Alerta de Seguridad

Riesgo de vulnerabilidades IT y OT

Octubre - 2023

Sobre Axus

Axus es una empresa líder 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 Octubre.

Alertas de Seguridad IT:

- La banda de ransomware BlackCat evoluciona a tácticas más peligrosas
- Una versión troyanizada del software PyCharm se despliega vía Ads de Google Search
- La Comisión de Valores y Bolsa de los Estados Unidos (SEC) avanza en su caso contra SolarWinds

Alertas de Seguridad OT/ICS:

- Casi 100.000 sistemas de control industrial expuestos a la Internet pública
- Vulnerabilidad Crítica 10 en CVSS en Rockwell Automation Stratix 5800 y Stratix 5200

La banda de ransomware BlackCat evoluciona a tácticas más peligrosas: RaaS

Tipo de Ataque: **Ransomware como Servicio (RaaS).**

Medio de Propagación: **Internet**

1. RESUMEN:

El grupo de operadores BlackCat ha anunciado recientemente actualizaciones a sus herramientas, incluyendo una utilidad llamada "Munchkin" que permite a los atacantes propagar la carga de BlackCat a máquinas remotas y compartirlas en la red de una organización víctima. Durante los últimos dos años, los operadores de BlackCat han continuado evolucionando y mejorando sus herramientas como parte de su modelo de negocio de ransomware como servicio (RaaS).

2. DETALLE:

En una investigación reciente, los investigadores de Unit 42 (PaloAlto) han adquirido una instancia única de Munchkin que se carga en una máquina virtual personalizada. Esta nueva táctica de aprovechar una máquina virtual personalizada para desplegar malware ha estado ganando tracción en los últimos meses, permitiendo a los actores de amenazas de ransomware eludir las soluciones de seguridad al desplegar sus cargas de malware.

El ransomware BlackCat se hizo público por primera vez en noviembre de 2021 y se destacó por su sofisticación y el uso del lenguaje de programación Rust. Al igual que otros actores de ransomware, BlackCat emplea un modelo de negocio RaaS que permite a los afiliados utilizar sus herramientas y compartir parte de las ganancias con los operadores.

El grupo BlackCat ha ampliado su enfoque a nivel mundial, atacando a víctimas en diversas industrias. A lo largo del tiempo, han evolucionado su conjunto de herramientas y han lanzado la herramienta "Munchkin" que se ejecuta en un sistema operativo Linux y permite ejecutar BlackCat en máquinas remotas o cifrar compartidos de SMB/CIFS.

El uso de máquinas virtuales para ejecutar malware es una tendencia creciente en la comunidad de ransomware, ya que permite evitar los controles de seguridad en el sistema operativo anfitrión. Como parte de su investigación, los investigadores de Unit 42 han adquirido una copia de esta utilidad de máquina virtual.

La utilidad Munchkin se entrega como un archivo ISO que se carga en una instancia recién instalada del producto de virtualización VirtualBox. El malware cambia la contraseña de root de la VM, ejecuta el malware y luego apaga la VM.

El malware utiliza archivos y scripts de Python para llevar a cabo operaciones de movimiento lateral, robo de contraseñas y ejecución de malware en la red de la víctima.

3. RECOMENDACIONES

- Concientizar y probar al personal sobre reconocer y reportar correos maliciosos y otras amenazas, así como entrenarlos en buenas prácticas que disminuyan el riesgo de infección.
- No proporcionar privilegios de administrador local a los usuarios finales.

- Herramientas especiales, como VirtualBox, solo deben permitirse por una necesidad justificada de negocio.
- Se recomienda contar con un equipo de ciberseguridad que pueda prevenir y/o contener este tipo de ataques y reducir los daños en las organizaciones, mediante un monitoreo 24x7.

4. REFERENCIAS:

- https://unit42.paloaltonetworks.com/blackcat-ransomware-releases-new-utility-munchkin/
- https://unit42.paloaltonetworks.com/blackcat-ransomware/
- https://securityintelligence.com/posts/blackcat-ransomware-levels-up-stealth-speed-exfiltration/

Una versión troyanizada del software PyCharm se despliega vía Ads de Google Search

Tipo de Ataque: Phishing - Malware - Malvertising

Medio de Propagación: Internet

1. RESUMEN:

En una nueva campaña de malvertising se ha observado cómo un sitio web comprometido promociona versiones falsas de PyCharm en los resultados de búsqueda de Google a través de Anuncios de Búsqueda Dinámica. Jérôme Segura, director de inteligencia de amenazas en Malwarebytes, informa que el dueño del sitio no tenía conocimiento de esto, ya que uno de sus anuncios fue creado automáticamente para promocionar un popular programa para desarrolladores de Python.

2. DETALLE:

Las víctimas que hicieron clic en el anuncio eran redirigidas a una página web comprometida con un enlace para descargar la aplicación PyCharm. Sin embargo, en lugar de la aplicación legítima, se instalaban más de una docena de malware diferentes en las computadoras de los usuarios.

El sitio web infectado en cuestión es un portal en línea especializado en planificación de bodas, que había sido inyectado con malware para servir enlaces falsos para descargar el software PyCharm.

Según Malwarebytes, los objetivos son dirigidos al sitio web utilizando Anuncios de Búsqueda Dinámica, una oferta de Google que utiliza programación para adaptar anuncios específicos basados en los términos de búsqueda de los usuarios y el contenido del sitio web.

Google explica que cuando alguien busca en Google con términos relacionados con los títulos y frases frecuentemente utilizados en un sitio web, Google Ads utilizará estos títulos y frases para seleccionar una página de destino del sitio web y generar un título claro y relevante para el anuncio.

En resumen, un actor de amenazas con la capacidad de alterar el contenido del sitio web también podría utilizar las campañas de anuncios como una herramienta lucrativa para abuso, sirviendo efectivamente anuncios de Google Search a usuarios que pueden llevar a un comportamiento no deseado.

Segura explica que "lo que sucedió aquí es que Google Ads generó dinámicamente este anuncio a partir de la página hackeada, lo que convierte al propietario del sitio web en un intermediario no intencional y víctima que paga por su propio anuncio malicioso".

Esta situación ocurre mientras Akamai detalla la infraestructura detrás de una sofisticada campaña de phishing que tiene como objetivo a sitios de hospitalidad y sus clientes. La campaña se considera una amenaza global y ha generado un tráfico significativo de DNS en Suiza, Hong Kong y Canadá. A pesar de que se pensaba que la campaña solo estaba activa desde septiembre de 2023, el registro de dominio muestra que los nombres de dominio se registraron y consultaron a partir de junio de 2023.

3. **RECOMENDACIONES:**
   - Se recomienda contar con un programa de concientización en ciberseguridad para su organización, el cual mejoraría los conocimientos de los colaboradores en las prácticas de seguridad de la información.
   - Contar con un Anti Malware avanzado o un EDR que esté totalmente desplegado en las PCs y servidores de la organización.
4. **REFERENCIAS:**
   - https://www.malwarebytes.com/blog/threat-intelligence/2023/10/malvertising-via-dynamic-search-ads-delivers-malware-bonanza

La Comisión de Valores y Bolsa de los Estados Unidos (SEC) avanza en su caso contra SolarWinds

1. RESUMEN:

La Comisión de Valores y Bolsa de los Estados Unidos (SEC) presentó una demanda contra SolarWinds, alegando que la empresa tenía medidas de seguridad digital deficientes y no las divulgó antes de la histórica violación de la empresa de software, que ha sido catalogada como una de las peores.

2. DETALLE:

El caso presenta varios aspectos únicos:

1. Es la primera vez en un caso cibernético de la SEC que la comisión alega que una organización tenía la intención de engañar a los inversores.
2. Es la primera vez en un caso cibernético de la SEC que la comisión ha tomado medidas contra un individuo.
3. Es la primera vez en un caso cibernético de la SEC que la comisión alega que una empresa tenía fallas en sus controles internos para protegerse.

En cuanto a los detalles de la demanda, la SEC se basó en declaraciones de empleados y funcionarios de la empresa para enfatizar que SolarWinds era consciente de sus problemas de seguridad. Se mencionaron preocupaciones expresadas por ingenieros y empleados sobre la falta de seguridad en el acceso remoto, problemas con los controles de acceso al sistema, y declaraciones preocupantes de que la empresa no tenía una mentalidad de seguridad sólida.

La SEC argumenta que SolarWinds y el oficial de seguridad de la información, Tim Brown, se involucraron en una campaña para crear una imagen falsa del entorno de control cibernético de la empresa, lo que privó a los inversores de información precisa y material.

SolarWinds ha manifestado su desacuerdo con las acusaciones de la SEC, afirmando que las acusaciones son infundadas y que esta acción podría poner en riesgo la seguridad nacional. Además, la compañía defiende su compromiso con la seguridad cibernética y espera aclarar los hechos en la corte.

El abogado de Tim Brown, Alec Koch, también defendió su reputación y la mejora continua de la postura de seguridad cibernética de la compañía durante su tiempo en SolarWinds.

3. RECOMENDACIONES:

- Se recomienda a las organizaciones verificar las medidas de seguridad digital de sus proveedores y socios estratégicos. Es importante asegurar que cumplen con los estándares necesarios para el manejo de la información, para evitar incidentes.

4. REFERENCIAS:

- What to know about the SEC's case against SolarWinds - The Washington Post

Casi 100.000 sistemas de control industrial expuestos a la Internet pública

Tipo de Ataque: Ransomware

Medio de Propagación: Internet

1. PRODUCTOS AFECTADOS:

- Sistemas de control industrial (ICS)

2. RESUMEN:

Bitsight, una empresa líder en la gestión y supervisión de riesgos cibernéticos ha identificado casi 100.000 sistemas de control industrial (ICS) expuestos a la Internet pública. Los ICS son un subconjunto de la tecnología operativa (OT) y se utilizan para gestionar procesos industriales como el flujo de agua en los sistemas municipales de agua, la transmisión de electricidad a través de las redes eléctricas y otros procesos críticos. Las infraestructuras críticas dependen en gran medida de los ICS para controlar los sistemas ciberfísicos, por lo que los sistemas expuestos identificados en esta investigación podrían presentar riesgos significativos para las organizaciones y las comunidades de todo el mundo.

3. DETALLE:

Sistemas expuestos y consecuencias potenciales

En los últimos años, tanto los actores de amenazas cibernéticas oportunistas como los avanzados han mostrado una mayor disposición a atacar sitios industriales y operativos.

A pesar de los avances, la seguridad de los ICS y, más ampliamente, de la OT, sigue siendo una preocupación compleja y global.

Consecuencias potenciales de los sistemas de control industrial expuestos

Muchos de los sistemas físicos controlados por los ICS pueden ser críticos para el funcionamiento de una región o una organización. Por lo tanto, la interrupción de estos sistemas podría provocar importantes trastornos comerciales, amenazas a la seguridad humana, la pérdida de datos y propiedad intelectual (IP), amenazas a la seguridad nacional y mucho más.

Los ciberataques que aprovechan las infraestructuras físicas no son nuevos:

- El mes pasado, hubo informes de que unos atacantes habían irrumpido en la red eléctrica nacional de un país asiático.
- Un ataque de ransomware dirigido al Colonial Pipeline interrumpió el suministro de petróleo y gas en la costa oriental de Estados Unidos, provocando escasez y pánico.
- El malware Industroyer, en 2016, se dirigió al suministro eléctrico de Kiev (Ucrania), provocando cortes de energía en las regiones afectadas.

Muchos sistemas industriales, ya sean infraestructuras críticas o no, utilizan software antiguo y difícil de parchear, pero siguen desempeñando un papel fundamental en las sociedades y las organizaciones, por lo que el tiempo de inactividad para aplicar parches es costoso o provoca inconvenientes o sufrimientos

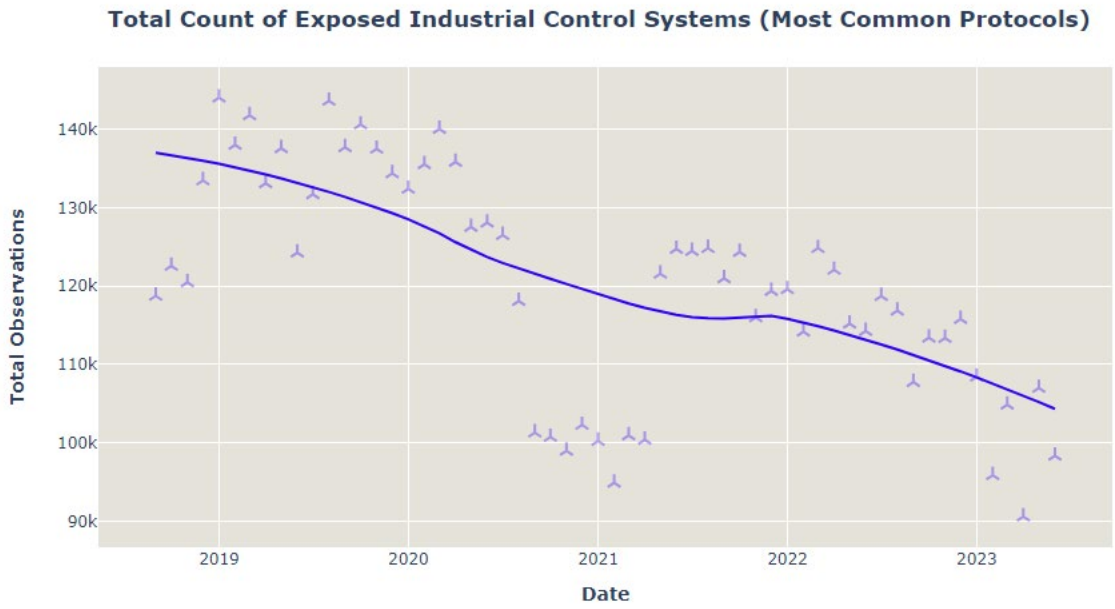
a la población. Apagar una red eléctrica o cualquier otro entorno industrial crítico para solucionar problemas tiene consecuencias de gran alcance, por lo general mayores que las que se experimentan al apagar un entorno de tecnología de la información (TI). Por lo tanto, los sistemas OT son más complicados de proteger y presentan cuellos de botella poco ortodoxos a diferencia de los que se experimentan en el frente de TI.

Estado mundial de la exposición

Bitsight identificó sistemas de control industrial expuestos en todo el mundo, revelando tendencias tanto preocupantes como prometedoras. Estudiamos los sistemas que se comunican a través de los protocolos ICS más utilizados, como Modbus, KNX, BACnet, Niagara Fox y otros.

La exposición de los ICS sigue siendo alta, pero está disminuyendo

El número de sistemas de control industrial expuestos, o accesibles a Internet, sigue siendo alto, con casi 100.000 en junio de 2023, pero la investigación de Bitsight reveló una tendencia prometedora. De 2019 a junio de 2023, observamos un descenso en el número de ICS expuestos a la Internet pública. Se trata de un avance positivo, que sugiere que las organizaciones pueden estar configurando correctamente, cambiando a otras tecnologías o eliminando de la Internet pública los ICS previamente expuestos.



Fuente: Bitsight identifies nearly 100,000 exposed industrial control systems

El descenso del número de organizaciones expuestas —aquellas que utilizan al menos un sistema de control industrial expuesto— sigue una trayectoria similar:

Si bien el número total de ICS expuestos ha ido disminuyendo, hemos detectado un comportamiento único en función del protocolo. Los sistemas y dispositivos expuestos que se comunican a través de los protocolos Modbus y S7 son más comunes en junio de 2023 que antes, con el primero aumentando en prevalencia desde 2020 y el segundo más recientemente desde mediados de 2022. Sin embargo, los

sistemas de control industrial expuestos que se comunican a través de Niagara Fox han ido disminuyendo desde aproximadamente 2021. Las organizaciones deben ser conscientes de estos cambios en la prevalencia para informar sus estrategias de seguridad de OT/ICS. Uno de los primeros pasos para mitigar el riesgo de OT es saber dónde

4. RECOMENDACIONES:

Las organizaciones deben emprender inmediatamente actividades de remediación:

- Identificar cualquier sistema de control industrial desplegado por su organización y/o sus socios comerciales externos, y evaluar rápidamente la seguridad de estos sistemas.
- Eliminar cualquier sistema de control industrial de la Internet pública.
- Emplear salvaguardias como cortafuegos para protegerse contra el acceso no autorizado a sus sistemas de control industrial.
- Los líderes de seguridad deben reconocer las necesidades de control únicas que se aplican a la OT, incluidos los sistemas de control industrial, en lugar de simplemente aplicar un modelo de riesgo de TI tradicional a esta infraestructura.

5. REFERENCIAS:

- Bitsight identifies nearly 100,000 exposed industrial control systems | Bitsight
- Casi 100.000 sistemas de control industrial expuestos a la Internet pública - infoPLC

Vulnerabilidad Crítica 10 en CVSS en Rockwell Automation Stratix 5800 y Stratix 5200:

Tipo de Ataque: Vulnerabilidad

Medio de Propagación: Red, Internet

1. **PRODUCTOS AFECTADOS:**
   - Rockwell Automation:
     - ❖ Stratix 5800 (ejecutando Cisco IOS XE Software con la función de interfaz web habilitada): Todas las versiones
     - ❖ Stratix 5200 (ejecutando Cisco IOS XE Software con la función de interfaz web habilitada): Todas las versiones
2. **RESUMEN:**
   - **CVSS v3:** 10.0
   - **Atención:** Explotable de forman remota/Complejidad de ataque baja/Explotación pública conocida
   - **Vulnerabilidad:** Canal Alternativo no Protegido
3. **DETALLE:**

Evaluación del riesgo

La explotación exitosa de esta vulnerabilidad podría permitir a un atacante no autenticado tomar el control del sistema afectado.

Canal alternativo no protegido CWE-420

Rockwell Automation tiene conocimiento de la explotación activa de una vulnerabilidad previamente desconocida en la función de interfaz web de Cisco IOS XE Software cuando está expuesta a Internet o a redes no confiables. Esta vulnerabilidad permite a un actor de amenazas remoto y no autenticado crear una cuenta en un sistema vulnerable con acceso de nivel de privilegio 15 (Incluye todos los comandos del permiso-nivel en el prompt del router). El actor de amenazas podría utilizar esa cuenta para potencialmente tomar el control del sistema afectado.

CVE-2023-20198 se ha asignado a esta vulnerabilidad. Se ha calculado una puntuación base CVSS v3 de 10.0; el vector CVSS es (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

4. **RECOMENDACIONES**

Rockwell Automation alienta a los usuarios a seguir la guía para deshabilitar los servidores HTTP de Stratix en todos los sistemas que están expuestos a Internet.

Para deshabilitar la función del servidor HTTP, utilice el comando `no ip http server` o `no ip http secure-server` en el modo de configuración global. Si tanto el servidor HTTP como el servidor HTTPS están en uso, se requieren ambos comandos para deshabilitar la función del servidor HTTP. Al implementar

controles de acceso para estos servicios, asegúrese de revisar los controles, ya que existe el potencial de una interrupción en los servicios de producción.

Cisco Talos ha proporcionado Indicadores de Compromiso y reglas Snort que se pueden encontrar en el enlace proporcionado. Para obtener más información, consulte el Aviso de Seguridad de Rockwell Automation.

- CISA recomienda a los usuarios tomar medidas defensivas para minimizar el riesgo de explotación de esta vulnerabilidad, como:
- Minimizar la exposición de la red para todos los dispositivos y/o sistemas de control, asegurándose de que no sean accesibles desde Internet.
- Colocar las redes de sistemas de control y dispositivos remotos detrás de firewalls y aislarlos de las redes empresariales.
- Cuando sea necesario el acceso remoto, utilizar métodos más seguros, como Redes Privadas Virtuales (VPN), reconociendo que las VPN pueden tener vulnerabilidades y deben actualizarse a la versión más reciente disponible. También reconocer que una VPN es tan segura como los dispositivos conectados.
- CISA recomienda a las organizaciones realizar un análisis de impacto adecuado y una evaluación de riesgos antes de implementar medidas defensivas.

CISA también proporciona una sección de prácticas recomendadas para la seguridad de sistemas de control en la página web de ICS en cisa.gov/ics. Varios productos de CISA que detallan las mejores prácticas de defensa cibernética están disponibles para su lectura y descarga, incluida la mejora de la ciberseguridad de sistemas de control industrial con estrategias de defensa en profundidad.

CISA alienta a las organizaciones a implementar estrategias de ciberseguridad recomendadas para una defensa proactiva de los activos de sistemas de control.

5. **REFERENCIAS:**
   - Rockwell Automation Stratix 5800 and Stratix 5200 | CISA
   - Security Advisory | Rockwell Automation