Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

Julio - 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 julio.

Alertas de Seguridad IT:

- Ataque de ransomware en Columbus, Ohio: Autoridades investigan posible robo de datos personales
- Brecha de datos en HealthEquity expone información personal y médica de 4.3 millones de personas
- Respuesta fallida de Microsoft a ataque DDoS provoca interrupción masiva en servicios de Azure
- Ciberataque a Leidos Holdings revela vulnerabilidades en la cadena de suministro de contratistas gubernamentales

Alertas de Seguridad OT/ICS:

- FrostyGoop: El nuevo malware ICS que dejó sin calefacción a una ciudad ucraniana
- Siemens advierte sobre vulnerabilidades críticas en productos SICAM: Urge actualización inmediata

Ataque de Ransomware en Columbus, Ohio: Autoridades investigan posible robo de datos personales

Tipo de Ataque: Ransomware

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   - Red Interna de la ciudad
2. **RESUMEN:**

La ciudad de Columbus, Ohio, está investigando un posible robo de datos personales tras un ataque de ransomware ocurrido el 18 de julio de 2024. El incidente causó interrupciones en los servicios públicos y afectó la conectividad entre agencias, aunque los servicios de emergencia continuaron operando normalmente. Las autoridades confirman que el ataque fue contenido rápidamente, sin que se cifraran sistemas, pero aún se evalúa el alcance total del impacto.

3. **DETALLE:**

El 18 de julio de 2024, la ciudad de Columbus, Ohio, sufrió un ataque de ransomware que interrumpió varios servicios municipales. Inicialmente, hubo confusión sobre si los cortes estaban relacionados con una actualización defectuosa de CrowdStrike Falcon. El alcalde Andrew J. Ginther confirmó el 23 de junio que se trataba de un incidente de ciberseguridad.

El ataque afectó los servicios de correo electrónico y la conectividad de TI entre agencias públicas, pero las líneas 911 y 311, así como todos los servicios de seguridad pública y emergencia, continuaron funcionando normalmente. Columbus, capital de Ohio, tiene una población metropolitana de 2,140,000 habitantes.

Las autoridades de la ciudad atribuyen el ataque a "un actor de amenazas establecido y sofisticado que opera en el extranjero", aunque no se proporcionaron nombres específicos de grupos de amenazas. La respuesta al incidente fue rápida, involucrando al FBI y al Departamento de Seguridad Nacional, lo que permitió contener la amenaza sin que se cifraran sistemas.

Sin embargo, aún se está evaluando el impacto total del ataque, y no se descarta la posibilidad de que se hayan robado datos de los ciudadanos. La ciudad está en proceso de identificar a las personas cuya información personal pudo haber sido expuesta y proporcionará notificaciones y orientación adicional a todos los afectados en las próximas semanas.

Según informes de Columbus Navigator, los hackers accedieron a la red interna de la ciudad después de que un empleado descargara un archivo ZIP de un sitio web. Se aconseja a los ciudadanos de Columbus que estén alerta ante posibles intentos de phishing o estafas que utilicen información robada.

Las autoridades de la ciudad esperan publicar una actualización en el próximo período para especificar si se han robado datos y, en caso afirmativo, notificar a los afectados.

4. **RECOMENDACIONES:**
   - Recomendaciones usuales para protegerse contra ataques de ransomware:
     - Capacitar al usuario para evitar vectores usuales de ataque como phishing, usbs infectados, páginas inseguras, etc.
     - Estrategia de backup acorde con las necesidades de disponibilidad de la información de la organización.
     - Sistema antimalware o XDR permanentemente actualizado.
     - Proceso de Gestión de respuesta a incidentes.

5. **REFERENCIAS:**
   - https://www.bleepingcomputer.com/news/security/columbus-investigates-whether-data-was-stolen-in-ransomware-attack/

Brecha de datos en HealthEquity expone información personal y médica de 4.3 millones de personas

Tipo de Ataque: Vulnerabilidad

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   Repositorio de datos en línea
2. **RESUMEN:**

HealthEquity ha notificado a 4.3 millones de personas que su información personal y de salud se vio comprometida en una violación de datos ocurrida en un proveedor externo. El incidente, identificado el 25 de marzo, involucró el acceso no autorizado a un repositorio de datos no estructurados fuera de los sistemas centrales de la empresa. La información expuesta puede incluir nombres, direcciones, números de Seguro Social, información de dependientes y datos de tarjetas de pago.

3. **DETALLE**

HealthEquity, una empresa de servicios de salud ha informado sobre una violación de datos que afecta a 4.3 millones de individuos. El incidente fue descubierto el 25 de marzo y requirió una "extensa investigación técnica", según un informe presentado ante la Oficina del Fiscal General de Maine.

La violación ocurrió cuando atacantes comprometieron las cuentas de usuario de un proveedor que tenía acceso a un repositorio de datos en línea, ganando así acceso a la información almacenada. La información comprometida incluye datos personales identificables (PII) y información de salud protegida (PHI).

Entre los datos potencialmente expuestos se encuentran:

- Nombres
- Direcciones
- Números de teléfono
- Números de Seguro Social
- ID de empleado
- Información del empleador
- Información de dependientes
- Información de tarjetas de pago

HealthEquity ha tomado medidas inmediatas para mitigar el riesgo, incluyendo:

- Desactivación de todas las cuentas de proveedores potencialmente comprometidas
- Terminación de todas las sesiones activas
- Bloqueo de direcciones IP asociadas con la actividad del atacante
- Implementación de un restablecimiento global de contraseñas para el proveedor afectado

La empresa comenzará a enviar cartas de notificación a las personas afectadas a partir del 9 de agosto. Además, HealthEquity está proporcionando dos años de servicios gratuitos de monitoreo de crédito, seguro y restauración de identidad a los afectados.

Aunque HealthEquity afirma no tener conocimiento de ningún uso indebido real o intentado de la información hasta la fecha, insta a los individuos afectados a monitorear sus cuentas en busca de actividades sospechosas.

4. RECOMENDACIONES:

- Gestionar el nivel de ciberseguridad de los proveedores que mantienen o acceden a nuestra información sensible.
- Asegurar que todo acceso a información en la nube, desde fuera de las oficinas, use autenticación de múltiples factores (MFA).

5. REFERENCIAS:

- https://www.securityweek.com/4-3-million-impacted-by-healthequity-data-breach/

Respuesta fallida de Microsoft a ataque DDoS provoca interrupción masiva en servicios de Azure

Tipo de Ataque: **Ataque DDoS: Ataque de denegación de servicio distribuido (Distributed Denial-of-Service, DDoS))**

Medio de Propagación: **Internet**

1. **RESUMEN:**

Microsoft ha informado que un reciente corte en los servicios de Azure fue causado por una respuesta defectuosa a un ataque de denegación de servicio distribuido (DDoS). La respuesta de Microsoft al ataque amplificó su impacto en lugar de mitigarlo, provocando interrupciones que afectaron a numerosos clientes durante aproximadamente 10 horas. El incidente impactó a diversos servicios de Azure, así como a algunas funciones de Microsoft 365 y Purview, afectando a empresas de servicios públicos, tribunales, bancos y otras organizaciones.

2. **DETALLE:**

Microsoft informó que un "subconjunto de clientes" experimentó problemas para conectarse a varios servicios de Azure, incluyendo Azure App Services, Application Insights, Azure IoT Central, Azure Log Search Alerts, Azure Policy, el portal de Azure y algunos servicios de Microsoft 365 y Purview.

La interrupción, que duró alrededor de 10 horas, afectó a una amplia gama de organizaciones, incluyendo servicios de agua, tribunales y bancos, según informó la BBC.

Inicialmente, Microsoft detectó un pico de uso inesperado que resultó en un rendimiento inferior al aceptable de los componentes Azure Front Door y Azure Content Delivery Network, lo que provocó errores, tiempos de espera y problemas de latencia.

Una investigación posterior reveló que un ataque DDoS contra los sistemas de Microsoft activó los mecanismos de protección. Sin embargo, debido a un error de implementación en estas defensas, el impacto del ataque se amplificó en lugar de mitigarse.

Microsoft se ha comprometido a publicar una revisión preliminar del incidente en un plazo de 72 horas y una revisión más detallada en dos semanas.

Aunque no está claro quién está detrás del ataque DDoS contra los servicios de Microsoft, no sería sorprendente que varios grupos hacktivistas se atribuyan la responsabilidad para aumentar su reputación.

Este incidente ocurre poco después de que millones de computadoras en todo el mundo se vieran afectadas por una actualización defectuosa distribuida por la empresa de ciberseguridad CrowdStrike. Aunque la mayoría de los dispositivos afectados por el incidente de CrowdStrike se restauraron en una semana, las aseguradoras prevén pérdidas millonarias para los principales clientes de la empresa de seguridad. Además, CrowdStrike se enfrenta a demandas por el incidente.

3. **RECOMENDACIONES**
   - Implementar una estrategia de multi-nube para reducir la dependencia de un único proveedor.
   - Implementar soluciones de protección DDoS en capas, incluyendo defensas en la red y aplicación.
   - Establecer acuerdos de nivel de servicio (SLAs) claros con proveedores de servicios en la nube.
   - Establecer planes de continuidad del negocio y recuperación ante desastres actualizados.
4. **REFERENCIAS:**

https://www.securityweek.com/microsoft-says-azure-outage-caused-by-ddos-attack-response/

Ciberataque a Leidos Holdings revela vulnerabilidades en la cadena de suministro de contratistas gubernamentales

Tipo de Ataque: Vulnerabilidades

Medio de Propagación: Internet

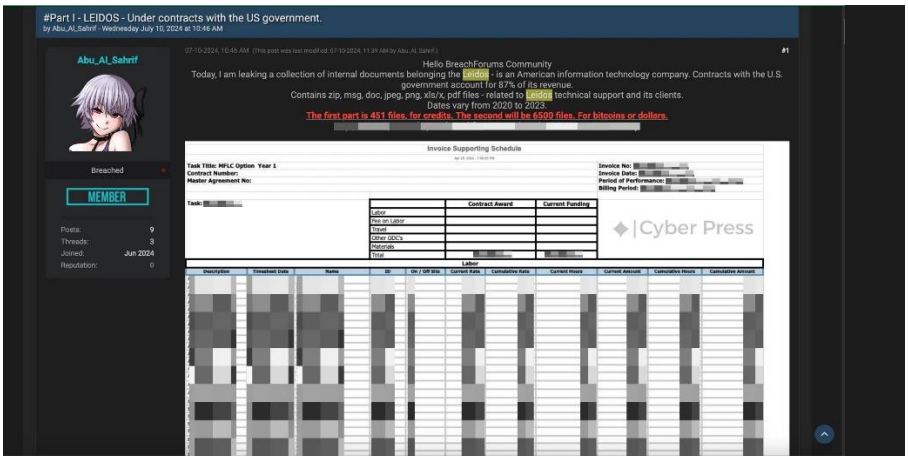
1. RESUMEN:

Investigadores de Cyber Press han descubierto una filtración masiva de documentos confidenciales de Leidos Holdings, uno de los principales proveedores de servicios de TI para agencias gubernamentales como el Pentágono, Seguridad Nacional y la NASA. Un grupo de hackers no identificado atacó a Leidos, resultando en la exposición pública de información confidencial de la empresa. La filtración, que contiene aproximadamente un gigabyte de datos diversos, ha sido puesta a la venta en foros de filtración de datos por $30,000.

2. DETALLE:

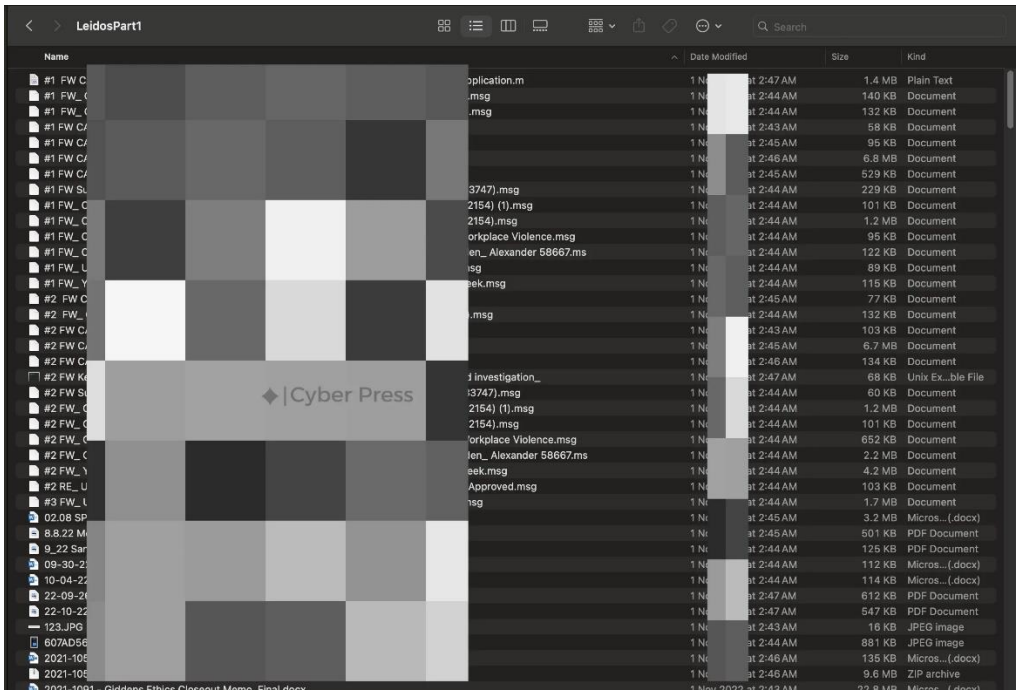
Leidos Holdings, una empresa estadounidense de tecnología de la información que sirve a sectores como seguridad nacional, defensa y salud, ha sido víctima de un ciberataque que resultó en la filtración de documentos internos confidenciales. La compañía obtiene el 87% de sus ingresos de contratos con el gobierno de los Estados Unidos.

Los investigadores de Cyber Press encontraron la filtración en un conocido foro de filtración de datos, publicada por un usuario llamado "Abu_Al_Sahrif", quien se sospecha se unió al foro en 2024 específicamente para filtrar los datos robados de Leidos.



Fuente: Cyberpress.org - Leaked data Samples

El conjunto de datos filtrados consta de aproximadamente un gigabyte de archivos en diversos formatos, incluyendo zip, msg, doc, jpg, png, xls/x y pdf. Estos archivos están relacionados con la asistencia técnica de Leidos y sus clientes. La filtración se divide en dos partes: la primera contiene 451 archivos relacionados con créditos, y la segunda incluye 6,500 archivos asociados con bitcoins o dólares.



Fuente: Cyberpress.org - Leaked files contains massive amount of data

Los hackers han puesto a la venta los datos filtrados por $30,000, indicando que el precio es negociable dependiendo del número de usuarios interesados. La misma información también se encontró en otro foro de filtración de datos bajo el nombre de usuario "Frog".

Según una fuente anónima, Leidos acaba de tomar conciencia del problema y sospecha que los registros robados formaban parte de una violación que involucró a un sistema de Diligent Corp., que la empresa había revelado previamente. Sin embargo, Leidos ha declarado que "este incidente no afectó nuestra red ni ningún dato sensible de los clientes".

Este incidente ha generado preocupaciones sobre el posible uso indebido de información sensible y ha desencadenado un debate más amplio sobre las normas y controles de seguridad que deben seguir los contratistas gubernamentales.

3. **RECOMENDACIONES**
   - Gestionar el nivel de ciberseguridad de los proveedores que mantienen o acceden a nuestra información sensible.
   - Asegurar que todo acceso a información en la nube, desde fuera de las oficinas, use autenticación de múltiples factores (MFA).
4. **REFERENCIAS:**

https://www.securityweek.com/microsoft-says-azure-outage-caused-by-ddos-attack-response/

FrostyGoop: El nuevo malware ICS que dejó sin calefacción a una ciudad ucraniana

Tipo de Ataque: Vulnerabilidades

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   - Dispositivo ICS
2. **RESUMEN:**

La firma de ciberseguridad industrial Dragos ha revelado detalles sobre FrostyGoop, un nuevo malware diseñado para atacar sistemas de control industrial (ICS). Este malware fue utilizado en enero de 2024 para interrumpir los sistemas de calefacción de una empresa energética municipal en Lviv, Ucrania, afectando a 600 edificios de apartamentos. FrostyGoop es el noveno malware ICS conocido y el primero que utiliza el protocolo Modbus para impactar directamente en la tecnología operativa (OT).

3. **DETALLE:**

Dragos comenzó a analizar FrostyGoop en abril de 2024, inicialmente creyendo que era un malware en fase de pruebas. Sin embargo, más tarde se supo que había sido utilizado en un ataque disruptivo en Ucrania. Los atacantes ganaron acceso a los sistemas de la instalación energética en abril de 2023, probablemente explotando una vulnerabilidad en un router Mikrotik expuesto a Internet.

El ataque se desarrolló en varias etapas:

- Abril 2023: Acceso inicial y despliegue de un webshell.
- Noviembre 2023: Obtención de credenciales de usuario del registro SAM.
- Diciembre 2023: Nuevos intentos de obtención de credenciales.
- 22 de enero 2024: Inicio del ataque disruptivo.

Los atacantes utilizaron FrostyGoop para enviar comandos Modbus directamente a los controladores ENCO de la instalación. Primero degradaron el firmware de los controladores para evitar su monitorización, y luego causaron que reportaran mediciones inexactas, haciendo que se bombeara agua fría a los edificios residenciales.

FrostyGoop es capaz de interactuar directamente con ICS usando Modbus a través del puerto 502, lo que lo hace potencialmente peligroso para muchos dispositivos y sectores industriales. Dragos estima que hay aproximadamente 46,000 dispositivos ICS expuestos a Internet que se comunican a través de este protocolo.

Aunque Dragos no ha atribuido el ataque a ningún país o actor de amenazas conocido, señalaron conexiones con direcciones IP basadas en Moscú durante el ataque de enero. Esto se suma a una historia de ataques rusos contra el sector energético ucraniano, incluyendo apagones causados por malware en 2015 y 2016.

El descubrimiento de FrostyGoop subraya la creciente sofisticación de las amenazas contra infraestructuras críticas y la necesidad de una mayor seguridad en los sistemas de control industrial.

4. RECOMENDACIONES:

- Actualizar de manera sistemática los sistemas industriales.
- Separa estrictamente las redes IT y OT (Tecnología Operacional). Implementa firewalls y zonas desmilitarizadas entre las redes.
- Monitore continuo para buscar cualquiera anomalía dentro de la red.
- Realizar un assessment del entorno OT y priorizar la mitigación según evaluación de riesgos.

5. REFERENCIAS:

- https://cyberpress.org/pentagen-nasa-it-service-provider-hacked/

Siemens advierte sobre vulnerabilidades críticas en productos SICAM: Urge actualización inmediata

Tipo de Ataque: Vulnerabilidades

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**
   - SICAM A8000
   - SICAM EGS
   - SICAM 8
2. **RESUMEN:**

Siemens ha emitido una advertencia sobre vulnerabilidades críticas que afectan a varios productos de su línea SICAM, incluyendo dispositivos SICAM A8000, SICAM EGS y la solución de software SICAM 8. Las vulnerabilidades, identificadas como CVE-2024-37998 y CVE-2024-39601, permiten el restablecimiento no autorizado de contraseñas y la degradación de firmware, lo que podría llevar a la escalada de privilegios y el compromiso del sistema. Siemens insta a los usuarios a actualizar inmediatamente el firmware y a implementar medidas de seguridad adicionales.

3. **DETALLE:**

Siemens ha revelado dos vulnerabilidades críticas que afectan a sus productos SICAM:

CVE-2024-37998: Permite a atacantes no autorizados restablecer contraseñas administrativas sin conocer la contraseña actual en aplicaciones con inicio de sesión automático habilitado. Esta vulnerabilidad de cambio de contraseña no verificada (CWE-620) otorga acceso administrativo completo y representa un riesgo crítico debido a su naturaleza accesible por red y su bajo nivel de complejidad.

CVE-2024-39601: Los dispositivos afectados carecen de autenticación adecuada para funciones críticas de degradación de firmware, permitiendo a atacantes autenticados remotos o no autenticados con acceso físico revertir los dispositivos a versiones de firmware más antiguas y vulnerables.

La empresa enfatiza que no abordar estas vulnerabilidades podría resultar en acceso no autorizado, filtraciones de datos y alteración de servicios críticos, especialmente en entornos donde los productos SICAM se utilizan para sistemas de control industrial y gestión de infraestructuras.

4. **RECOMENDACIONES:**
   - Actualizar inmediatamente el firmware a V5.40 y V1.4.0 respectivamente.
   - Deshabilitar la función de inicio de sesión automático.
   - Implementar medidas estrictas de seguridad de red, incluyendo el uso de firewalls y segmentación de red segura.
   - Monitorear los sistemas en busca de actividades inusuales.
5. **REFERENCIAS:**

- https://cyberpress.org/hackers-could-install-backdoor/
- https://www.securityweek.com/siemens-patches-power-grid-product-flaw-allowing-backdoor-deployment/