Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Junio - 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 Junio.

Alertas de Seguridad IT:

- Ahold Delhaize, empresa del sector retail alimentario, sufre brecha de datos que afecta a 2.2 millones de personas
- UNFI, empresa mayorista de alimentos, restablece sistemas tras ciberataque que afectó operaciones clave
- FBI alerta sobre ciberdelincuentes que roban datos de salud haciéndose pasar por investigadores de fraude

Alertas de Seguridad OT/ICS:

- Ramnit, malware vinculado a la ciberseguridad industrial, incrementa sus infecciones en entornos OT, con indicios de orientación hacia sistemas ICS
- Interfaces HMI mal configuradas exponen sistemas de agua en EE. UU. a cualquiera con un navegador
- 35,000 sistemas solares expuestos a internet, vulnerables a ataques remotos

Ahold Delhaize, , empresa del sector retail alimentario, sufre brecha de datos que afecta a 2.2 millones de personas

Tipo de Ataque: Ransomware

Medio de Propagación: Acceso a sistemas internos

1. **PRODUCTOS AFECTADOS:**
   - Sistemas internos de Ahold Delhaize USA
   - Registros de empleo e información financiera y de salud

2. **RESUMEN:**

Ahold Delhaize, uno de los mayores minoristas de alimentos del mundo, ha confirmado que un ataque de ransomware ocurrido en noviembre de 2024 comprometió la información personal, financiera y médica de más de 2.2 millones de personas en Estados Unidos. El incidente afectó a varias marcas del grupo, incluyendo farmacias y operaciones de comercio electrónico. Aunque la empresa no ha confirmado públicamente al grupo responsable, INC Ransom se atribuyó el ataque y filtró documentos en su portal de extorsión. La información robada incluye desde datos de contacto y números de identificación hasta registros médicos y bancarios. Ahold Delhaize asegura que no hay evidencia de que los sistemas de pago o de farmacia de clientes hayan sido comprometidos

3. **DETALLE:**

El 6 de noviembre de 2024, Ahold Delhaize fue víctima de un ataque de ransomware que comprometió sus sistemas internos en Estados Unidos. La intrusión permitió a los atacantes acceder y robar información sensible de más de 2.2 millones de personas. Los datos sustraídos incluyen nombres, direcciones, fechas de nacimiento, números de identificación (como pasaportes y licencias de conducir), información bancaria, registros médicos y detalles laborales.

Aunque la empresa no ha confirmado públicamente al grupo responsable, el colectivo de ransomware INC Ransom se atribuyó el ataque y publicó muestras de los documentos robados en su portal de extorsión en la dark web. Ahold Delhaize ha evitado comentar si hubo cifrado de sistemas o si se estableció contacto con los atacantes para negociar un rescate.

La compañía aclaró que no hay evidencia de que los sistemas de pago o de farmacia de clientes hayan sido comprometidos, y que no se encontraron números de tarjetas de crédito en los archivos afectados. Sin embargo, el incidente sí impactó a varias marcas estadounidenses del grupo, incluyendo farmacias y plataformas de comercio electrónico.

4. **RECOMENDACIONES:**
   - Supervisar cuentas bancarias y reportar actividades sospechosas
   - Activar monitoreo de identidad y protección contra robo de datos personales

5. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/security/retail-giant-ahold-delhaize-says-data-breach-affects-22-million-people/

UNFI, empresa mayorista de alimentos, restablece sistemas tras ciberataque que afectó operaciones clave

Tipo de Ataque: **Ciberataque no especificado, posiblemente ransomware**

Medio de Propagación: **Acceso a sistemas internos**

1. **PRODUCTOS AFECTADOS:**
   - Sistemas centrales de UNFI
   - Plataformas de pedidos electrónicos
   - Sistemas de facturación

2. **RESUMEN:**

United Natural Foods Inc. (UNFI), proveedor mayorista de Whole Foods y otras cadenas de supermercados en EE. UU., sufrió un ciberataque que interrumpió sus sistemas principales, incluyendo pedidos y facturación. La empresa ha logrado restaurar sus operaciones clave tras varios días de interrupciones.

3. **DETALLE**

El ataque, ocurrido en junio de 2025, afectó los sistemas centrales de UNFI, lo que obligó a la compañía a operar manualmente durante varios días. Esto impactó directamente la capacidad de procesar pedidos y emitir facturas electrónicas, afectando a clientes y socios comerciales. Aunque UNFI no ha confirmado públicamente la naturaleza exacta del ataque ni si se trató de ransomware, la interrupción fue significativa. La empresa activó sus protocolos de respuesta a incidentes, trabajó con expertos en ciberseguridad y notificó a las autoridades correspondientes. Tras una semana de esfuerzos, UNFI anunció que sus sistemas principales ya han sido restaurados y están plenamente operativos.

4. **RECOMENDACIONES:**
   - Reforzar medidas de ciberseguridad en proveedores críticos
   - Implementar planes de contingencia para continuidad operativa ante incidentes.

5. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/security/whole-foods-supplier-unfi-restores-core-systems-after-cyberattack/

FBI alerta sobre ciberdelincuentes que roban datos de salud haciéndose pasar por investigadores de fraude

Tipo de Ataque: Ingeniería social
Medio de Propagación: Llamadas telefónicas y correos electrónicos fraudulentos

1. **PRODUCTOS AFECTADOS:**
   - Información médica personal
   - Datos de identificación (nombres, fechas de nacimiento, números de seguro social)
   - Registros de salud protegidos (PHI)
2. **RESUMEN:**

El FBI ha emitido una advertencia sobre una campaña de fraude en la que ciberdelincuentes se hacen pasar por investigadores de fraude en salud para engañar a víctimas y obtener acceso a su información médica y personal sensible.

3. **DETALLE:**

Según el FBI, los atacantes contactan a las víctimas por teléfono o correo electrónico, haciéndose pasar por representantes de aseguradoras médicas, agencias gubernamentales o investigadores de fraude. Utilizan tácticas de presión y lenguaje técnico para convencer a las personas de que deben proporcionar información confidencial para resolver supuestos casos de fraude. En algunos casos, los atacantes incluso solicitan acceso remoto a dispositivos o enlaces a formularios falsos. Esta campaña representa una amenaza significativa para la privacidad de los datos de salud y puede derivar en robo de identidad, fraude financiero y exposición de información médica protegida.

4. **RECOMENDACIONES:**
   - Verificar siempre la identidad de quien solicita información médica o personal
   - No compartir datos sensibles por teléfono o correo electrónico sin confirmar la legitimidad del contacto

5. **RECOMENDACIONES:**

   - https://www.bleepingcomputer.com/news/security/fbi-warns-cybercriminals-steal-health-data-posing-as-fraud-investigators/

Ramnit, malware vinculado a la ciberseguridad industrial, incrementa sus infecciones en entornos OT, con indicios de orientación hacia sistemas ICS

Tipo de Ataque: Malware bancario con capacidades de robo de credenciales

Medio de Propagación: Descargas maliciosas, correos electrónicos de phishing, y explotación de vulnerabilidades

1. PRODUCTOS AFECTADOS:

- Sistemas de Tecnología Operativa (OT)
- Credenciales de acceso a sistemas de control industrial (ICS)
- Infraestructura crítica industrial

2. RESUMEN:

El malware Ramnit, históricamente asociado con el robo de credenciales bancarias, ha experimentado un repunte significativo en entornos de Tecnología Operativa (OT), lo que sugiere un cambio preocupante hacia objetivos industriales y sistemas de control (ICS).

3. DETALLE:

Según un informe de Honeywell, Ramnit pasó de no registrar infecciones en el primer trimestre de 2024 a convertirse en la amenaza más detectada en entornos OT en el segundo trimestre. Este cambio sugiere que los operadores del malware podrían estar adaptando sus tácticas para apuntar a credenciales utilizadas en sistemas industriales. Ramnit es conocido por su capacidad de propagarse a través de medios extraíbles, redes comprometidas y correos electrónicos maliciosos, y por su habilidad para robar información sensible. El informe destaca que este tipo de malware representa una amenaza creciente para la seguridad de infraestructuras críticas, ya que comprometer credenciales ICS puede permitir el acceso a sistemas que controlan procesos físicos en plantas industriales.

4. RECOMENDACIONES:

- Restringir el uso de dispositivos USB y medios extraíbles en entornos OT
- Implementar segmentación de red entre sistemas IT y OT
- Fortalecer la autenticación y monitoreo de accesos a sistemas ICS

5. REFERENCIAS:

- https://www.securityweek.com/ramnit-malware-infections-spike-in-ot-as-evidence-suggests-ics-shift/

Interfaces HMI mal configuradas exponen sistemas de agua en EE. UU. a cualquiera con un navegador

Tipo de Ataque: Exposición involuntaria / Configuración insegura

Medio de Propagación: Acceso directo vía navegador web

1. PRODUCTOS AFECTADOS:

- Interfaces Hombre-Máquina (HMI)
- Sistemas de control de plantas de tratamiento de agua
- Paneles de control de bombas, válvulas y dosificación química

2. RESUMEN:

Investigadores de seguridad descubrieron que cientos de paneles de control de sistemas de agua en EE. UU. estaban expuestos públicamente en internet debido a configuraciones incorrectas, permitiendo acceso sin contraseña a funciones críticas como bombas y válvulas.

3. DETALLE:

Un error en un certificado TLS llevó a investigadores a descubrir que múltiples interfaces HMI utilizadas por plantas de tratamiento de agua en EE. UU. estaban accesibles desde cualquier navegador, sin autenticación. Estas interfaces permiten controlar directamente operaciones como el flujo de agua, la dosificación de químicos y el monitoreo de sensores. En algunos casos, los paneles ofrecían control total sin requerir credenciales. Esta exposición representa un riesgo crítico para la infraestructura de agua potable, ya que podría ser explotada por actores maliciosos para alterar procesos físicos esenciales. La situación pone en evidencia la falta de controles básicos de ciberseguridad en sistemas industriales conectados a internet.

4. RECOMENDACIONES:

- Asegurar todas las interfaces HMI con autenticación robusta
- Eliminar el acceso público a sistemas de control industrial mediante segmentación de red y VPNs

5. REFERENCIAS:

- https://www.securityweek.com/misconfigured-hmis-expose-us-water-systems-to-anyone-with-a-browser/

35,000 sistemas solares expuestos a internet, vulnerables a ataques remotos

Tipo de Ataque: Exposición por mala configuración / Riesgo de acceso remoto no autorizado

Medio de Propagación: Acceso directo vía internet sin autenticación

6. PRODUCTOS AFECTADOS:

- Sistemas de energía solar conectados a internet
- Interfaces web de monitoreo y control
- Inversores solares y plataformas de gestión remota

7. RESUMEN:

Una investigación de la firma de ciberseguridad Forescout reveló que más de 35,000 sistemas solares en todo el mundo están expuestos públicamente a internet, lo que los hace vulnerables a accesos no autorizados y posibles ciberataques.

8. DETALLE:

El análisis identificó decenas de miles de sistemas solares accesibles sin autenticación, muchos de ellos con interfaces de administración web abiertas. Estos sistemas incluyen inversores solares y plataformas de monitoreo que permiten controlar la producción de energía, el almacenamiento y la conexión a la red. La mayoría de los dispositivos expuestos se encuentran en EE. UU., Alemania, Brasil y Australia. La exposición de estos sistemas no solo representa un riesgo para la privacidad y la seguridad energética individual, sino que también podría ser explotada en ataques a gran escala contra infraestructuras críticas. Forescout advirtió que algunos dispositivos incluso permiten cambios de configuración remota sin requerir credenciales.

9. RECOMENDACIONES:

- Restringir el acceso remoto a sistemas solares mediante firewalls y VPNs
- Cambiar credenciales predeterminadas y aplicar autenticación robusta en interfaces web

10. REFERENCIAS:

- https://www.securityweek.com/35000-solar-power-systems-exposed-to-internet/