Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Febrero - 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 Febrero.

Alertas de Seguridad IT:

- Robo de Tarjetas de Crédito en la Tienda Online de Casio UK
- Ransomware a Blue Yonder Impacta Cadenas de Suministro
- Trabajadores de TI norcoreanos se infiltran en empresas internacionales con identidades falsas

Alertas de Seguridad OT/ICS:

- Siemens y Schneider Electric abordan vulnerabilidades críticas en sus sistemas
- Hackers chinos atacan organizaciones industriales con el sofisticado FatalRAT
- Southern Water pierde £4.5M tras devastador ataque de ransomware de Black Basta

Robo de Tarjetas de Crédito en la Tienda Online de Casio UK

Tipo de Ataque: **Exposición de datos sensibles.**

Medio de Propagación: **Bases de dato**

1. **PRODUCTOS AFECTADOS:**
   - Información personal de clientes y Datos de tarjetas de crédito

2. **RESUMEN:**

Casio UK sufrió una vulneración en su tienda en línea mediante la inyección de un script malicioso diseñado para capturar la información de pago de sus clientes. Este ataque fue detectado el 28 de enero de 2025 por la firma de ciberseguridad JSCrambler, la cual notificó a la empresa para que tomara medidas inmediatas.

El método de ataque se basó en la explotación de vulnerabilidades en la plataforma de comercio electrónico Magento, permitiendo la inyección de código malicioso en el proceso de pago. Este skimmer interceptaba los datos ingresados por los clientes en un formulario fraudulento antes de redirigirlos al proceso de pago legítimo. Los datos capturados eran cifrados mediante el algoritmo AES-256-CBC y posteriormente enviados a servidores bajo control de los atacantes con direcciones IP registradas en Rusia.

Casio contaba con una política de seguridad de contenido (CSP) para restringir la ejecución de scripts maliciosos, sin embargo, su configuración estaba en modo de solo reporte, lo que permitía registrar los intentos de ataque sin bloquearlos de manera efectiva.

3. **DETALLE:**

El ataque consistió en dos fases principales. En la primera fase, los atacantes inyectaron un script malicioso en el código del sitio web de Casio UK, el cual cargaba dinámicamente un segundo script alojado en un servidor en Rusia. Este segundo script utilizaba técnicas avanzadas de ofuscación, como la codificación personalizada y el uso de cadenas encriptadas mediante XOR, lo que dificultaba su detección por herramientas de seguridad.

En la segunda fase, el skimmer se activaba en el proceso de pago cuando un usuario agregaba productos al carrito. En lugar de ser dirigido al formulario de pago legítimo de Casio, se desplegaba un formulario falso con el mismo propósito. Este formulario capturaba en tiempo real la información ingresada por el cliente y la transmitía a los servidores de los atacantes. Para evitar sospechas, después de capturar los datos, se mostraba un mensaje de error falso antes de redirigir al usuario a la pasarela de pago legítima, permitiendo que la compra se realizara con normalidad.

La información capturada, incluyendo los datos completos de la tarjeta de crédito, era encriptada utilizando el algoritmo AES-256-CBC antes de ser enviada a servidores ubicados en Rusia.

Este ataque expuso la deficiente configuración de seguridad en el sitio de Casio UK. A pesar de contar con una política de seguridad de contenido (CSP), esta estaba configurada en modo de solo reporte y sin una directiva de notificación, lo que permitió que los intentos de ejecución del script malicioso quedaran únicamente registrados en la consola del navegador, sin que se bloquearan de manera efectiva.

4. RECOMENDACIONES:

- Utilizar Sistemas de Detección de Intrusos (IDS) para monitorear tráfico web en busca de patrones de ataque.
- Implementar escaneo regular de código fuente y scripts activos para detectar modificaciones no autorizadas.
- Activar HTTP Strict Transport Security (HSTS) para forzar conexiones seguras y evitar ataques de intermediarios.
- Restringir la ejecución de código y modificaciones de configuración a un grupo limitado de administradores.

5. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/casio-uk-online-store-hacked-to-steal-customer-credit-cards/

Ransomware a Blue Yonder Impacta Cadenas de Suministro

Tipo de Ataque: Ransomware

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   - Blue Yonder
2. **RESUMEN:**

El proveedor de software de gestión de cadenas de suministro, Blue Yonder, sufrió un ataque de ransomware que ha causado interrupciones significativas en los servicios de varias empresas. Entre los afectados se encuentran Starbucks, que ha experimentado problemas con el pago de salarios y la gestión de turnos de empleados, así como los supermercados Morrisons y Sainsbury's en el Reino Unido, que han visto afectadas sus operaciones logísticas y la disponibilidad de productos.

El incidente fue detectado el 21 de noviembre de 2024, cuando Blue Yonder informó sobre interrupciones en su entorno de servicios gestionados. La compañía inició una investigación y comenzó el proceso de restauración de los servicios, aunque hasta el 24 de noviembre no había estimaciones claras sobre la recuperación total del sistema.

Hasta el momento, ningún grupo de ransomware ha reivindicado el ataque. Sin embargo, es común que los ciberdelincuentes solo revelen su autoría si las negociaciones de pago con la empresa fallan.

3. **DETALLE**

Blue Yonder es un proveedor global de soluciones de software para la gestión de cadenas de suministro con más de 3,000 clientes en 76 países. Sus servicios son utilizados por importantes compañías de retail, manufactura y logística, lo que hace que un ataque de esta magnitud tenga un impacto significativo en múltiples industrias.

El ransomware comprometió la infraestructura en la nube donde se alojan los servicios gestionados de Blue Yonder. Como resultado, empresas como Morrisons han tenido que recurrir a sistemas manuales de respaldo para la gestión de almacenes y logística, afectando la entrega de productos desde los proveedores.

Starbucks, por su parte, ha informado que el incidente ha afectado la administración de turnos y pagos de sus empleados, lo que ha generado problemas operativos. Mientras tanto, Sainsbury's ha reconocido la afectación, aunque asegura contar con medidas de mitigación para reducir el impacto.

Se desconoce el vector exacto del ataque, pero es probable que los atacantes hayan explotado vulnerabilidades en la infraestructura de Blue Yonder o utilizado credenciales comprometidas para infiltrarse en sus sistemas.

4. **RECOMENDACIONES:**
   - Aplicar controles de acceso estrictos con autenticación multifactor (MFA) para todas las cuentas administrativas.
   - Implementar segmentación de red para aislar servicios críticos y limitar el impacto de una intrusión.
   - Usar cifrado de datos en tránsito y en reposo para proteger información sensible contra exfiltración.
   - Evaluar regularmente la **postura de seguridad de proveedores de software** y exigir certificaciones de seguridad.
5. **REFERENCIAS:**
   - https://www.securityweek.com/starbucks-grocery-stores-hit-by-blue-yonder-ransomware-attack/

Trabajadores de TI norcoreanos se infiltran en empresas internacionales con identidades falsas

Tipo de Ataque: Ingeniería social, ataque de malware

Medio de Propagación: Plataformas de empleo remoto, paquetes NPM, empresas ficticias

1. **AFECTADOS:**
   - Empresas de tecnología, criptomonedas, desarrollo de software

2. **RESUMEN:**

Trabajadores de TI de Corea del Norte han logrado infiltrarse en empresas internacionales obteniendo empleos remotos con identidades falsas. Esta táctica no solo viola las sanciones internacionales, sino que también plantea riesgos significativos de ciberseguridad, incluyendo el robo de datos y la instalación de puertas traseras en sistemas comprometidos.

El Insikt Group ha revelado estas actividades, destacando el uso de malware sofisticado y empresas fachada para evadir la detección. El régimen de Corea del Norte ha adaptado sus actividades ilícitas, incluyendo el cibercrimen, en respuesta a las sanciones más estrictas.

El aumento del trabajo remoto ha proporcionado nuevas oportunidades para que los trabajadores de TI norcoreanos obtengan empleo en empresas globales, a menudo utilizando perfiles fraudulentos y empresas fachada. Los expertos del Insikt Group descubrieron que estos operativos están vinculados a campañas maliciosas que apuntan a industrias dependientes de la propiedad intelectual. Entre las herramientas maliciosas identificadas están **BeaverTail**, **InvisibleFerret** y **OtterCookie**, las cuales permiten robar información y establecer accesos no autorizados a los sistemas de las empresas.

3. **DETALLE**

El Insikt Group ha identificado varias familias de malware utilizadas por estos operativos, incluyendo:

- **BeaverTail**: Un infostealer de JavaScript que recopila información sensible como detalles de billeteras de criptomonedas. Se distribuye a través de paquetes NPM y apunta a entornos Windows y macOS.
- **InvisibleFerret**: Un backdoor multiplataforma en Python que introduce cargas maliciosas adicionales, realiza robo de información y utiliza protocolos legítimos para comunicaciones de comando y control (C2).
- **OtterCookie**: Un backdoor que establece conectividad C2 a través de Socket.IO, ejecuta comandos de shell y exfiltra datos sensibles.

Estas herramientas de malware a menudo se entregan a través de entrevistas de trabajo aparentemente legítimas o desafíos de codificación. Por ejemplo, un desarrollador informó que se le pidió descargar un archivo de desafío de codificación que contenía una función maliciosa, posteriormente identificada como un infostealer BeaverTail.

Corea del Norte opera una red de empresas fachada que imitan a firmas de TI legítimas. Estas entidades crean ofertas de trabajo falsas en plataformas como Telegram, GitHub y Upwork. Una de estas empresas, "AgencyHill99", fue encontrada publicando anuncios de trabajo en múltiples plataformas, incluyendo una posición de desarrollador de blockchain en levels.fyi. El sitio web de la empresa estaba registrado en Hostinger, pero ya no está activo.

4. RECOMENDACIONES:

- Implementar procesos robustos de verificación de identidad para contrataciones remotas, incluyendo entrevistas por video y documentos de identificación notariados.
- Establecer controles técnicos como monitoreo de amenazas internas, geolocalización de dispositivos y restricción de la exposición de datos.
- Capacitar y concienciar a los equipos de recursos humanos y seguridad de TI para prevenir la infiltración de estos actores en operaciones comerciales críticas.

La infiltración de trabajadores de TI norcoreanos en empresas internacionales plantea una doble amenaza de violaciones de sanciones y riesgos graves de ciberseguridad. A medida que el trabajo remoto continúa creciendo, es crucial que las organizaciones y los gobiernos colaboren en medidas de seguridad mejoradas y el intercambio de inteligencia para combatir esta amenaza en evolución.

5. REFERENCIAS:

- https://cybersecuritynews.com/north-korean-it-workers-infiltrate-international-companies/

Siemens y Schneider Electric abordan vulnerabilidades críticas en sus sistemas

Tipo de Ataque: Ejecución remota de código

Medio de Propagación: Explotación de vulnerabilidades en software

1. **PRODUCTOS AFECTADOS:**
   - FactoryTalk View
2. **RESUMEN:**

Los gigantes industriales Siemens y Schneider Electric han publicado sus boletines de seguridad de febrero de 2025, abordando múltiples vulnerabilidades críticas y de alta severidad en sus productos ICS/OT. Siemens ha identificado aproximadamente 100 vulnerabilidades, de las cuales 70 provienen de componentes de terceros en dispositivos Scalance W. Schneider Electric, por su parte, ha emitido cuatro avisos de seguridad para un total de nueve vulnerabilidades en su línea de productos.

3. **DETALLE:**

Siemens:

Siemens ha lanzado 14 nuevos avisos de seguridad, destacando dos vulnerabilidades críticas en Opcenter Intelligence que pueden permitir ejecución remota de código/comandos. Además, ha solucionado fallos en:

- Ruggedcom APE1808: 10 vulnerabilidades de severidad alta y media que afectan el firewall embebido basado en Fortinet FortiOS (parches en desarrollo).
- Siprotec 5: Riesgo de ejecución arbitraria de comandos y filtración de información sensible.
- Simatic y Sirius: Posible reutilización de tokens de sesión, lo que aumenta el riesgo de secuestro de sesión.
- Simatic S7-1200: Vulnerabilidad de denegación de servicio (DoS).
- Apogee PXC y Talon TC: Riesgo de descifrado de contraseñas almacenadas en los dispositivos.
- Simatic IPC: Posible escalamiento de privilegios en sistemas industriales.
- Teamcenter: Fallo de redirección abierta que podría ser explotado para ataques de phishing.

Schneider Electric:

La empresa ha abordado vulnerabilidades en varias de sus soluciones:

- ASCO Remote Annunciator: Cuatro fallos de alta severidad que pueden ser explotados para interrumpir operaciones y obtener información sensible.
- EcoStruxure: Un fallo de alta severidad que permite escalamiento de privilegios.
- EcoStruxure y Enerlin: Problemas de severidad media que pueden provocar ataques DoS.

4. RECOMENDACIONES:

- Aplicar los parches de seguridad tan pronto como estén disponibles.
- Segmentar redes OT e IT para limitar la exposición de sistemas industriales a amenazas externas.
- Monitorear actividad sospechosa en equipos como Simatic, Sirius y Siprotec

5. REFERENCIAS:

- https://www.securityweek.com/rockwell-patches-critical-high-severity-vulnerabilities-in-several-products/

Hackers chinos atacan organizaciones industriales con el sofisticado FatalRAT

Tipo de Ataque: Campaña de ciberespionaje con troyano de acceso remoto (RAT).

Medio de Propagación: Servicios en la nube chinos legítimos y correos electrónicos de phishing.

6. PRODUCTOS AFECTADOS:

- Servicios en la nube como Youdao Cloud Notes y Tencent Cloud (myqcloud).

7. RESUMEN:

Un informe de Kaspersky ICS CERT revela una campaña de ciberespionaje sofisticada que utiliza el troyano de acceso remoto FatalRAT para atacar organizaciones industriales en la región APAC incluyendo sectores de manufactura, energía, TI y logística en Taiwán, China, Japón, Tailandia y Singapur. Los atacantes, presuntamente actores de amenazas de habla china, emplean una cadena de infección en múltiples etapas que explota servicios en la nube chinos legítimos para entregar cargas útiles y evadir la detección. La campaña se dirige principalmente a los sectores de manufactura, energía, TI y logística en Taiwán, China, Japón, Tailandia y Singapur.

Los atacantes distribuyen correos electrónicos de phishing y mensajes a través de WeChat/Telegram, haciéndose pasar por documentos fiscales o facturas.

Los expertos en ciberseguridad de Kaspersky ICS CERT señalaron que estos archivos ZIP contienen cargadores de primera etapa empaquetados con AsProtect o UPX, que inician un proceso de infección complejo de siete pasos.

8. DETALLE:

La cadena de infección del malware comienza con un cargador que recupera configuraciones C2 actualizadas dinámicamente desde Youdao Cloud Notes a través de solicitudes HTTP a URLs como http://note.youdao[.]com/yws/api/note/4b2eead06fc72ee2763ef1f653cdc4ae. La respuesta JSON incluye enlaces cifrados a módulos secundarios como Before.dll (configurador) y Fangao.dll (cargador de segunda etapa), que se descifran utilizando claves XOR (0x58).

Fangao.dll despliega software legítimo como PureCodec y DriverAssistant para la carga lateral de DLL, inyectando bibliotecas maliciosas como wke.dll en la memoria. La carga final, FatalRAT (MD5: bcec6b78adb3cf966fab9025dacb0f05), realiza 17 comprobaciones anti-VM, incluyendo escaneos de registro para artefactos de VMware y verificación de configuraciones regionales chinas.

El RAT registra pulsaciones de teclas en C:\Windows\Fatal.key, exfiltra datos a través de canales C2 cifrados (1.12.37[.]113:8081) y permite la ejecución remota de comandos destructivos como la corrupción del MBR.

La telemetría de Kaspersky reveló estaciones de trabajo de ingeniería comprometidas, destacando los riesgos para los entornos de tecnología operativa (OT).

9. RECOMENDACIONES:

- Configurar adecuadamente los servicios en la nube expuestos a Internet, asegurando autenticación y restricciones de acceso.
- Implementar monitoreo continuo para detectar accesos no autorizados y exposiciones accidentales de datos.
- Segmentar las redes, monitorear la carga lateral de DLL (wke.dll) y bloquear IoCs como el dominio C2 fakaka16[.]top

10. REFERENCIAS:

- https://cybersecuritynews.com/hackers-attacking-industrial-organizations-with-fatalrat/

Southern Water pierde £4.5M tras devastador ataque de ransomware de Black Basta

Tipo de Ataque: Ransomware

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   - ABB
2. **RESUMEN:**

Southern Water, empresa proveedora de agua en el Reino Unido, sufrió un ataque de ransomware en febrero de 2024, atribuido al grupo Black Basta. La compañía reveló recientemente que el incidente tuvo un impacto financiero significativo, con costos de respuesta estimados en £4.5 millones ($5.7M). A pesar de que el ataque no interrumpió sus operaciones, sí resultó en el robo de datos de una parte de sus servidores.

El ataque fue reportado inicialmente como una "intrusión ilegal" en los sistemas de TI de Southern Water. Posteriormente, se confirmó que Black Basta había exigido un rescate de $3.5M por los datos robados. Sin embargo, informes filtrados sugieren que la empresa ofreció pagar £750,000 ($950k) en negociaciones privadas con los atacantes. Al final de febrero de 2024, la entrada de Southern Water fue eliminada del sitio de extorsión de Black Basta, lo que indica que podría haberse llegado a un acuerdo.

3. **DETALLE:**

Southern Water es responsable de proveer servicios de agua a 2.7 millones de personas y gestionar el saneamiento de más de 4.7 millones en Inglaterra. La empresa opera con una infraestructura extensa, transportando diariamente 570 millones de litros de agua a través de una red de 13,973 km y gestionando 1,522 millones de litros de aguas residuales mediante un sistema de alcantarillado de 40,058 km.

El ataque de ransomware dirigido a la empresa fue llevado a cabo por Black Basta, un grupo cibercriminal conocido por atacar infraestructuras críticas. Black Basta suele utilizar técnicas avanzadas para infiltrarse en redes empresariales, robar información sensible y exigir rescates millonarios a sus víctimas.

Southern Water asegura que no hubo impacto en sus sistemas operacionales ni en los servicios financieros o de atención al cliente. Sin embargo, el incidente generó preocupaciones sobre la posible exposición de datos personales, lo que llevó a la empresa a contratar expertos en ciberseguridad y asesores legales para gestionar la crisis.

El informe financiero de Southern Water, citado por DataBreaches.net, detalla que el ataque generó costos significativos, comparables a los gastos anuales en control de contaminación de la empresa. Además de la respuesta inmediata, la compañía continúa monitoreando la dark web en busca de filtraciones de datos.

.

4. RECOMENDACIONES:

- Implementar estrategias de segmentación de red para evitar la propagación de ransomware en infraestructuras críticas.
- Realizar auditorías de seguridad periódicas en todos los sistemas de TI para detectar vulnerabilidades antes de que sean explotadas.
- Monitoreo constante de la dark web para identificar posibles filtraciones de datos corporativos y de clientes.

5. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/southern-water-says-black-basta-ransomware-attack-cost-45m-in-expenses/