Boletín de Ciberseguridad

Riesgo de vulnerabilidades IT y OT

20-Dic-2022

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 Diciembre.

Alertas de Seguridad IT:

- Piratas informáticos firman aplicaciones de malware para Android con certificados comprometidos.
- Posible Filtración de Datos de SUNAT.
- Investigadores descubren troyanos en aplicaciones de Android y Windows.

Alertas de Seguridad OT/ICS:

- Investigadores de CLAROTY detallan un nuevo método de ataque para eludir WAFs.
- Vulnerabilidad en los productos MicroSCADA Pro/X SYS600 de Hitachi Energy.

Piratas informáticos firman aplicaciones de malware para Android con certificados comprometidos

Tipo de Ataque: Explotación de vulnerabilidades conocidas

Medio de Propagación: Red, Internet

1. PRODUCTOS AFECTADOS:

Se ha descubierto que los certificados de plataforma utilizados por los proveedores de teléfonos inteligentes Android como Samsung, LG y MediaTek se abusan para firmar aplicaciones maliciosas. La lista de paquetes de apps de Android que están abusando de los certificados son:

- com.russian.signato.renewis
- com.sledsdffsjkh.Search
- com.android.power
- com.management.propaganda
- com.sec.android.musicplayer
- com.houla.quicken
- com.attd.da
- com.arlo.fappx
- com.metasploit.stage
- com.vantage.ectronic.cornmuni

2. RESUMEN:

Una aplicación no autorizada, firmada con un certificado comprometido, puede obtener el nivel más alto de privilegios del sistema operativo Android, lo que le permite recopilar todo tipo de información confidencial de un dispositivo comprometido.

3. DETALLE:

Se han utilizado certificados de múltiples plataformas para firmar malware. Un certificado de plataforma es el certificado de firma de la aplicación que se usa para firmar la aplicación "android" en la imagen del sistema. La aplicación "android" se ejecuta con una identificación de usuario altamente privilegiada, android.uid.system, y tiene permisos del sistema, incluidos los permisos para acceder a los datos del usuario. Cualquier otra aplicación firmada con el mismo certificado puede declarar que quiere ejecutarse con la misma identificación de usuario, dándole el mismo nivel de acceso al sistema operativo Android.

4. RECOMENDACIONES:

- Todas las partes afectadas (desarrolladores de software) deben rotar el certificado de la plataforma reemplazándolo con un nuevo conjunto de claves públicas y privadas. Además, deben realizar una

investigación interna para encontrar la causa raíz del problema y tomar medidas para evitar que el incidente vuelva a ocurrir en el futuro.

- Recomendamos minimizar la cantidad de aplicaciones firmadas con el certificado de la plataforma, ya que reducirá significativamente el costo de rotar las claves de la plataforma en caso de que ocurra un incidente similar en el futuro.

5. REFERENCIAS:

- https://thehackernews.com/2022/12/hackers-sign-android-malware-apps-with.html
- https://bugs.chromium.org/p/apvi/issues/detail?id=100

Posible Filtración de Datos de SUNAT

Tipo de Ataque: Explotación de vulnerabilidades

Medio de Propagación: Red, Internet

1. PRODUCTOS AFECTADOS:

- Exchange server
- Fortinet, múltiples productos
- Cisco AnyConnect Secure
- Otros

2. RESUMEN:

El 05 de diciembre de 2022, el Equipo de Trabajo de Seguridad Digital (ETSD) de la DINI, mediante acciones de Cibercontrainteligencia, detectó una publicación en el sitio web "hxxps://breached.vc/", en el cual, el usuario identificado como "Kelvinsecurity", hizo público una supuesta base de datos que pertenecería a la Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT).

3. DETALLE:

El actor de amenazas identificado como "Kelvinsecurity", publicó el 03 de diciembre a las 13:22 horas, una supuesta base de datos que podría pertenecer a la SUNAT. En la publicación, el cibercriminal publicó veinte (20) registros de datos personales de los contribuyentes como muestra de la información que ha sido filtrada.

Lista de vulnerabilidades:

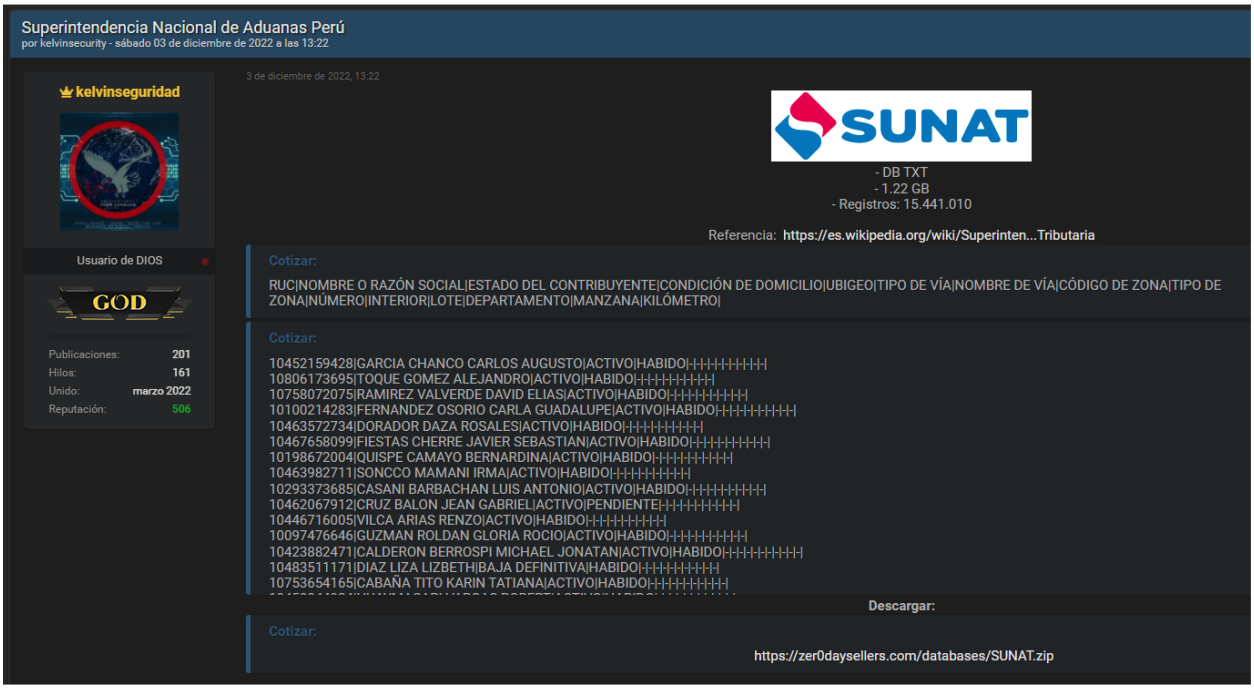

Figura 1: Base de Datos Filtrada

Entre los datos filtrados, figuran los siguientes:

- RUC
- Nombre o Razón Social
- Estado del Contribuyente
- Condición de Domicilio
- Ubigeo
- Nombre de Vía
- Código de Zona
- Tipo de Zona
- Número
- Interior
- Lote
- Departamento
- Kilómetro

No se tiene evidencia de datos de mayor sensibilidad que los mostrados. Este evento aún está en investigación por parte del Centro Nacional de Seguridad Digital.

4. RECOMENDACIONES:

- Se recomienda estar alertas a las actualizaciones de esta filtración y otras similares, por la posibilidad de mostrar información sensible a agentes de amenaza.

5. REFERENCIAS:

- https://breached.vc/Thread-National-Superintendency-of-Customs-Peru
- Centro Nacional de Seguridad Digital

Investigadores descubren troyanos en aplicaciones de Android y Windows

Tipo de Ataque: Troyano

Medio de Propagación: Red, Internet, correo electrónico, entre otros

1. PRODUCTOS AFECTADOS:

- Sistemas operativos Android y Windows

2. RESUMEN:

Investigadores han detectado una nueva campaña de malware híbrido dirigida a los sistemas operativos Android y Windows. Los ataques implican el uso de diferentes programas maliciosos como ERMAC, Erbium, Aurora y Laplas, según un informe de ThreatFabric compartido con The Hacker News. Mediante la campaña Erbium extrajo con éxito datos de más de 1300 víctimas.

3. DETALLE:

Las infecciones de ERMAC comienzan con un sitio web fraudulento que afirma ofrecer un software de autorización de Wi-Fi para Android y Windows que, cuando se instala, viene con funciones para robar frases iniciales de billeteras criptográficas y otros datos confidenciales.

ThreatFabric afirmo que encontró una serie de aplicaciones maliciosas que eran versiones troyanizadas de aplicaciones legítimas como Instagram, y los operadores las usaban como goteros para entregar la carga maliciosa ofuscada.

Las aplicaciones maliciosas, denominadas Zombinder, se desarrollaron utilizando un servicio de vinculación de APK anunciado en la web oscura (Dark Web) por un conocido actor de amenazas desde marzo de 2022.

Estas aplicaciones zombis también se han utilizado para distribuir troyanos bancarios de Android como SOVA y Xenomorph dirigidos a clientes en España, Portugal y Canadá, entre otros:

Figura 2: Panel de menú del troyano Xenomorph

4. RECOMENDACIONES:

- Mantener un software antimalware actualizado y con escaneos programados. Debe tener capacidad de detectar malware de día cero.
- Mantener actualizados los últimos parches de seguridad en los sistemas operativos y aplicaciones

5. REFERENCIAS:

- https://thehackernews.com/2022/12/researchers-uncover-darknet-service.html

Investigadores de Claroty detallan un nuevo método de ataque para eludir WAFs (firewalls de aplicaciones web)

Tipo de Ataque: Explotación de vulnerabilidades

Medio de Propagación: Red, Internet

1. PRODUCTOS AFECTADOS:

Principales proveedores de WAF:

- Palo-Alto Next Generation Firewall
- F5 Big-IP
- Amazon AWS ELB
- Cloudflare
- Imperva

2. RESUMEN:

Investigadores de Claroty, equipo nombrado Team82, demuestran que se puede utilizar un nuevo método de ataque para eludir los firewalls de aplicaciones web (WAF) de varios proveedores e infiltrarse en los sistemas, lo que podría permitir a los atacantes obtener acceso a información comercial y confidencial de clientes.

3. DETALLE:

Los firewalls de aplicaciones web (WAF) son una línea de defensa clave para ayudar a filtrar, monitorear y bloquear el tráfico HTTP(S) hacia y desde una aplicación web, mediante la verificación de que cumplan con las reglas del firewall. Estos protegen contra ataques como cross-site-forgery, cross-site-scripting (XSS), file inclusion y SQL Injection (SQLi).

El bypass genérico "implica agregar la sintaxis JSON (formato de texto de JavaScript) a las cargas útiles de inyección SQL que un WAF no puede analizar", dijo el investigador de Claroty, Noam Moshe. "La mayoría de los WAF detectarán fácilmente los ataques SQLi, pero anteponer JSON a la sintaxis SQL dejó al WAF ciego ante estos ataques".

```
' and '{"C":2}' <@ '{"a":1, "b":2}' union select (id+num) from
(select ((ASCII(a[1])::BIGINT<<8) + (ASCII(a[2])::BIGINT<<16) +
(ASCII(a[3])::BIGINT<<24) + (ASCII(a[4])::BIGINT<<32) +
(ASCII(a[5])::BIGINT<<40) + (ASCII(a[6])::BIGINT<<48)) as
num,row_number() over() as id from regexp_matches((select 'this
is a test'),'(.)(.)(.)(.)(.)(.)','g') as a) bb-- -;
```

WAF Evasion
Solving Limitation 1: Casting strings to integers
Solving Limitation 2: Exfiltrating character index
Solving Limitation 3: Exfiltrating multiple characters in a single returned row.
The actual data we want to exfiltrate

Figura 3: Código para extracción de datos

La empresa de ciberseguridad industrial y de IoT, Claroty, dijo que su técnica funcionó con éxito contra los WAF de proveedores como Palo-Alto Next Generation Firewall, F5 Big-IP, Amazon AWS ELB, Cloudflare e Imperva, quienes desde entonces han lanzado actualizaciones para admitir la sintaxis JSON durante la inspección de inyección SQL.

Team82 reveló sus hallazgos a cinco de los principales proveedores de WAF, todos los cuales agregaron soporte de sintaxis JSON a sus productos. Es posible que los productos de otros proveedores pueden verse afectados y que se deban realizar revisiones para la compatibilidad con JSON.

4. RECOMENDACIONES:

- Instalar las últimas actualizaciones de seguridad para los WAFs de las marcas: Palo-Alto Next Generation Firewall, F5 Big-IP, Amazon AWS ELB, Cloudflare e Imperva.
- Si su WAF no es de los proveedores mencionados, consultar con su marca sobre este método de evasión.
- También puede pedir a su Ethical Hacker que incluya este método entre sus pruebas de evasión de WAF.

5. REFERENCIAS:

- https://claroty.com/team82/research/js-on-security-off-abusing-json-based-sql-to-bypass-waf
- https://thehackernews.com/2022/12/researchers-detail-new-attack-method-to.html

Vulnerabilidad en los productos MicroSCADA Pro/X SYS600 de Hitachi Energy

Tipo de Ataque: Explotación de Vulnerabilidades conocidas

Medio de Propagación: Red, Internet

1. **PRODUCTOS AFECTADOS:**

- SYS600 versión 10.4 y anteriores
- SYS600 versión 9.4 FP2 Hotfix 4 y anteriores

2. **RESUMEN:**

Existe una vulnerabilidad de validación de entrada en la interfaz Monitor Pro de MicroSCADA Pro y MicroSCADA X SYS600. Un usuario autenticado puede iniciar una ejecución remota de código a nivel de administrador independientemente del rol del usuario autenticado.

3. **DETALLE:**

EL SYS600 es un producto SCADA utilizado para el monitoreo y control de sistemas eléctricos. Se ha reportado una vulnerabilidad de severidad ALTA de tipo validación de entrada incorrecta en los productos MicroSCADA Pro/X SYS600 de Hitachi Energy. La explotación exitosa de esta vulnerabilidad podría permitir a un usuario no autorizado ejecutar scripts de nivel de administrador. Debido a que se requiere acceso al SYS600 y una cuenta de usuario válido, esta vulnerabilidad no se vincula al network stack.

4. **RECOMENDACIONES:**

- Para SYS600 9.x: actualice a SYS600 versión SYS600 9.4 FP2 Hotfix 5 cuando se lance o actualice al menos a SYS600 versión 10.4.1. Un requisito para instalar SYS600 9.4 FP2 Hotfix 5 es tener instalado al menos el SYS600 9.4 FP2 Hotfix 4.
- Para SYS600 10.x, actualice al menos a SYS600 versión 10.4.1 o aplique factores de mitigación generales.

RECOMENDACIÓN GENERAL: Las prácticas de seguridad recomendadas y las configuraciones de firewall pueden ayudar a proteger una red de control de procesos de ataques que se originan desde fuera de la red. Dichas prácticas incluyen que los sistemas de control de procesos estén protegidos físicamente del acceso directo por parte de personal no autorizado, no tengan conexiones directas a Internet y estén separados de otras redes por medio de un sistema de firewall que tenga un número mínimo de puertos expuestos, y otros que tengan a evaluar caso por caso. Los sistemas de control de procesos no deben utilizarse para navegar en Internet, enviar mensajes instantáneos o recibir correos electrónicos.

Las computadoras portátiles y los medios de almacenamiento extraíbles deben escanearse cuidadosamente en busca de virus antes de conectarlos a un sistema de control. Se deben seguir las políticas y los procesos de contraseña adecuados.

5. REFERENCIAS:

- https://search.abb.com/library/Download.aspx?DocumentID=8DBD000123&LanguageCode=en&DocumentPartId=&Action=Launch&elqaid=4293&elqat=1
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3388