Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Diciembre - 2024

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 septiembre.

Alertas de Seguridad IT:

- EE. UU. estudia prohibir los routers TP-Link por riesgos de ciberseguridad.
- Japan Airlines sufrió un ciberataque que retrasó sus vuelos durante la temporada de vacaciones de fin de año.
- Los piratas informáticos podrían haber robado datos personales del operador de cajeros automáticos de Bitcoin Byte Federal.

Alertas de Seguridad OT/ICS:

- Los piratas informáticos iraníes utilizan el malware IOCONTROL para atacar dispositivos OT e IoT en Estados Unidos e Israel.
- El contratista del sector energético ENGlobal es blanco de un ataque de ransomware.
- Se insta a las instalaciones de agua de EE. UU. a proteger el acceso a las HMI expuestas a Internet.

EE. UU. estudia prohibir los routers TP-Link por riesgos de ciberseguridad

Tipo de Ataque: **Riesgos de seguridad nacional por uso de enrutadores comprometidos.**

Medio de Propagación: **Enrutadores SOHO fabricados por TP-Link utilizados en ataques rociado de contraseñas.**

1. **PRODUCTOS AFECTADOS:**
   - Enrutadores TP-Link para pequeñas oficinas y oficinas domésticas (SOHO)
   - Dispositivos utilizados en redes de agencias gubernamentales como NASA, DEA y el Departamento de Defensa de EE. UU.

2. **RESUMEN:**

El gobierno de EE. UU. está investigando el uso de enrutadores TP-Link en ciberataques y considera su prohibición debido a riesgos para la seguridad nacional. Según informes, la botnet Quad7, compuesta mayoritariamente por dispositivos TP-Link comprometidos, esta vinculada a actores de amanezas chinos que realizan ataques de rociado de contraseñas. TP-Link posee el 65% del mercado estadounidense de enrutadores SOHO, con dispositivos presentes en más de 300 proveedores de Internet y redes gubernamentales. Además, la empresa es investigada por supuestamente vender enrutadores por debajo de su costo de fabricación, un posible factor en su expansión de mercado. La administración Biden también ha intensificado medidas contra otros fabricantes chinos relacionados con riesgo de ciberseguridad.

3. **DETALLE:**

La vulnerabilidad en los enrutadores TP-Link fue destacada tras un informe de Microsoft en octubre, que rastreó una red de bots utilizada en ataques de pulverización de contraseñas y otras actividades maliciosas. El Departamento de Justicia, Comercio y Defensa investiga si esta infraestructura representa un riesgo crítico para redes sensibles, incluyendo agencias gubernamentales. TP- Link ha respondido afirmando que está comprometido con las normativas de seguridad estadounidenses y dispuesto a colaborar en las investigaciones. Este incidente resalta preocupaciones más amplias sobre el uso de dispositivos tecnológicos chinos, que ya han llevado a prohibiciones previas de equipos Huawei ZTE y otras compañías por la FCC.

4. **RECOMENDACIONES:**
   - Sustituir enrutadores TP-Link en entornos sensibles o críticos por equipos certificados por agencias de ciberseguridad.
   - Implementar controles robustos de autenticación y monitoreo en redes que utilizan enrutadores SOHO.
   - Realizar auditorías periódicas de dispositivos en la infraestructura de red para detectar actividad sospechosa.
   - Colaborar con proveedores tecnológicos que cumplan estrictamente con estándares internacionales de ciberseguridad.

- Mantenerse actualizado sobre restricciones gubernamentales y cambios regulatorios relacionados con dispositivos tecnológicos extranjeros.

5. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/us-considers-banning-tp-link-routers-over-cybersecurity-risks/

Japan Airlines sufrió un ciberataque que retrasó sus vuelos durante la temporada de vacaciones de fin de año

Tipo de Ataque: **Ataque de denegación de servicio distribuido (DDoS).**

Medio de Propagación: **Sobrecarga de sistemas mediante transmisiones masivas de datos.**

1. **PRODUCTOS AFECTADOS:**
   - Sistemas internos y externos de red de Japan Airlines (JAL).
   - Servicio de emisión de boletos para vuelos nacionales e internacionales.

2. **RESUMEN:**

Japan Airlines enfrentó un ataque DDoS que provocó retrasos en 24 vuelos nacionales, afectando a miles de pasajeros durante la temporada alta de viajes de fin de año. El ataque, que saturó la red con tráfico masivo, no comprometió la seguridad de los vuelos ni la privacidad de los datos de los clientes. La aerolínea logró detener el ataque y restablecer sus sistemas en pocas horas. Este incidente subraya la creciente preocupación por las vulnerabilidades en la ciberseguridad en Japón, especialmente en un contexto de mayor colaboración internacional en defensa y ciberseguridad.

3. **DETALLE**

El ataque comenzó en la mañana del jueves, cuando las redes JAL comenzaron a fallar debido a la saturación de datos. Aunque no hubo filtración de datos ni instalación de malware, el ataque causó interrupciones significativas, con vuelos retrasados por mas de 30 minutos y la suspensión temporal de la venta de boletos. Las terminales del aeropuerto de Haneda en Tokio se llenaron de pasajeros afectados, muchos de ellos viajando por festividades de Año Nuevo. El incidente se suma a una serie de ciberataques recientes en Japón, incluyendo el de la agencia espacial japonesa en 2023 y el ataque que paralizó un puerto en Nagoya durante tres días.

4. **RECOMENDACIONES:**
   - Implementar soluciones avanzadas de mitigación de ataques DDoS, como sistemas de detección temprana y tráfico filtrado.
   - Establecer redundancia en los sistemas críticos para evitar la dependencia de una sola red en caso de ataque.
   - Realizar simulacros regulares de respuesta ante incidentes para minimizar el impacto en los servicios y operaciones.
   - Colaborar con organismos internacionales y expertos en ciberseguridad para reforzar la defensa de infraestructuras críticas.
   - Fortalecer las medidas de seguridad en periodos de alta demanda, como la temporada de festividades, para reducir la vulnerabilidad ante ataques dirigidos.

5. **REFERENCIAS:**
   - https://www.securityweek.com/japan-airlines-was-hit-by-a-cyberattack-delaying-flights-during-the-year-end-holiday-season/

Los piratas informáticos podrían haber robado datos personales del operador de cajeros automáticos de Bitcoin Byte Federal

Tipo de Ataque: **Violación de datos a través de una explotación de vulnerabilidad Gitlab.**

Medio de Propagación: **Acceso no autorizado a servidores mediante la explotación de fallos de seguridad.**

1. **PRODUCTOS AFECTADOS:**
   - Plataforma de cajeros automáticos de Bitcoin de Byte Federal.
   - Información personal de 58,000 usuarios.

2. **RESUMEN:**

Byte Federal, un importante operador de cajeros automáticos de Bitcoin, notificó a 58,000 personas sobre una posible violación de datos tras un ataque descubierto el 18 de noviembre. Los atacantes explotaron una vulnerabilidad en GitLab para acceder a uno de sus servidores. Aunque no se comprometieron fondos ni activos de usuarios, el incidente puede haber expuesto información personal como nombres, direcciones y números de seguro social. BYTE Federal ha tomado medidas preventivas, incluyendo el cierre de su plataforma y la actualización de contraseñas, y continúa investigando el alcance del ataque.

3. **DETALLE:**

El ataque permitió a los actores de amenazas acceder a información sensible, aunque la compañía no ha encontrado evidencia de uso indebido de los datos hasta el momento. Byte Federal ha restablecido todas las cuentas de clientes y actualizado su sistema de gestión de contraseñas. La empresa ha instado a los usuarios a monitorear sus estados de cuenta para detectar actividades sospechosas y a considerar medidas como alertas de fraude. La notificación a la Oficina del Fiscal General de Maine refleja la seriedad del incidente.

4. **RECOMENDACIONES:**

   - Implementar medidas de seguridad robustas para proteger la infraestructura de IT, incluyendo auditorías regulares de vulnerabilidades.
   - Informar a los usuarios sobre las mejores prácticas en la gestión de sus datos personales y la importancia de la seguridad en línea.
   - Ofrecer servicios de monitoreo de crédito y protección contra robo de identidad para los usuarios afectados.
   - Colaborar con expertos en ciberseguridad para mejorar las defensas contra futuras amenazas.
   - Mantener una comunicación transparente con los usuarios sobre el estado de la investigación y las medidas tomadas para prevenir incidentes similares en el futuro.

5. REFERENCIAS:

- https://www.securityweek.com/hackers-possibly-stole-personal-data-from-bitcoin-atm-operator-byte-federal/

Los piratas informáticos iraníes utilizan el malware IOCONTROL para atacar dispositivos OT e IoT en Estados Unidos e Israel

Tipo de Ataque: Ataques cibernéticos a infraestructura crítica mediante malware personalizado.

Medio de Propagación: Malware IOCONTROL dirigido a dispositivos IoT y OT vulnerables.

1. **PRODUCTOS AFECTADOS:**
   - Dispositivos IoT y OT, incluidos cámaras IP, enrutadores, sistemas SCADA, PLC, HMI y firewalls
   - Soluciones para estaciones de servicio de Orpak Systems y sistemas de control de combustible Gasboy.

2. **RESUMEN:**

CyberAv3ngers, un grupo de hackers vinculado al Cuerpo de la Guardia Revolucionaría Islámica de Irán, ha utilizado el malware IOCONTROL para atacar infraestructuras críticas en EE. UU. e Israel. Estos ataques han impactado sistemas de control industrial (ICS) y dispositivos IoT, generando interrupciones significativas como el corte del suministro de agua en Irlanda durante dos días y la inhabilitación de surtidores de gasolina en Israel. IOCONTROL utiliza el protocolo MQTT para comunicaciones de comando y control (C&C) y es capaz de ejecutar código remoto y realizar movimientos laterales en redes comprometidas. Loa ataques explotan dispositivos protegidos con credenciales predeterminadas y expuestos a Internet, subrayando la importancia de medidas de seguridad robustas en infraestructura crítica.

3. **DETALLE:**

El malware IOCONTROL está diseñado específicamente para dispositivos basados en Linux y permite adaptar su funcionalidad según el sistema objetivo. Los atacantes emplearon esta herramienta para comprometer dispositivos de múltiples proveedores como D-Link, Hikvision y Phoenix Contact. En octubre 2023, CyberAv3ngers interrumpió operaciones en 200 surtidores de gasolina en Israel, utilizando dispositivos vinculados con Orpak Systems. Claroty, la firma de ciberseguridad que analizó el malware, señala que las campañas del grupo se intensificaron nuevamente en julio y agosto de 2024. Este incidente destaca como las organizaciones que no protegen adecuadamente sus dispositivos ICS e IoT se convierten en objetivos fáciles para actores maliciosos.

4. **RECOMENDACIONES:**

- Asegurar que todos los dispositivos IoT y OT cuenten con configuraciones personalizadas y credenciales robustas, eliminando las predeterminadas de fábrica.
- Implementar firewalls y sistemas de detección de intrusos para proteger redes que incluyen sistemas ICS y OT.
- Realizar auditorías periódicas de dispositivos conectados a Internet para identificar posibles vulnerabilidades.
- Capacitar al personal en la detección y respuesta ante ataques dirigidos a dispositivos IoT y OT.

- Establecer protocolos de segmentación de redes para minimizar el impacto de movimientos laterales en caso de una intrusión.

5. REFERENCIAS:

- https://www.securityweek.com/iranian-hackers-use-iocontrol-malware-to-target-ot-iot-devices-in-us-israel/

El contratista del sector energético ENGlobal es blanco de un ataque de ransomware.

Tipo de Ataque: Ataque de Ransomware

Medio de Propagación: Acceso no autorizado al sistema de tecnología de la información (TI)

1. **PRODUCTOS AFECTADOS:**
   - Sistemas de TI en ENGblobal Corporation
   - Operaciones comerciales esenciales

2. RESUMEN:

ENGlobal Corporation anunció que algunas de sus operaciones fueron atacadas por un ataque de Ransomware descubierto el 25 de noviembre. La compañía desconectó ciertos sistemas para contener el incidente. Aunque la investigación preliminar indica que se accedió ilegalmente a su red y se cifraron archivos, ENGlobal no ha determinado aún si el ataque afectará materialmente su situación financiera. Los esfuerzos de recuperación están en curso, pero no se ha proporcionado una estimación para el restablecimiento completo de los sistemas.

3. DETALLE:

Tras detectar el acceso no autorizado, ENGlobal tomó medidas inmediatas, incluyendo la contención del incidente, la evaluación de los daños y la contratación de especialistas externos en ciberseguridad. Actualmente, solo se permite el acceso a operaciones comerciales esenciales. La empresa no ha ofrecido detalles sobre si se robaron datos durante el ataque ni ha identificado al grupo de ransomware responsable. ENGlobal con sede en Houston, Texas, ofrece servicios de ingeniería y profesionales, principalmente para el sector energético y agencias gubernamentales en EE. UU. y en el extranjero.

4. **RECOMENDACIONES:**
   - Implementar medidas de seguridad más robustas para proteger sistemas críticos.
   - Realizar auditorías regulares de seguridad cibernética.
   - Capacitar al personal en la identificación y respuesta a posibles amenazas.
   - Establecer un plan de respuesta a incidentes que incluya protocolos claros para la contención y recuperación.
   - Colaborar con expertos de ciberseguridad para mejorar las defensas contra ataques ransomware.

5. REFERENCIAS:

- https://www.securityweek.com/energy-sector-contractor-englobal-targeted-in-ransomware-attack/

Se insta a las instalaciones de agua de EE. UU. a proteger el acceso a las HMI expuestas a Internet.

Tipo de Ataque: Amenazas cibernéticas a sistemas de agua y aguas residuales.

Medio de Propagación: Acceso no autorizado a interfaces hombre – máquina (HMI).

1. **PRODUCTOS AFECTADOS:**
   - Sistemas de control industrial (ICS) en instalaciones de agua y aguas residuales.
   - Interfaces hombre – máquina (HMI) que permiten la supervisión y control remoto.

2. **RESUMEN:**

El Gobierno de Estados Unidos está instando a las organizaciones del sector de agua y aguas residuales a proteger adecuadamente las HMI expuestas a Internet. Estas interfaces, si no están adecuadamente aseguradas, pueden ser vulnerables a accesos no autorizados que podrían manipular sistemas críticos. En 2024, se reportó que hackers prorrusos lograron manipular HMI, alterando parámetros operativos y deshabilitando alarmas, lo que forzó a las instalaciones a operar manualmente. La Agencia de Protección Ambiental (EPA) y la Agencia de ciberseguridad CISA han emitido recomendaciones para mitigar estos riesgos.

3. **DETALLE:**

La advertencia del gobierno se centra en la creciente amenaza de las interfaces hombre – máquina (HMI) que permiten el control remoto de sistemas de agua y aguas residuales. Los ataques recientes han demostrado que los hackers pueden manipular configuraciones y desactivar controles, lo que afecta la operación normal de estos sistemas. Se insta a las organizaciones a realizar un inventario de dispositivos expuestos y a implementar medidas de seguridad robustas, como las de autenticación multifactor. También se enfatiza la importancia de utilizar recursos gubernamentales disponibles para fortalecer la ciberseguridad, dado que varios sistemas de agua potable en EE. UU. enfrentan riesgos significativos.

4. **RECOMENDACIONES:**
   - Asegurar las HMI con nombres de usuario y contraseñas robustas.
   - Implementar autenticación multifactor para todas las HMI y la red OT.
   - Mantener los sistemas y aplicaciones actualizados.
   - Realizar un registro de inicios de sesión remotos en las HMI.
   - Seguir las recomendaciones de los proveedores para la protección de los productos.
   - Aprovechar recursos gubernamentales para mejorar la seguridad.

5. **REFERENCIAS:**
   - https://www.securityweek.com/us-water-facilities-urged-to-secure-access-to-internet-exposed-hmis/