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

EL PERÚ PRIMERO

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

EJERCITO DEL PERU

MARINA DE GUERRA DEL PERU

FUERZA AEREA DEL PERU

DIRECCIÓN NACIONAL DE INTELIGENCIA DINI

asbanc ASOCIACIÓN DE BANCOS DEL PERÚ

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Lima, 14 de junio de 2020

N° 071-2020-PECERT

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 Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, en el marco del Centro Nacional de Seguridad Digital.

El objetivo de esta Alerta **es informar a los responsables de la Seguridad de la Información de las entidades públicas y las empresas privadas sobre las amenazas en el ciberespacio** 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 a 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. **Esta información no ha sido preparada ni dirigida a ciudadanos.**

Contenido

PERÚ Presidencia del Consejo de Ministros	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 071	Fecha: 14-06-2020
		Página: 3 de 10

Componente que reporta	**PECERT | EQUIPO DE RESPUESTAS ANTE INCIDENTES DE SEGURIDAD DIGITAL NACIONAL**			
Nombre de la alerta	Ataques contra dispositivos de almacenamiento conectado a la red (NAS) QNAP.			
Tipo de ataque	Ransomware		Abreviatura	Ransomware
Medios de propagación	Red, internet			
Código de familia	C	Código de subfamilia		C09
Clasificación temática familia	Código malicioso			

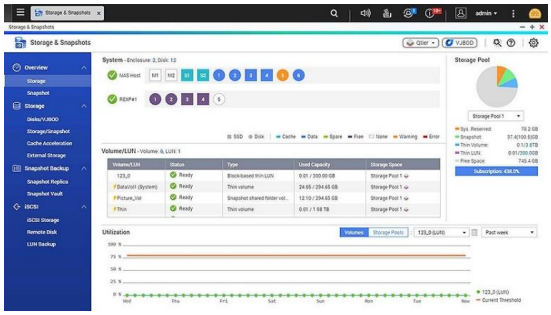
Descripción

1. Resumen

   El Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional, informa existe una versión de ransomware dirigidos contra dispositivos ONAP NAS.

2. Detalle de la alerta

   A través del monitoreo y búsqueda de amenazas en el ciberespacio, los ciberdelincuentes quienes están detrás del ransomware eCh0raix (MR1904) han lanzado una nueva ola de ataques contra dispositivos de almacenamiento conectado a la red (NAS) QNAP, y explota ciertas vulnerabilidades en versiones anteriores de QTS y Photo Station. Aprovechando vulnerabilidades publicadas en el 2019



   Las fallas se corrigen en las siguientes versiones del sistema operativo QTS:

   - QTS 4.4.2.1270 compilación 20200410 y posterior
   - QTS 4.4.1.1261 compilación 20200330 y posterior
   - QTS 4.3.6.1263 compilación 20200330 y posterior
   - QTS 4.3.4.1282 compilación 20200408 y posterior
   - QTS 4.3.3.1252 compilación 20200409 y posterior
   - QTS 4.2.6 compilación 20200421 y posterior

   Una vez que un dispositivo se ve comprometido, el ransomware, que encripta los archivos almacenados en el dispositivo y muestra una nota de rescate que exige aproximadamente $ 500 en bitcoin.

   Actualmente, no hay forma de recuperar archivos de forma gratuita. Sin embargo, los usuarios que han habilitado la función de instantánea basada en bloques de QNAP pueden recuperar sus archivos mediante instantáneas.

3. Recomendaciones frente a un ataque de ransomware
   - Deshabilitar powershell en aquellos equipos en los que no sea necesaria la ejecución de comandos en dicho lenguaje.
   - Si el antivirus ha logrado detectar un ransomware, no necesariamente la red está limpia.
   - No todas las soluciones de seguridad endpoint lo detectan.
   - Si tenemos dudas, pensar en aislar a nivel de red.
   - Pensar en soluciones EDR (Endpoint Detect & Response).
   - Las copias de seguridad deben permanecer aisladas.
   - El Directorio del Dominio debe ser reconstruido, reseteando las credenciales de todos los usuarios.
   - Tras la infección será necesaria la reinstalación de todos los equipos afectados, es importante realizar este paso y NO intentar limpiar los equipos porque es probable que haya una reinfección.
   - Sobre dichos equipos se deberá realizar una copia de seguridad de la información, incluso si éstos han sido cifrados por ransomware, manteniendo el cuidado y aislamiento adecuado.

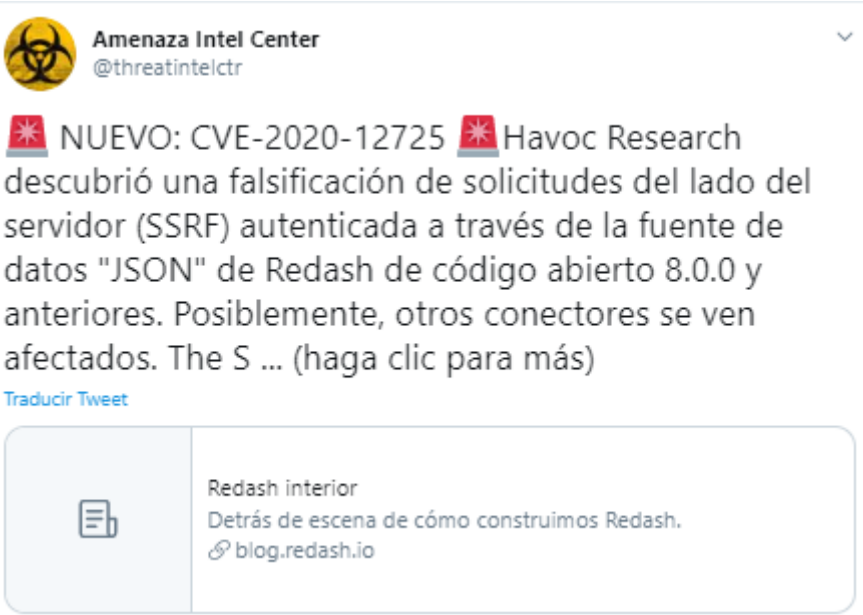
Fuentes de información	Equipo de Respuestas ante Incidentes de Seguridad Digital Nacional

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 071	Fecha: 14-06-2020
		Página: 4 de 10

Componente que reporta	**COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS**		
Nombre de la alerta	Vulnerabilidad de problema de código Redash		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. El 14 de junio del 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tuvo conocimiento de la publicación, sobre una vulnerabilidad de problema de código en Redash que fue descubierta por Havoc Research. El identificador asignado a esta vulnerabilidad es el CVE-2020-12725.
2. Redash, es un conjunto de soluciones de integración y análisis de datos de la compañía de israelí Redash. El cual admite integración de datos, visualización de datos, edición de consultas y uso compartido de datos. Esta herramienta de código abierto en la versión 8.0.0 y versiones anteriores del origen de datos “JSON” tienen una vulnerabilidad de problema de código. La vulnerabilidad surge del problema del diseño o implementación inadecuados en el proceso de desarrollo de código de sistemas o productos de red, debido a que la fuente de datos JSON proporciona mucha flexibilidad en términos de poder elaborar solicitudes HTTP, por ejemplo, al agregar encabezados, seleccionar cualquier verbo HTTP, etc. afectando la confidencialidad, integridad y disponibilidad.



3. Recursos afectados:
   - Redash de código abierto versiones 8.0.0 y versiones anteriores.
4. Se recomienda:
   - Instalar las actualizaciones del sitio del proveedor.

Fuentes de información	https[://]github.com/getredash/redash/issues/4869

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 071	Fecha: 14-06-2020
		Página: 5 de 10

Componente que reporta	**COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS**			
Nombre de la alerta	Vulnerabilidad de Cross-site Scripting en PI web API de OSIsoft			
Tipo de ataque	Explotación de vulnerabilidades conocidas		Abreviatura	EVC
Medios de propagación	Red, internet			
Código de familia	H	Código de subfamilia	H01	
Clasificación temática familia	Intento de intrusión			

Descripción

1. El 14 de junio del 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tuvo conocimiento de la publicación, sobre la vulnerabilidad de secuencia de comandos entre sitios en su PI Web API 2019, fue reportada por OSIsoft junto con Dor Yandeni y Eliad Mualem, de OTORIO. El identificador asignado a esta vulnerabilidad es el CVE-2020-12021.
2. OSIsoft PI Web API es una interfaz RESTful de un conjunto de sistemas PI, el producto admite aplicaciones cliente para leer y escribir el acceso a sus datos de AF y PI a través de HTTPS. Este producto es vulnerable a las secuencias de comando entre sitios, causada por la validación incorrecta de la entrada proporcionada por el usuario. Un atacante remoto autentificado podría aprovechar esta vulnerabilidad para ejecutar código arbitrario.

3. Recursos afectados:
   - PI Web API 2019 Patch 1 (1.12.0.6346) y todas las versiones anteriores.
4. Se recomienda:
   - Actualizar a la versión PI Web API 2019 SP1.
   - Instalar actualizaciones del sitio del proveedor.

Fuentes de información	https[://]www.incibe-cert.es/alerta-temprana/avisos-sci/vulnerabilidad-cross-site-scripting-pi-web-api-osisoft

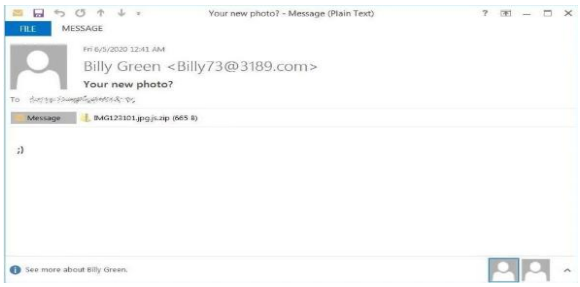
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 071	Fecha: 14-06-2020
		Página: 6 de 10

Componente que reporta	**CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Detección de malware Avaddon que infecta la red		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	Red, Navegación de Internet		
Código de familia	C	Código de subfamilia	C02
Clasificación temática familia	Código de malicioso		

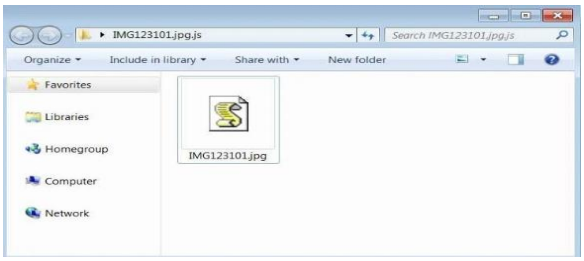
Descripción

1. El 14 de junio del 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tuvo conocimiento por expertos de una empresa de seguridad, sobre un malware 'Avaddon' cuyos desarrolladores han estado reclutando nuevos actores de amenazas y distribuidores de malware para infectar a tantas víctimas como sea posible, esta información fue publicada el 09 de junio del 2020 por la web de Noticias de Seguridad Informática.

2. Según los expertos de ciberseguridad, los hackers envían correos masivos con líneas de asunto como "¿Te gusta mi foto?" o "¿Esta es tu nueva foto?". El cuerpo del mensaje realmente no contiene fotos del usuario, sino que simplemente muestra una carita sonriente que oculta una herramienta de descarga de JavaScript para iniciar la infección de Avaddon.



3. Los hackers pueden enviar hasta 500 mil emails en periodos muy cortos de tiempo. El JavaScript adjunto a estos mensajes está disfrazado como un archivo JPG con nombres aleatorios (como IMG123101.jpg)



4. Se recomienda:

   - Tener un antivirus licenciado.
   - Debe tener un antimalware instalado.

Fuentes de información	https[://]noticiasseguridad.com/malware-virus/el-nuevo-ransomware-avaddon-viene-con-tu-foto-cuando-ves-tu-foto-se-infecta-tu-red/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 071	Fecha: 14-06-2020
		Página: 7 de 10

Componente que reporta	**CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Fallas en el firewall de palo alto permiten hackear la seguridad de red		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. El 14 de junio del 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se identificó a mediante especialistas en seguridad en redes inalámbricas, la revelación del hallazgo de al menos tres vulnerabilidades en PAN-OS, el software que se ejecuta en todas las soluciones de firewall de última generación de la firma de seguridad Palo Alto Networks. Acorde al reporte, la explotación de estas fallas de seguridad podría conducir a escenarios maliciosos como la ejecución de comandos.

2. La vulnerabilidad (CVE-2020-2027), existe debido a un límite dentro del componente authd del servidor de administración PAN-OS que permitiría a un administrador remoto escalar privilegios en el sistema objetivo. Un actor de amenazas podría enviar una solicitud especialmente diseñada al servicio de autenticación, desencadenar un desbordamiento de buffer y ejecutar código arbitrario con altos privilegios.

3. La vulnerabilidad (CVE-2020-2029), existe debido a una validación de entrada incorrecta que permitiría a los actores de amenazas escalar privilegios en el sistema. Un usuario autenticado podría enviar una solicitud especialmente diseñada para generar nuevos certificados y ejecutar comandos arbitrarios en PAN-OS. Esta vulnerabilidad también podría ser explotada de forma remota, aunque no existe un exploit asociado a este ataque.

4. La vulnerabilidad (CVE-2020-2028), existe debido a una validación de entrada incorrecta en el servidor de administración PAN-OS al cargar un nuevo certificado en modo FIPS-CC, lo que permitiría escalar privilegios en el sistema objetivo. Un administrador autenticado remoto puede pasar datos especialmente diseñados a la aplicación y ejecutar comandos arbitrarios del sistema operativo en el sistema de destino con privilegios de root, afirman los expertos en seguridad en redes inalámbricas.

5. Se recomienda:
   - Realizar las actualizaciones y configuraciones de seguridad de Palo Alto.

Fuentes de información	https[://]noticiasseguridad.com/vulnerabilidades/3-fallas-en-el-firewall-de-palo-alto-permiten-hackear-la-seguridad-de-red/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 071	Fecha: 14-06-2020
		Página: 8 de 10

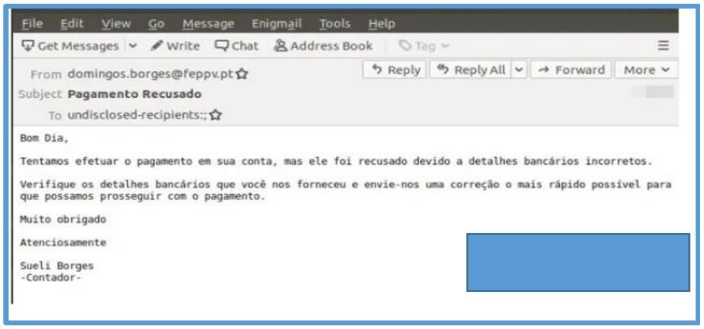
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**			
Nombre de la alerta	Detección de troyano TroyStealer			
Tipo de ataque	Troyano		Abreviatura	Troyano
Medios de propagación	USB, disco, red, correo, navegación de internet			
Código de familia	C	Código de subfamilia	C01	
Clasificación temática familia	Código malicioso			

Descripción

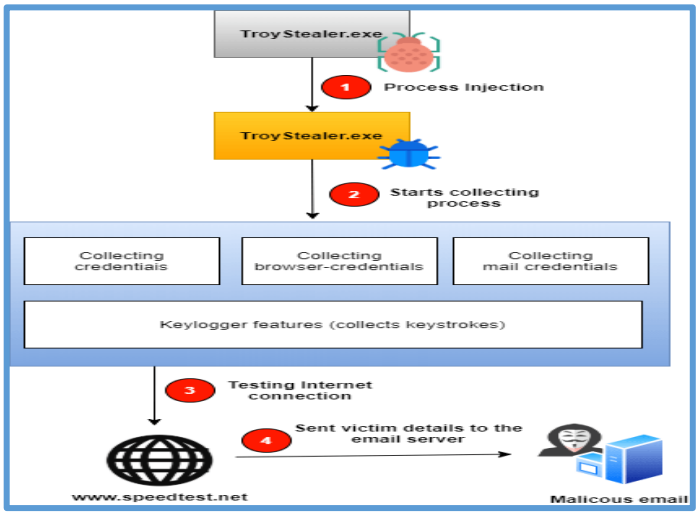
1. El 13 de junio del 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, en el sitio web securityaffairs.co, se informa sobre la aparición del Troyano "TroyStealer", el cual tiene la finalidad del robo de información y está dirigido a usuarios portugueses de internet.

   - El malware recopila información de inicio de sesión, como nombres de usuario y contraseñas almacenados en navegadores web, que envía a otro sistema por correo electrónico. Otra forma común de este malware es registrar las pulsaciones de teclas del usuario que pueden revelar información confidencial.

     - La propagación del malware es a través de correos electrónicos, enviados a usuarios de entidades bancarias, en idioma portugués.
     - Imágenes:



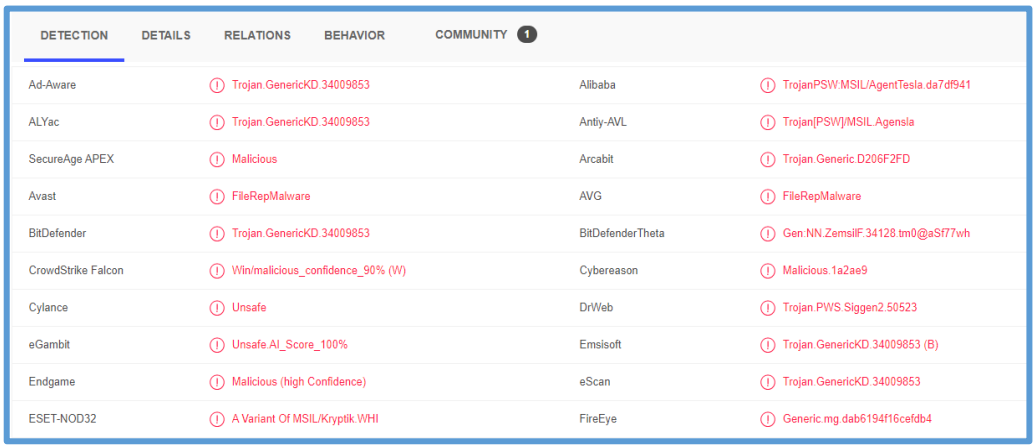
- Plantilla de correo electrónico TroyStealer (en portugués)



- Diagrama de Flujo del Malware TroyStealer

- Indicadores de Compromiso:

  - Nombre de Archivo: Paint.exe
    - Tipo: Win32 EXE
    - Tamaño: 317.00 KB (324608 bytes)
    - MD5: dab6194f16cefdb400e3fb6c11a76861
    - SHA-1: c76a9fb1a2ae927bf9c950338be5b391fed29cd7
    - SHA-256: 7c3289cdc59a8cf32feac66069d09c48a930d4665f740968521adaf870172644



DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY 1			
Ad-Aware	Trojan.GenericKD.34009853			Alibaba	TrojanPSW.MSIL/AgentTesla.da7df941		
ALYac	Trojan.GenericKD.34009853			Antiy-AVL	Trojan[PSW]/MSIL.Agensla		
SecureAge APEX	Malicious			Arcabit	Trojan.Generic.D206F2FD		
Avast	FileRepMalware			AVG	FileRepMalware		
BitDefender	Trojan.GenericKD.34009853			BitDefenderTheta	Gen:NN.ZemsilF.34128.tm0@aSf77wh		
CrowdStrike Falcon	Win/malicious_confidence_90% (W)			Cybereason	Malicious.1a2ae9		
Cylance	Unsafe			DrWeb	Trojan.PWS.Siggen2.50523		
eGambit	Unsafe.AI_Score_100%			Emsisoft	Trojan.GenericKD.34009853 (B)		
Endgame	Malicious (high Confidence)			eScan	Trojan.GenericKD.34009853		
ESET-NOD32	A Variant Of MSIL/Kryptik.WHI			FireEye	Generic.mg.dab6194f16cefdb4		

  - Archivo Asociado:
    - Nombre: troystealer.exe
    - SHA-256: 7c3289cdc59a8cf32feac66069d09c48a930d4665f740968521adaf870172644

Antivirus	Amenaza
FireEye	Generic.mg.dab6194f16cefdb4
McAfee	Artemis! DAB6194F16CE
CrowdStrike	win / malware_confidence_70% (D)
Invincea	heuristico
BitDefenderTheta	Gen: NN.ZemsilF.34128.tm0@aSf77wh
ESET-NOD32	una variante de MSIL / Kryptik.WHI
APENDICE	Malicioso
Kaspersky	HEUR: Trojan-PSW.MSIL.Agensla.gen
Juego final	malicioso (alta confianza)
McAfee-GW-Edition	BehavesLike.Win32.Generic.fc
Alarma de zona	HEUR: Trojan-PSW.MSIL.Agensla.gen
Microsoft	Troyano: Win32 / Wacatac.C! Ml
Centinela	DFI - PE malicioso

2. Referencia:

   Exe: significa es una extensión que se refiere a un archivo ejecutable de código reubicable, es decir, sus direcciones de memoria son relativas. Los sistemas operativos que utilizan de forma nativa este formato son DOS, Microsoft Windows, OS/2 y ReactOS.

3. Algunas Recomendaciones:
   - Verifica las Aplicaciones en otros sitios web.
   - Verifica la Reputación de las Aplicaciones.
   - Descarga Aplicaciones de sitios seguros.
   - Desconfías de Aplicaciones gratuitas.
   - Ten presente que, los ciberdelincuentes buscan la oportunidad para infectar tu dispositivo.

Fuentes de información	https[://]www.hackread.com/adware-barcode-reader-apps-on-play-store/

Índice alfabético