: Uso de métodos inseguros que pueden ser eludidos, otorgando acceso indebido.
- Almacenamiento inseguro de contraseñas: Las credenciales se guardan de manera que pueden ser recuperadas y explotadas por atacantes.

Un atacante que explote estas vulnerabilidades podría:

- Monitorear en secreto las transmisiones en vivo de video y audio, facilitando el espionaje industrial y comprometiendo la privacidad de los empleados.
- Manipular o eliminar grabaciones, lo que podría dificultar el análisis de incidentes y afectar la eficiencia operativa.

El informe destaca que el 20% de los sistemas de información hospitalaria que gestionan datos clínicos de pacientes, así como información administrativa y financiera, contienen vulnerabilidades conocidas explotadas (KEVs) vinculadas a ransomware y están inseguramente conectados a internet. Además, el 89% de estas organizaciones operan sistemas médicos susceptibles a exploits públicos, incluyendo aquellos utilizados por grupos de ransomware. Hasta la fecha, estas vulnerabilidades permanecen sin parchear, lo que aumenta el riesgo de explotación

4. RECOMENDACIONES:

- Priorizar la actualización de firmware y la aplicación de parches de seguridad proporcionados por el fabricante para mitigar el riesgo de explotación de estas vulnerabilidades.
- Implementar controles de acceso sólidos y segmentación de la red para limitar el acceso no autorizado a los dispositivos IoMT y OT.
- Configurar alertas de seguridad para detectar actividades sospechosas y responder rápidamente a posibles incidentes.
- Realizar auditorías de seguridad periódicas para identificar y corregir posibles vulnerabilidades en los sistemas de monitoreo.

5. REFERENCIAS:

- https://industrialcyber.co/reports/claroty-reports-alarming-iomt-ot-device-risks-as-critical-vulnerabilities-found-in-99-of-healthcare-networks/