PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

109-2024-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aéreadel Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y lasempresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°109	Fecha: 10-05-2024
		Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Dell sufre un robo de datos de 49 millones de clientes		
Tipo de Ataque	Robo de información	Abreviatura	RobInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K01
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. ANTECEDENTES:

Una nueva violación de datos ha puesto en riesgo a millones de clientes que, supuestamente, se han visto afectados. Afecta a quienes tengan equipos Dell y, en total, puede haber unos 49 millones de clientes cuya información ha quedado comprometida.

El fabricante de computadoras comenzó ayer a enviar por correo electrónico notificaciones de violación de datos a los clientes, indicando que se había violado un portal de Dell que contenía información del cliente, relacionada con las compras.

2. DETALLES:

La infracción expuso nombres de clientes, direcciones físicas e información detallada de los pedidos, incluidas etiquetas de servicio, descripciones de artículos, fechas de pedidos y detalles de la garantía.

El 28 de abril, un actor de amenazas llamado Menelik ha reclamado la incidencia en BreachForums y ha ofrecido vender estos datos que comprenden entre 2017 y 2024. Enumeró datos robados de Dell en BreachForum que incluían información del cliente con campos no financieros como ciudad, nombre completo, dirección, provincia, código postal, plan de garantía, nombre de la empresa, número de pedido de Dell, número de cliente de Dell, fecha de envío (fecha del pedido) y etiqueta de servicio única de siete dígitos del sistema.

Sin embargo, Dell ha confirmado que no se accedió a datos financieros, direcciones de correo electrónico, números de teléfono u otra información altamente confidencial durante el incidente.

Aunque son inofensivos desde el punto de vista del adversario, los datos robados podrían ser utilizados por empresas de marketing y competidores para elaborar perfiles, o en campañas de phishing.

Según parece, esa base de datos ya no está a la venta en BreachForums. Eso puede indicar que alguien lo ha comprado. Esto, inevitablemente, hace que los clientes afectados deban estar alertas ante posibles intentos de ataques. Aunque la información robada es limitada, podría ser utilizada en un momento dado.

Se está llevando a cabo una investigación de Dell mientras los clientes esperan más detalles sobre la infracción. "Al identificar el incidente, implementamos rápidamente nuestros procedimientos de respuesta a incidentes, comenzamos a investigar, tomamos medidas para contener el incidente y notificamos a las autoridades", dijo la compañía en el correo electrónico. "También hemos contratado a una empresa forense externa para investigar este incidente".

3. RECOMENDACIONES:

- Controlar sus cuentas para detectar cualquier actividad inusual y que tomen precauciones para proteger su información personal.
- Tener cuidado con las estafas telefónicas de soporte técnico que podrían implicar la explotación de los datos robados.
- Utilizar contraseñas únicas difíciles de descifrar para proteger cuentas y datos confidenciales, además de permitir la autenticación de 2 factores.

Fuente de Información:	• hxxps://www.redeszone.net/noticias/seguridad/hackeo-dell-millones-datos/ • hxxps://cso.computerworld.es/empresas/dell-sufre-un-robo-de-datos-de-49-millones-de-clientes • hxxps://gbhackers.com/apple-infrastructure-sql-injection/ • hxxps://www.infordisa.com/soc/brecha-de-datos-dell/ • hxxps://www.ciberseguridadlatam.com/2024/05/09/dell-advierte-sobre-violacion-de-datos/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°109	Fecha: 10-05-2024 Página: 5 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Nueva campaña de troyano bancario para Android "Zanubis" dirigido a entidades financieras en Perú que suplanta a la SUNAT		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

El investigador de ciberamenazas en la red social en X (Twitter), Germán Fernández (@1ZRR4H), ha publicado un aviso sobre una nueva campaña de correo electrónico de phishing para distribuir el troyano bancario para Android "Zanubis" dirigido a múltiples entidades financieras en el Perú. En esta campaña, el actor de amenazas está suplantando a la Superintendencia Nacional de Aduanas y de Administración Tributaria – SUNAT.

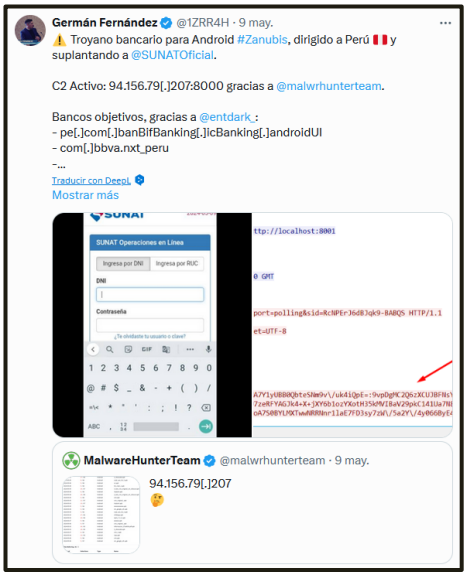
2. DETALLES:

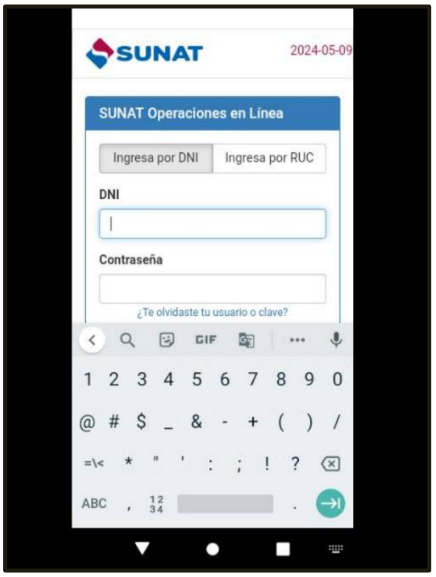
Zanubis es un troyano bancario avanzado para Android que ha atacado a cerca de 40 aplicaciones de bancos y otras entidades financieras en Perú, convirtiéndose en la principal amenaza de malware bancario móvil en el país.

El malware Zanubis se infiltra en los dispositivos a través de aplicaciones maliciosas que simulan ser legítimas. Una vez instalado, realiza las siguientes acciones para robar dinero y credenciales de inicio de sesión de las cuentas bancarias de las víctimas:

- Muestra la página web real de la institución bancaria para evitar sospechas.
- Registra todos los textos digitalizados y graba la pantalla para robar credenciales de acceso a apps bancarias.
- Solicita ser la aplicación predeterminada para validación de SMS y eliminar los códigos de verificación enviados por los bancos.
- Puede bloquear el teléfono para impedir que la víctima acceda a sus aplicaciones.
- Interceptar mensajes SMS y accede a contactos y sitios web.
- Instalar software de acceso remoto para que el cibercriminal controle el dispositivo sin ser detectado.

El troyano bancario Zanubis también dirige sus ataques a aplicaciones como Gmail y WhatsApp para el robo de información de las víctimas. Aunque no hay una atribución definitiva, varios indicios sugieren que este troyano es de origen peruano y podría expandirse por la región. Para protegerse, los expertos recomiendan instalar apps de fuentes confiables, verificar permisos, usar soluciones de seguridad, no hacer clic en enlaces sospechosos y no hacer rooting al dispositivo.





A. Entidades afectadas:

La lista de aplicaciones de entidades financieras a las que apunta el malware es:

- pe[.]com[.]banBifBanking[.]icBanking[.]androidUI
- com[.]bbva.nxt_peru
- pe[.]com[.]interbank[.]mobilebanking
- com[.]mibanco[.]bancamovil
- pe[.]com[.]scotiabank[.]blpm[.]android[.]client
- com[.]bcp[.]bank[.]bcp
- pe[.]com[.]bn[.]app[.]bancodelanacion
- per[.]bf[.]desa
- com[.]bcp[.]innovacxion[.]yapeapp
- com[.]pe[.]cajasullana[.]cajamovil
- pe[.]pichincha[.]bm
- com[.]ripley[.]banco[.]peru
- com[.]cmac[.]cajamovilaqp
- com[.]cajahuancayo[.]cajahuancayo[.]appcajahuancayo
- com[.]cmacica[.]prd
- pe[.]cajapiura[.]bancamovil
- pe[.]solera[.]tarjetaoh
- com[.]alfinbanco[.]appclientes
- pe[.]com[.]bancomercio[.]mobilebanking
- com[.]bm_gnb_pe
- com[.]zoluxiones[.]officebanking
- pe[.]com[.]cajametropolitana[.]homebankingcml[.]cmlhomebanking
- com[.]pe[.]cajacusco[.]movil
- com[.]caja[.]myapplication
- com[.]cajamaynas[.]cajamaynas
- com[.]cajatacna[.]droid
- com[.]appcajatrujillo
- pe[.]com[.]tarjetacencosud[.]canales[.]mitarjetacencosud
- pe[.]com[.]cajacentro
- pe[.]com[.]prymera[.]digital[.]app
- pe[.]com[.]compartamos[.]bancamovil
- pe[.]confianza[.]bancamovil
- com[.]credinkamovil[.]pe
- pe[.]com[.]scotiabank[.]blpm[.]android[.]client[.]csf
- com[.]efectivadigital[.]appclientes
- com[.]qapaq[.]banking
- pe[.]com[.]tarjetasperuanasprepago[.]tppapp
- maximo[.]peru[.]pe
- air[.]PrexPeru
- pe[.]com[.]tarjetaw[.]neobank
- com[.]fif[.]fpay[.]android[.]pe
- com[.]cencosud[.]pe[.]metro
- com[.]cencosud[.]pe[.]wong
- com[.]tottus
- com[.]pichincha[.]cashmanagement

- com[.]binance[.]dev
- com[.]gateio[.]gateio
- com[.]google[.]android[.]apps.authenticator2
- com[.]bbva[.]GEMA[.]global
- pe[.]com[.]scotiabank[.]businessbanking
- com[.]bcp[.]bank[.]tlc
- com[.]scotiabank[.]telebankingapp
- com[.]bitkeep[.]wallet
- com[.]bitmart[.]bitmarket
- com[.]bitcoin[.]mwallet
- com[.]bbva[.]bbvawalletpe
- com[.]bbva[.]lukita
- cash[.]klever[.]blockchain[.]wallet
- org[.]theta[.]wallet
- com[.]wallet[.]crypto[.]trustapp
- com[.]myetherwallet[.]mewwallet
- pe[.]interbank[.]bie.

B. Indicadores de Compromiso:

- Servidor de Comando y Control (C2) activo: 94.156.79[.]207:8000
- SHA256: 0c4a870da8f87c8e5af00f6f6f42b4a4af0b0b55e80b8ac97ac500379932

Communicating Files (24)

Scanned	Detections	Type	Name
2024-05-06	3 / 66	Android	sunat_1.apk
2024-05-03	17 / 66	Android	2_ofuscado.apk
2024-05-09	8 / 66	Android	cript_aes_tst_1.apk
2024-05-06	5 / 66	Android	oJ.apk
2024-05-08	5 / 68	Android	tst_cript_1.apk
2024-05-05	19 / 67	Android	3_bot_crio_original_sin_ofuscar.apk
2024-05-06	6 / 66	Android	implant.apk
2024-05-04	10 / 66	Android	2_bot_crio_original_sin_ofuscar.apk
2024-05-05	5 / 66	Android	crio.apk
2024-05-05	11 / 67	Android	crio_original_.apk

Files Referring (4)

Scanned	Detections	Type	Name
2024-05-03	4 / 63	Android	classes.dex
2024-05-03	6 / 63	Android	classes.dex
2024-05-03	6 / 63	Android	classes.dex
2024-05-03	6 / 63	Android	classes.dex

3. RECOMENDACIONES:

- Instalar aplicaciones únicamente de fuentes confiables y verificar los permisos que solicitan antes de aceptarlos.
- Usar soluciones de seguridad móvil de proveedores reconocidos para detectar y bloquear amenazas.
- No hacer clic en enlaces sospechosos recibidos por SMS, WhatsApp u otras aplicaciones, ya que pueden contener el malware.
- Evitar hacer rooting o jailbreak al dispositivo, ya que esto debilita las medidas de seguridad.
- Estar atento a actualizaciones sospechosas de Android que bloquean el teléfono, ya que podrían ser falsas y parte del ataque de Zanubis.
- Revisar los permisos de las aplicaciones instaladas y eliminar aquellas que parezcan sospechosas o no se usen.
- Estar alerta a cualquier comportamiento extraño del dispositivo, como lentitud, consumo excesivo de batería o aplicaciones que se cierran solas.
- Mantener el sistema operativo y las aplicaciones actualizadas con las últimas versiones para corregir vulnerabilidades.

Fuente de Información:	• hxxps://twitter.com/1ZRR4H/status/1788631668682584112 • hxxps://labs.k7computing.com/index.php/an-upsurge-of-new-android-banking-trojan-zanubis/ • hxxps://www.entdark.net/2022/11/zanubis-updates-with-screenshot.html

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°109	Fecha: 10-05-2024 Página: 9 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en InfraSuite Device Master de Delta Electronics		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo deserialización de datos que no son de confianza que afecta a InfraSuite Device Master de Delta Electronics. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la ejecución remota de código.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-46604 de tipo deserialización de datos que no son de confianza, se debe a que InfraSuite Device Master de Delta Electronics ejecuta una versión vulnerable de Apache ActiveMQ (5.15.2).

Esta vulnerabilidad puede permitir que un atacante remoto con acceso de red a un broker o cliente OpenWire basado en Java ejecute comandos de shell arbitrarios manipulando tipos de clases serializadas en el protocolo OpenWire para hacer que el cliente o el broker (respectivamente) creen instancias de cualquier clase en el camino de clases.

A. Productos afectados:

- InfraSuite Device Master: versión 1.0.10 y anteriores.
- Apache ActiveMQ, versiones anteriores a 5.18.3.
- Módulo OpenWire heredado de Apache ActiveMQ, versiones anteriores a 5.18.3.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que aborda estas vulnerabilidades.
- Actualizar InfraSuite Device Master a la versión 1.0.11 o posterior.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-130-03

Índice alfabético