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, 9 de junio de 2020

N° 066-2020-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° 066	Fecha: 09-06-2020
		Página: 3 de 21

Componente que reporta	**PECERT | EQUIPO DE RESPUESTAS ANTE INCIDENTES DE SEGURIDAD DIGITAL NACIONAL**			
Nombre de la alerta	Ciberataque a usuarios de la red social LinkedIn			
Tipo de ataque	Phishing		Abreviatura	Phishing
Medios de propagación	Redes sociales y correo electrónico			
Código de familia	G	Código de subfamilia	G01	
Clasificación temática familia	Fraude			

Descripción

1. Resumen

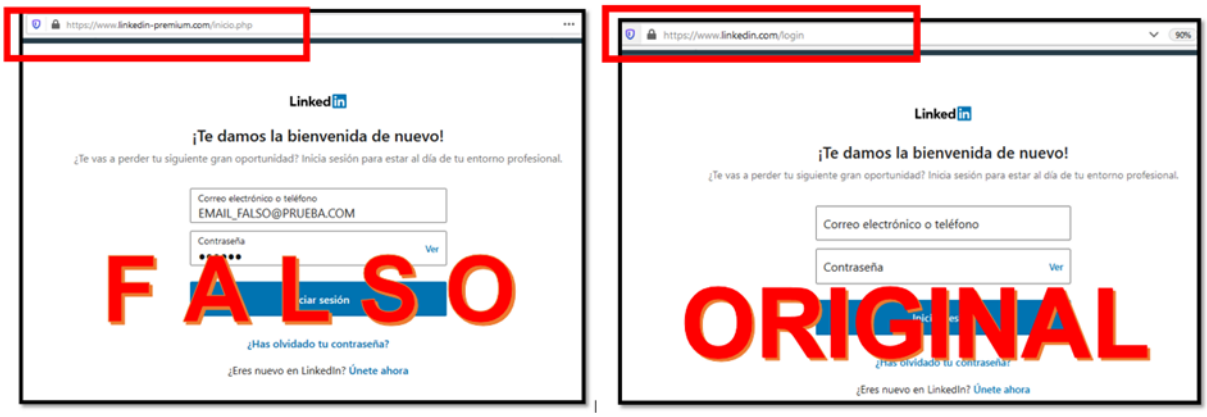
   El Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional, advierte sobre una campaña de "phishing" que se está difundiendo a través de redes sociales y cuentas de correo electrónico con contenido falso que aparentemente proviene de la red social LinkedIn.

2. Detalle

   El mensaje indica al usuario sobre una campaña para obtener una cuenta Premium en la red social LinkedIn ingresando al siguiente enlace https[://]lnkd.in/e6Yk6s5 y al presionar re-direcciona a la URL https[://]www.linkedin-premium.com/inicio.php la cual suplanta a la página web oficial de la citada red social, seguidamente le solicita al usuario ingresar sus credenciales (usuario y contraseña) para iniciar la sesión. Una vez ingresado los datos, se expone al robo de sus credenciales.

3. Indicadores de compromiso
   - URL sitio falso : https[://]lnkd.in/e6Yk6s5.
   - URL Redirecciones : https[://]www.linkedin-premium.com/inicio.php
   - IP : 185[.]173[.]235[.]4
   - Localización : Netherlands
   - Asunto : Obtén tu cuenta Premium en Linkedin de forma gratuita.

4. Imágenes



https://www.linkedin-premium.com/inicio.php

https://www.linkedin.com/login

5. Recomendaciones:
   - Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
   - Evaluar el bloqueo preventivo de los indicadores de compromisos.
   - Revisar los controles de seguridad de los AntiSpam.
   - Visualizar los sitios web que se ingresen sean los oficiales.
   - Realizar concientización constante a los usuarios sobre este tipo de amenaza.

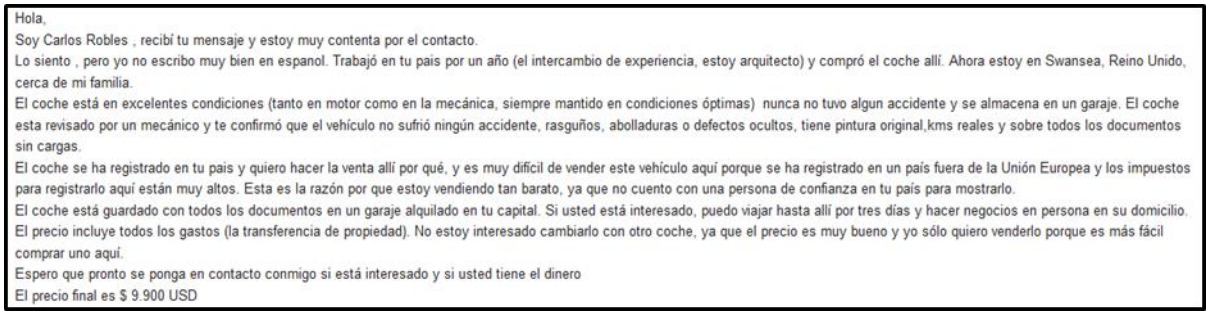
Fuentes de información	Equipo de Respuestas ante Incidentes de Seguridad Digital Nacional

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 066	Fecha: 09-06-2020
		Página: 4 de 21

Componente que reporta	**COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS**			
Nombre de la alerta	Cuidado con el "phishing car", estafa en la venta de coches por internet			
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 subfamilia	G02	
Clasificación temática familia	Fraude			

Descripción

1. El 09 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tuvo conocimiento que en España se comercializan más vehículos usados que nuevos. En 2019, se vendieron 2,23 millones de unidades de ocasión, una cifra superior a la del ejercicio anterior. Este dato lo ha facilitado la Asociación Nacional de Vendedores de Vehículos a Motor, Reparación y Recambios (Ganvam), que asegura que por cada ejemplar nuevo se venden 1,7 de segunda mano. Y una parte de estas transacciones se lleva a cabo entre particulares, lo que aumenta el riesgo de estafa.
2. Existen grupos organizados que se dedican a realizar timos a través de internet, en lo que se conoce como "phishing car". Normalmente utilizan portales de compra-venta de vehículos para publicar anuncios falsos utilizando fotos de coches reales que están a la venta. Esto dificulta identificar el timo de primeras. Sin embargo, hay indicios que deben activar las alertas del comprador para no caer en la trampa.
3. El primero es el precio del ejemplar, en numerosos casos más bajo que la media para atraer a las víctimas. Otra señal que debe levantar sospechas es que cuando el interesado pide ver el coche personalmente, el supuesto vendedor le dice que éste se encuentra fuera de la zona y que para traerlo necesita que le dé un avance de dinero. Lo más probable es que le pida que realice una transferencia a través de alguna empresa de envío de dinero, con la que no se puede rastrear el destinatario del envío.



Hola,
Soy Carlos Robles , recibí tu mensaje y estoy muy contenta por el contacto.
Lo siento , pero yo no escribo muy bien en espanol. Trabajó en tu pais por un año (el intercambio de experiencia, estoy arquitecto) y compró el coche allí. Ahora estoy en Swansea, Reino Unido, cerca de mi familia.
El coche está en excelentes condiciones (tanto en motor como en la mecánica, siempre mantido en condiciones óptimas) nunca no tuvo algun accidente y se almacena en un garaje. El coche esta revisado por un mecánico y te confirmó que el vehículo no sufrió ningún accidente, rasguños, abolladuras o defectos ocultos, tiene pintura original,kms reales y sobre todos los documentos sin cargas.
El coche se ha registrado en tu pais y quiero hacer la venta allí por qué, y es muy difícil de vender este vehículo aquí porque se ha registrado en un país fuera de la Unión Europea y los impuestos para registrarlo aquí están muy altos. Esta es la razón por que estoy vendiendo tan barato, ya que no cuento con una persona de confianza en tu país para mostrarlo.
El coche está guardado con todos los documentos en un garaje alquilado en tu capital. Si usted está interesado, puedo viajar hasta allí por tres días y hacer negocios en persona en su domicilio.
El precio incluye todos los gastos (la transferencia de propiedad). No estoy interesado cambiarlo con otro coche, ya que el precio es muy bueno y yo sólo quiero venderlo porque es más fácil comprar uno aquí.
Espero que pronto se ponga en contacto conmigo si está interesado y si usted tiene el dinero
El precio final es $ 9.900 USD

4. Con el objetivo de conseguir engañar a la víctima dando credibilidad al asunto, los timadores pueden enviarle fotos detalladas del vehículo e incluso la documentación del mismo. Para conseguir este material, previamente se hacen pasar por compradores interesados en un automóvil que está realmente a la venta -el mismo que es objeto de la estafa- y le piden al propietario que, antes de cerrar el trato, quieren que les mande imágenes detalladas del automóvil, así como el permiso de circulación y la ficha de la ITV.
5. Se recomienda:
   - No abrir correos de usuarios desconocidos o que no se haya solicitado.
   - No abrir, ni descargar archivos adjuntos a correos, SMS, redes sociales de usuarios de dudosa procedencia.
   - No ingresar a páginas sospechosas.
   - No proporcionar datos bancarios.

Fuentes de información	https[://]www.lavanguardia.com/motor/actualidad/20200609/481004612343/phishing-car-estafa-compra-venta-coches-ocasion-segunda-mano-internet.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 066	Fecha: 09-06-2020
		Página: 5 de 21

Componente que reporta	**CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Falla crítica en los enrutadores Cisco IOS permite hackers remotos tomar el control completo de los sistemas		
Tipo de ataque	Troyanos	Abreviatura	Troyanos
Medios de propagación	USB, disco, red, correo, navegación de internet		
Código de familia	C	Código de subfamilia	C02
Clasificación temática familia	Código malicioso		

Descripción

1. El 09 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se encontró información que se detalla a continuación: Recientemente, Cisco ha anunciado que ha solucionado muchas vulnerabilidades en los enrutadores Cisco IOS, incluidas más de una docena de vulnerabilidades que afectan a los enrutadores y conmutadores industriales de la compañía.

2. Uno de los problemas críticos más serios es CVE-2020-3205, que permite a un atacante no autenticado ejecutar comandos de shell arbitrarios en un servidor VDS. Un atacante puede explotar esta falla de seguridad simplemente enviando paquetes especialmente diseñados al dispositivo de la víctima, y un ataque exitoso puede llevar a un compromiso completo del sistema.

3. La vulnerabilidad CVE-2020-3198 también es similar a la primera. Como permite que un atacante no autenticado ejecute de forma remota el código arbitrario en el sistema vulnerable, eso simplemente causa un bloqueo y luego reinicia el dispositivo, enviando los paquetes maliciosos al dispositivo. Estos problemas afectan a los enrutadores industriales Cisco ISR 809 y 829 y también a las CGR de la serie 1000.

4. En la falla CVE-2020-3227, el problema es con los controles de autorización para la infraestructura Cisco IOx en Cisco IOS XE. Como el error permite que un atacante sin credenciales y autorización acceda a la API Cisco IOx y ejecute comandos de forma remota.

5. La falla de seguridad CVE-2020-3205 está presente en el canal entre máquinas virtuales del software Cisco IOS para los enrutadores Cisco 809, Cisco 829 y Cisco 1000 Series (CGR1000); Estos son los enrutadores diseñados en una arquitectura de hipervisor. Y esto podría permitir fácilmente que un atacante no autenticado ejecute comandos de shell arbitrarios VDS del dispositivo afectado.

6. Se recomienda:

   Para usar estas fallas de seguridad, se requerirá autenticación, acceso local o actividad de funciones que están deshabilitadas por defecto. Algunas de las vulnerabilidades de alta gravedad están relacionadas con IOx, ya que permiten a los atacantes escribir y modificar los archivos arbitrarios, dirigir ataques DoS y ejecutar código arbitrario con derechos elevados.

Fuentes de información	https[://]gbhackers.com/flaws-in-cisco-ios-routers/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 066	Fecha: 09-06-2020
		Página: 6 de 21

Componente que reporta	**CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Operadores de eCh0raix Ransomware, apuntan a dispositivos de almacenamiento QNAP en una nueva campaña.		
Tipo de ataque	Ataque de fuerza Bruta	Abreviatura	AtaqFueBru
Medios de propagación	Red, Correo, Navegación de Internet		
Código de familia	A	Código de subfamilia	A01
Clasificación temática familia	Acceso no autorizado		

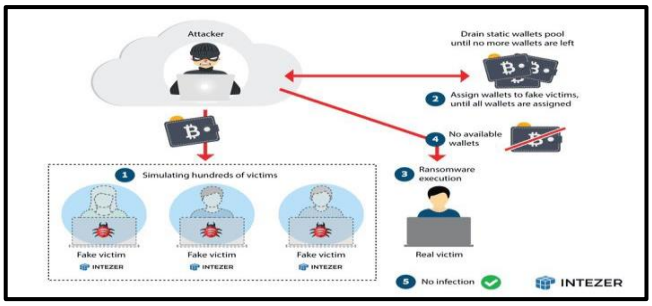
Descripción

1. El 09 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se encontró información que se detalla a continuación: Actores de la amenaza detrás del eCh0raix Ransomware han lanzado una nueva campaña destinada a infectar los dispositivos de almacenamiento QNAP. El ransomware se dirige a servidores NAS poco protegidos o vulnerables fabricados por QNAP Systems con sede en Taiwán, los atacantes explotan vulnerabilidades conocidas o llevan a cabo ataques de fuerza bruta.

2. Los ransomware " QNAPCrypt " y " eCh0raix ", están escrito en el lenguaje de programación Go y utiliza el cifrado AES. El código malicioso agrega la extensión .encrypt a los nombres de archivos cifrados. Desde inicios de junio expertos de BleepingComputers observaron un aumento en el número de usuarios que informaron infecciones con eCh0raix en sus foros.

3. Los hackers están apuntando a dispositivos QNAP que intentan explotar vulnerabilidades bien conocidas o forzando contraseñas débiles por fuerza bruta. QNAP lanzó un dispositivo de seguridad para el siguiente NAS que podría ser explotado por los atacantes para inyectar código malicioso o ejecutar código remoto. Un atacante podría desencadenar estos problemas para instalar el ransomware en dispositivos vulnerables.

4. Los delincuentes exigen $ 500 en bitcoin para descifrar los archivos, las instrucciones para pagar el rescate se incluyen en la nota "README_FOR_DECRYPT.txt" que se encuentra en el dispositivo. Los expertos advierten que, a diferencia de las versiones anteriores del ransomware eCh0raix, esta última no permite a las víctimas recuperar archivos de forma gratuita.



5. Se recomienda:

   - Asegurar de estar utilizando las últimas versiones del firmware del servidor, ya que este ransomware utiliza varios exploits para ganar privilegios dentro del sistema.
   - Es recomendable habilitar los sistemas de doble autenticacion para reducir la probabilidad de que usuarios no autorizados se conecten a nuestro servidor.

Fuentes de información	https[://]securityaffairs.co/wordpress/104365/malware/ech0raix-ransomware-qnap.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 066	**Fecha: 09-06-2020**
		Página: 7 de 21

Componente que reporta	**CIBERDEFENSA Y TELEMÁTICA DEL EJÉRCITO DEL PERÚ**			
Nombre de la alerta	Vulnerabilidades en base de datos Adaptive Server Enterprise			
Tipo de ataque	Explotación de vulnerabilidades		Abreviatura	EVC
Medios de propagación	Red, Navegación de internet			
Código de familia	H	Código de subfamilia	H01	
Clasificación temática familia	Intento de intrusión			

Descripción

1. El 09 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tuvo conocimiento del informe de los especialistas en seguridad web, sobre la vulnerabilidad del SAP (proceso de información de sistemas y aplicaciones) de la base de datos Adaptive Server Enterprise este tipo de proceso es empleado por empresas a nivel mundial, esta información fue publicada el 03 de junio de 2020 por la web de Noticias de seguridad informática.

2. Una de las vulnerabilidades está relacionada con los controles de autorización para la infraestructura de hosting de aplicaciones de Cisco IOS XE Software. Esta condición permite a los hackers remotos no autenticados ejecutar comandos de API sin la autenticación requerida.

3. El software IOx administra de forma errónea las solicitudes de tokens de autorización, lo que permite a los actores de amenazas explotar la vulnerabilidad empleando una llamada API especialmente diseñada para solicitar el token y ejecutar comandos API IOx en el dispositivo.

4. Se recomienda:

   Instalar las actualizaciones y parches de la página oficial de Cisco.

Fuentes de información	https[://]noticiasseguridad.com/vulnerabilidades/vulnerabilidades-de-sap-adaptive-server-enterprise-rompen-la-seguridad-de-red-y-base-de-datos/

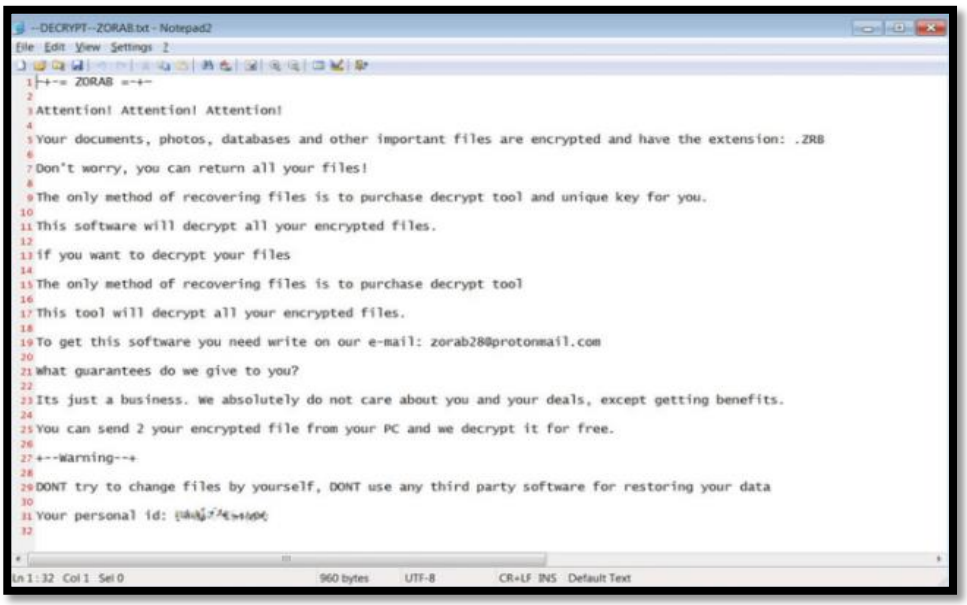
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 066	Fecha: 09-06-2020
		Página: 8 de 21

Componente que reporta	**COMANDANCIA DE CIBERDEFENSA DE LA MARINA DE GUERRA DEL PERÚ**		
Nombre de la alerta	Herramienta para descifrar ransomware infecta el sistema.		
Tipo de ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros.		
Código de familia	C	Código de subfamilia	C09
Clasificación temática familia	Código malicioso.		

Descripción

1. El 09 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se identificó una herramienta para protegerse de los ataques de ransomware llamado **STOP DJVU**, el cual se aprovecha de los usuarios que puedan estar desesperados buscando la manera de descifrar su equipo y no tener que pagar una cantidad importante de dinero, para infectar nuevamente el equipo, hoy en día tiene más víctimas diariamente que la suma de otras variedades más populares como Maze, REvil, Netwalker y DoppelPaymer. Además, se trata de un malware que ataca especialmente a usuarios domésticos, frente a otras variedades que están más orientadas en empresas.

2. Asimismo; se ofrece en la red un programa capaz de descifrar el ransomware STOP Djvu. El problema es que cuando la víctima lo ejecuta lo que hace no es descifrar el ransomware, sino que crea otra capa de cifrado adicional. De nombre **ZORAB,** este ransomware agregará la extensión .ZRB a los archivos. A partir de ahí actúa como cualquier otro ransomware: nos muestra un documento para contactar con los atacantes y así tener las instrucciones de pago.



3. Se recomienda:
   - Evitar abrir correos de remitentes desconocidos.
   - No instalar softwares desconocidos y sin analizar.
   - Evitar abrir enlaces no solicitados o de dudosa procedencia.
   - Realizar copias de seguridad de datos.
   - Mantener los equipos protegidos y actualizado.

Fuentes de información	Comandancia de Ciberdefensa de la Marina, OSINT.

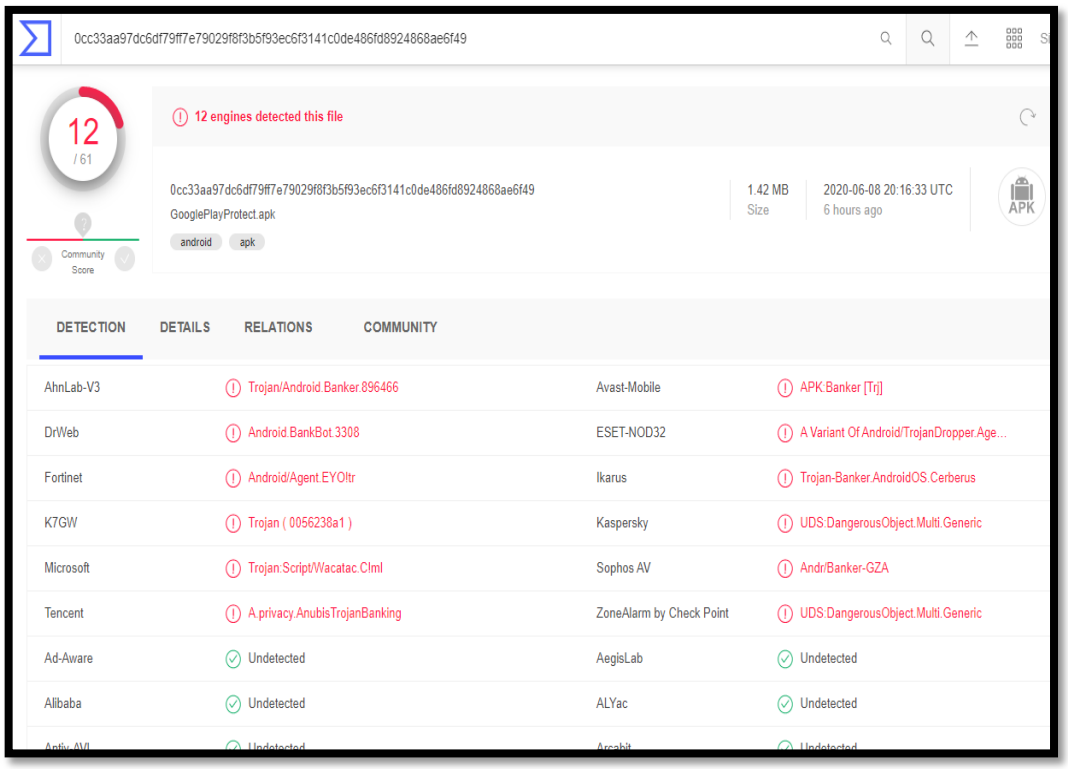
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 066	Fecha: 09-06-2020
		Página: 9 de 21

Componente que reporta	**COMANDANCIA DE CIBERDEFENSA DE LA MARINA DE GUERRA DEL PERÚ**		
Nombre de la alerta	Malware se hace pasar por aplicación que brinda seguridad y protección a dispositivos Android		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	Red, Correo electrónico.		
Código de familia	C	Código de subfamilia	C03
Clasificación temática familia	Código malicioso		

Descripción

1. El 09 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se identificó un aplicativo fraudulento de nombre "GooglePlayProtect.apk" circulando principalmente por redes sociales, invitando a los usuarios a descargar e instalarlo, para proteger su dispositivo Android contra apps dañinas, que en su lugar sería una aplicación maliciosa.

2. Se analizó el citado aplicativo en la página web "Virus Total" donde es catalogado como malicioso.



3. Se recomienda:
   - Evitar ingresar a enlaces no confiables.
   - Evitar descargar y abrir archivos de fuentes no confiables.
   - Mantener los equipos protegidos, con el software actualizado.

Fuentes de información	Comandancia de Ciberdefensa de la Marina, OSINT.

	ALERTA INTEGRAL DE SEGURIDAD DIGITAL N° 066	**Fecha : 09-06-2020**
		Página: 10 de 21

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA FUERZA AÉREA DEL PERÚ**		
Nombre de la alerta	Defacement a la página web de la Defensoría del Pueblo de Ecuador		
Tipo de ataque	Modificación del sitio web	Abreviatura	ModSitWeb
Medios de propagación	Red, internet		
Código de familia	L	Código de subfamilia	L01
Clasificación temática familia	Vandalismo		

Descripción

1. El 09 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó en la red Social Twitter, al usuario con el nombre **"Sin1peCrew" (@sin1pecrew),** quien publicó un (01) link, donde se muestra el ataque denominado "Defacement" (ataque a un sitio web que cambia la apariencia visual de una página web), realizado a la página web de la Defensoría del Pueblo de Ecuador.

Cabe mencionar, que los administradores de la página web, al percatarse de lo sucedido, iniciaron un plan de contingencia, que les permitió a los usuarios trabajar con normalidad.

2. Se recomienda:

Los administradores de red de las áreas de informática, deben extremar medidas y políticas de seguridad en las configuraciones de las páginas web del estado.

Fuentes de información	https[://]twitter.com/sin1pecrew/status/1270275589577080834

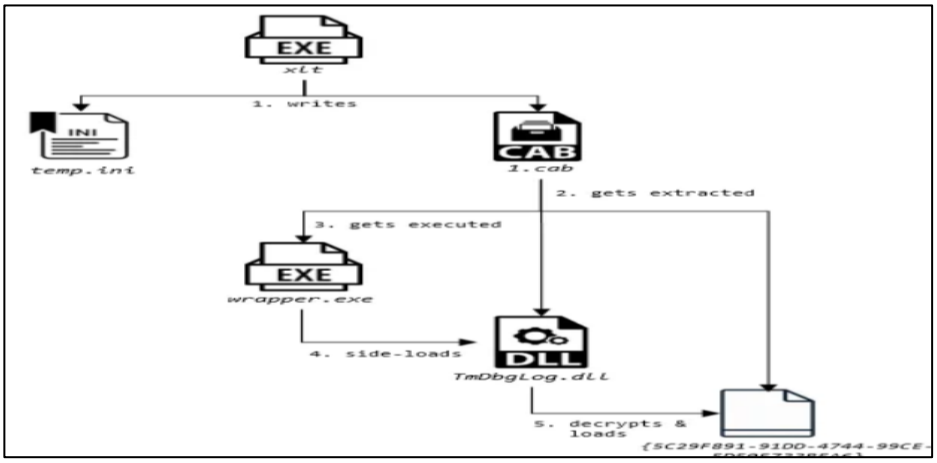
	ALERTA INTEGRAL DE SEGURIDAD DIGITAL N° 066		Fecha : 09-06-2020
			Página: 11 de 21
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA FUERZA AÉREA DEL PERÚ		
Nombre de la alerta	Malware “CCycldek”, afecta a diversas computadoras		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, disco, red, correo, navegación por internet		
Código de familia	C	Código de subfamilia	C02
Clasificación temática familia	Código malicioso		

Descripción

1. El 09 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que los investigadores de ciberseguridad de Israel descubrieron un nuevo malware denominado “CCyldek”, que sustrae información de las computadoras por los puertos USB, modalidad que se han venido utilizando por mucho tiempo. El malware en mención tiene nuevas funcionalidades, dentro de ellos destaca, la infección por vulnerabilidades conocidas de Office como CVE-2012-0158, CVE-2017-11882 o CVE-2018-0802, introduciendo el malware NewCore RAT.

2. Cabe indicar que, el modo de operar del malware consiste en extraer información mediante la descarga de herramientas adicionales para facilitar “movimientos laterales” e introducir el malware. Entre ellos, se encuentra el HDoor, un popular foro de hackeo chino, donde se realizan escaneos de redes internas y crear VPN en ordenadores infectados para evitar detecciones de red y saltarse los proxis, esto les permite extraer información del ordenador aislado si éste es accesible desde una red local, pero no está conectado de manera directa.

3. Asimismo, se encuentran otras herramientas denominadas JsonCookies (utilizada para robar cookies de bases de datos SQLite) y ChromePass (permite robar contraseñas guardadas en el navegador). Además, entre esas herramientas adicionales se encuentra USBCulprit, capaz de escanear diversas rutas del ordenador buscando archivos PDF, DOC, WPS, DOCX, PPT, XLS, XLSX, PPTX y RTF, y exportarlos a una unidad USB conectada al ordenador.



4. Se recomienda:

   Los administradores de los equipos informáticos, deben prever medidas preventivas para la infección por parte del malware.

Fuentes de información	http[://]www.enhacke.com/2020/06/08/un-nuevo-malware-roba-informacion-de-tu-pc-incluso-si-no-tienes-internet/

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 066**	**Fecha: 09-06-2020**
		Página: 12 de 21

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**			
Nombre de la alerta	Nueva campaña de distribución de malware “Metamorfo”			
Tipo de ataque	Malware		Abreviatura	Malware
Medios de propagación	USB, disco, red, correo, navegación de internet			
Código de familia	C	Código de subfamilia	C03	
Clasificación temática familia	Código malicioso			

Descripción

1. Resumen:

   Los investigadores de Bitdefender han descubierto una nueva campaña que utiliza como vector de ataque el secuestro de la biblioteca de enlaces dinámicos (DLL). El actor de esta amenaza llamado “Metamorfo” es conocido por atacar a usuarios de la banca brasileña. La campaña está dirigida principalmente a usuarios brasileños, pero también se ha detectado infecciones en Suiza y Argentina.

   Metamorfo es una potente pieza de malware, cuya capacidad principal es el robo de información bancaria y otros datos personales del usuario y su filtración al servidor de Comando y Control (C2). El malware también intenta descargar otros archivos del servidor C2, lo que sugiere que también podría descargar una versión actualizada de sí mismo con un conjunto de comandos extendido.

2. Detalles:

   El malware llega al sistema en un instalador MSI que parece legítimo para el usuario. Sin embargo, los atacantes han manipulado el archivo para incluir algunos archivos legítimos junto con el ejecutable de destino y la DLL maliciosa. Tras la ejecución, el programa instala el componente legítimo y el malware en una subcarpeta, ya sea en la carpeta de la biblioteca de un usuario público (Documentos, Música, Imágenes, Videos o Descargas) o en ProgramData. Una vez completada la instalación, ejecuta el binario legítimo que carga automáticamente la DLL maliciosa.

   Cuando comienza la ejecución, el proceso de destino carga sus archivos DLL importados, incluido el malicioso. Además de ejecutar el código desde la rutina de inicio de la DLL, la aplicación legítima se ejecuta como lo haría en un escenario limpio. La DLL de malware tiene todas sus funciones exportadas apuntando a la misma dirección en el código. Por lo tanto, una llamada legítima desde la aplicación limpia activa la ejecución del código malicioso.

   Los autores de malware utilizan con frecuencia Delphi, ya que esto permite la creación rápida de prototipos de una GUI para su ejecutable, por lo que tiene muchas bibliotecas estándar, fácilmente integrables en un solo archivo ejecutable. La ventaja de tener todo el código malicioso en una DLL es que las acciones maliciosas parecen ser realizadas por el proceso legítimo. Por lo tanto, el atacante podría evadir la detección de comportamiento si los binarios con una firma digital de confianza están en la lista blanca. La información de la versión de la DLL maliciosa imita la de la limpia.

   La DLL tiene un mecanismo de verificación para que no se ejecute a menos que la computadora esté configurada con configuraciones regionales brasileñas. Después de verificar los requisitos del entorno brasileño, el malware crea un mutex con un nombre aparentemente aleatorio (holexrel), para garantizar que no ejecute el mismo código malicioso cada vez que el proceso de limpieza llama a una de las funciones exportadas. Luego crea una copia del archivo ejecutable legítimo original en la misma carpeta donde se ejecuta desde, pero bajo otro nombre aleatorio con una extensión .EXE, .SCR o .PIF. A continuación, escribe un script VBS en AppData \ Roaming \ Microsoft \ Windows \ Start Menu \ Programs \ Startup \ con un nombre aleatorio para asegurar la persistencia. Si ya hay un archivo de script en esa ubicación, el malware lo elimina.

   El script es responsable de iniciar el ejecutable legítimo, ejecutando la DLL maliciosa junto a él cada vez que se inicia la computadora. El script crea una instancia del objeto COM WScript.Shell, con CLSID {72c24dd5-d70a-438b-8a42-98424b88afb8}, así como FileSystemObject con CLSID {0d43fe01-f093-11cf-8940-00a0c9054228}. El método de referir objetos COM en lugar de interactuar directamente con el sistema de archivos y procesos a través de funciones integradas que ayuda a evadir los mecanismos de detección clásicos.

   El contenido de la VBS descartada es similar al siguiente, y solo los nombres de las variables son aleatorios. El script verifica si la DLL de carga lateral está presente en la misma carpeta que el ejecutable, luego inicia el EXE.

   El malware busca algún software relacionado con la banca en el sistema y espera a que el usuario acceda a las páginas bancarias. Los supervisa mirando los títulos de las ventanas y comparándolos con un conjunto de cadenas.

   Luego intenta conectarse a buleva [.] Webcindario [.] Com, que se traduce en IP 5[.]57[.]226[.]202. Esta IP se ha

utilizado anteriormente para varias resoluciones de nombres. Estos nombres de dominio confunden a los usuarios ya que parecen legítimos, excepto por la parte webcindario [.] Com (por ejemplo, bankofamerica [.] Webcindario [.] Com, disney [.] webcindario [.] com).

El malware también es capaz de descargar archivos del servidor C2 en la misma carpeta con nombres aleatorios. Finalmente, el ejecutable sigue ejecutándose en segundo plano, esperando los comandos del servidor. Es capaz de registrar pulsaciones de teclas en el sistema cuando el usuario completa una contraseña en una de las páginas bancarias. También puede deshabilitar la función de autocompletar de los navegadores para que el usuario tenga que volver a escribir la contraseña manualmente.

El malware también tiene la capacidad de capturar capturas de pantalla con la ayuda de la API de ampliación de Windows, importada desde Magnification.dll. Se ha capturado algunos de los comandos junto con los nombres de las aplicaciones buscadas, los nombres de los archivos y los recursos web al descifrar los recursos del malware.

El directorio de recursos de la DLL contiene algunas imágenes que imitan las notificaciones de seguridad de varios bancos brasileños, engañando al usuario para que crea que algo sucedió con su cuenta bancaria. Este pánico se puede utilizar en beneficio del atacante para robar información confidencial.

3. Indicadores de Compromiso (IoC):

   Hash

   - a9effadaaf45280c79984be5266e829b, 3c212baf7e6dc3f279339e978ee97bd6,
   - 1056133be70f5ab824e2508a8c3045a8, 71f7436994df0b6cd9b1b080c5a8093f,
   - 35ac5e66364658bbdbcb39737e9a347c, 9eb538a6ec86ced18237cc99e37cf2c9,
   - 8b0845c2847a13126dfc59582835f6fd, 4685fbd6a4dfbae8c4c0d09d925f63a8,
   - 78b91c3e56c5c0466e3490e91d9ef0bd, f1a74b3e266126ed8edde3d819bfe864,
   - 3e28dca2d50c26c7e22cf9f7c716b0bb, 1602c73365718cba8599dc6fcc06c175,
   - d31d8cd4230ac53ab8c564a44e5a7a0d, 85c83ec905de2e99b19c6d0ce5027d00,
   - 19a9b387eea6936cf93b0b21db62d49d, db4f176c985fe2f801d4f8e19f01f323,
   - e15304e98d2f65f16889d2ade97fe687, 3a64344ac4c9c5f3e0f4bb47a3303d4a,
   - 1b1dc38264689840d8243cc6c2717e4b

   URL

   - hxxp://buleva[.]webcindario[.]com/my/
   - Más URL, aquí.

   Dirección IP

   - 5[.]57[.]226[.]202

   Archivos de descarga

   - Los nombres de los archivos .vbs descartados son aleatorios, por ejemplo: \ AppData \ Roaming \ Microsoft \ Windows \ Menú Inicio \ Programas \ Inicio \ shzvmmraec.vbs

4. Recomendaciones:
   - Asegúrese de que el software antivirus y los archivos asociados estén actualizados.
   - Mantenga las aplicaciones y los sistemas operativos en ejecución en el nivel de parche lanzado actualmente.
   - No abrir archivos adjuntos o enlaces web que en correos electrónicos recibidos que son irrelevantes, y/o enviados desde direcciones desconocidas y sospechosas.
   - Todo el software y los archivos deben descargarse de sitios web oficiales y confiables y a través de enlaces directos.
   - Busque signos existentes de los IoC indicados en su entorno.
   - Considere bloquear y / o configurar la detección de todas las IoC basadas en URL e IP.
   - Concientizar constantemente a los usuarios en temas relacionados a seguridad informática.

Fuentes de información	hxxps://www.bitdefender.com/files/News/CaseStudies/study/333/Bitdefender-PR-Whitepaper-Metamorfo-creat4500-en-EN-GenericUse.pdf

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 066	Fecha: 09-06-2020
		Página: 14 de 21

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**			
Nombre de la alerta	Detección de Ransomware Avaddon.			
Tipo de ataque	Ransomware		Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros			
Código de familia	C	Código de subfamilia	C09	
Clasificación temática familia	Código malicioso			

Descripción

5. El 08 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, en el sitio web pcrisk.com, se informa sobre la aparición del Ransomware Avaddon, el cual cifra los archivos de la víctima con el algoritmo de cifrado AES y la clave AES mediante el algoritmo RSA. Además, cambia el fondo de escritorio y renombra todos los archivos agregando la extensión " .avdn ". Por ejemplo, cambia el nombre de un archivo llamado " 1.jpg " a " 1.jpg.avdn ", " 2.jpg " a " 2.jpg.avdn ", y así sucesivamente.
6. Por lo general, los usuarios infectan las computadoras con malware (incluido el ransomware) a través de campañas de Malspam, activadores y actualizadores de software no oficiales, canales de descarga de software y archivos no confiables y troyanos. Es común que los ciberdelincuentes utilicen campañas de spam como herramientas para proliferar malware enviando correos electrónicos con archivos adjuntos maliciosos o enlaces a sitios web diseñados para descargar archivos maliciosos. Intentan engañar a los usuarios para que ejecuten un archivo malicioso al disfrazar sus correos electrónicos como importantes, oficiales y / o legítimos de otras maneras.
7. Luego de infectar el dispositivo, Los ciberdelincuentes, en la nota de rescate, le proporcionan a la víctima, una URL del sitio web hxxp://avaddonbotrxmuyl.onion/, a la cual deben ingresar para realizar el proceso de descifrado, utilizando el navegador Tor , asimismo se le amenaza a la víctima sino paga el rescate de 500 dólares en Bitcoin en el plazo de 07 horas, se duplicará el precio.
8. Imágenes:

1

Resumen de amenazas:	
Nombre	Virus Avaddon
Tipo de amenaza	Ransomware, Crypto Virus, Armario de archivos
Extensión de archivos cifrados	.avdn
Mensaje exigente de rescate	readme.html (con números aleatorios en su nombre) y el sitio web de Tor
Cantidad de rescate	0.05346968 de Bitcoin
Dirección de BTC Wallet	3JtU8efLk6c176nnntDYCTyBg9biuSdKiE
Nombres de detección	Avast (JS: Downloader-FYY [Trj]), BitDefender (Exploit.HTML.BitsAdmin.Gen), ESET-NOD32 (PowerShell / TrojanDownloader.Agent.DV), Kaspersky (HEUR: Trojan-Downloader.Script.Generic), Completo Lista de detecciones (VirusTotal)
Nombre de proceso deshonesto	237502353.exe (su nombre puede variar)
Síntomas	No se pueden abrir archivos almacenados en su computadora, los archivos previamente funcionales ahora tienen una extensión diferente (por ejemplo, my.docx.locked). Se muestra un mensaje de solicitud de rescate en su escritorio. Los ciberdelincuentes exigen el pago de un rescate (generalmente en bitcoins) para desbloquear sus archivos.
Métodos de distribución	Archivos adjuntos de correo electrónico infectados (macros), sitios web de torrents, anuncios maliciosos.
Dañar	Todos los archivos están encriptados y no se pueden abrir sin pagar un rescate. Se pueden instalar troyanos adicionales que roban contraseñas e infecciones de malware junto con una infección de ransomware.

2

Avaddon ha infectado su red
Todos sus documentos, fotos, bases de datos y otros archivos importantes han sido encriptados y usted no puede desencriptarlos. ¡Pero no se preocupe, podemos ayudarlo a restaurar todos sus archivos!

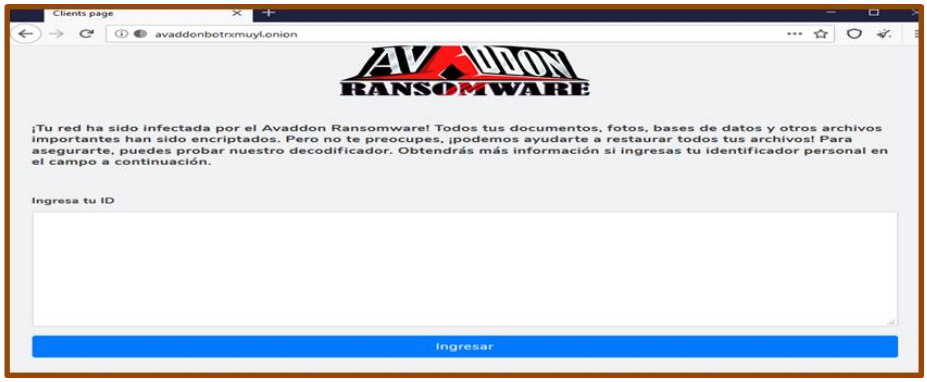
La única forma de restaurar sus archivos es comprar nuestro software especial: Avaddon General Decryptor. ¡Solo nosotros podemos brindarle este software y solo nosotros podemos restaurar sus archivos!

Puede obtener más información en nuestra página, que se encuentra en una red oculta de Tor.

Cómo llegar a nuestra página
Descargar el navegador Tor - hxxps: //www.torproject.org/
Instalar el navegador Tor
Abrir enlace en el navegador Tor - avaddonbotrxmuyl.onion
Siga las instrucciones en esta página
Su ID:
-

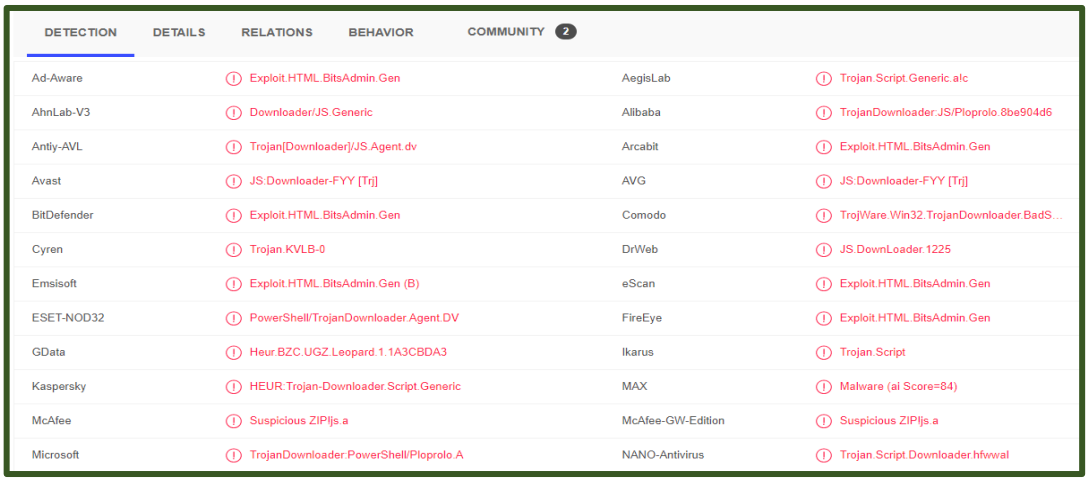
¡NO INTENTE RECUPERAR ARCHIVOS USTED MISMO!
¡NO MODIFIQUE LOS ARCHIVOS ENCRIPTADOS!
¡DE LO CONTRARIO, PUEDE PERDER TODOS SUS ARCHIVOS PARA SIEMPRE!

3



- Sitio web de Avaddon, utilizando el navegador Tor.

- Análisis de Archivo Infectado:
  - Nombre de Archivo: IMG159131.jpg.js.zip
  - Clasificación: Ransomware Avaddon
  - Tipo de Archivo: ZIP
  - Tamaño de Archivo: 546.00 B (546 bytes)
  - MD5: e861a858d56a2f38468dc82d9e6197cd
  - SHA-1: 72e52b870fb670bc7d3294afb51d4d3756251f2e
  - SHA-256: 94faa76502bb4342ed7cc3207b3158027807a01575436e2b683d4816842ed65d
  - Creado: 04JUN20
  - Virustotal:



DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 2

Ad-Aware	Exploit.HTML.BitsAdmin.Gen	AegisLab	Trojan.Script.Generic.alc
AhnLab-V3	Downloader/JS.Generic	Alibaba	TrojanDownloader:JS/Ploprolo.8be904d6
Antiy-AVL	Trojan[Downloader]/JS.Agent.dv	Arcabit	Exploit.HTML.BitsAdmin.Gen
Avast	JS:Downloader-FYY [Trj]	AVG	JS:Downloader-FYY [Trj]
BitDefender	Exploit.HTML.BitsAdmin.Gen	Comodo	TrojWare.Win32.TrojanDownloader.BadS...
Cyren	Trojan.KVLB-0	DrWeb	JS.DownLoader.1225
Emsisoft	Exploit.HTML.BitsAdmin.Gen (B)	eScan	Exploit.HTML.BitsAdmin.Gen
ESET-NOD32	PowerShell/TrojanDownloader.Agent.DV	FireEye	Exploit.HTML.BitsAdmin.Gen
GData	Heur.BZC.UGZ.Leopard.1.1A3CBDA3	Ikarus	Trojan.Script
Kaspersky	HEUR:Trojan-Downloader.Script.Generic	MAX	Malware (ai Score=84)
McAfee	Suspicious ZIP!js.a	McAfee-GW-Edition	Suspicious ZIP!js.a
Microsoft	TrojanDownloader:PowerShell/Ploprolo.A	NANO-Antivirus	Trojan.Script.Downloader.hfwwal

9. Algunas Recomendaciones
   - No aceptes correos electrónicos de remitentes que no conoces.
   - Verifica los remitentes usando google.
   - No abras archivos sospechosos.
   - No ejecutes ningún programa sino conoces su contenido.
   - Siempre ten presente que los ciberdelincuentes, quieren obtener siempre tus datos personales.

Fuentes de información	https[://]www.pcrisk.com/removal-guides/18039-avaddon-ransomware

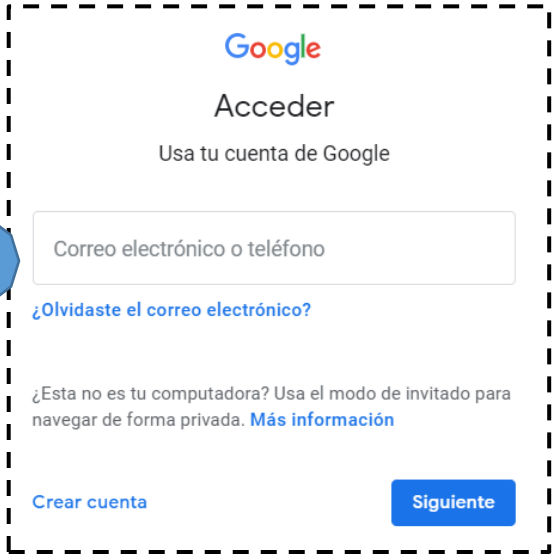
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 066	Fecha: 09-06-2020
		Página: 16 de 21

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantando la identidad de la cuenta google.		
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 subfamilia	G02
Clasificación temática familia	Fraude		

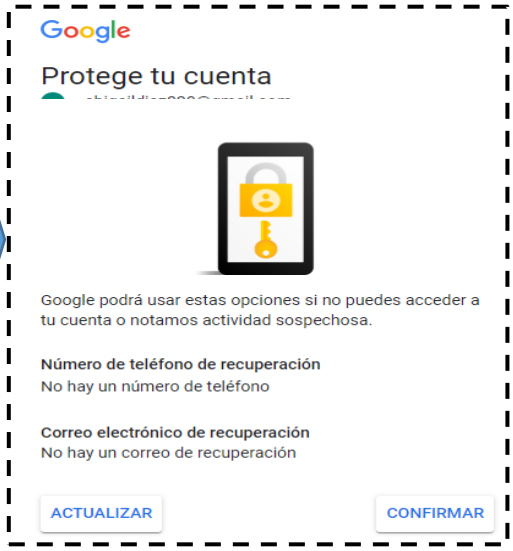
Descripción

10. El 08 de junio de 2020, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de phishing, a través de los diferentes navegadores web, que vienen suplantando la identidad del sitio web "google Gmail" (servicio de correo electrónico gratuito proporcionado por el motor de búsqueda Google), el cual incita al usuario iniciar sesión ingresando los datos del correo electrónico y luego informa que google usará la información cuando no puedas acceder a dicha cuenta, la cual tienen como finalidad obtener información confidencial de manera fraudulenta.

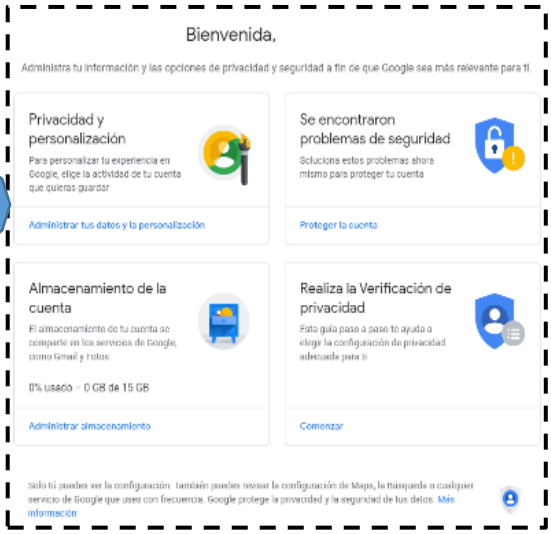
1



2



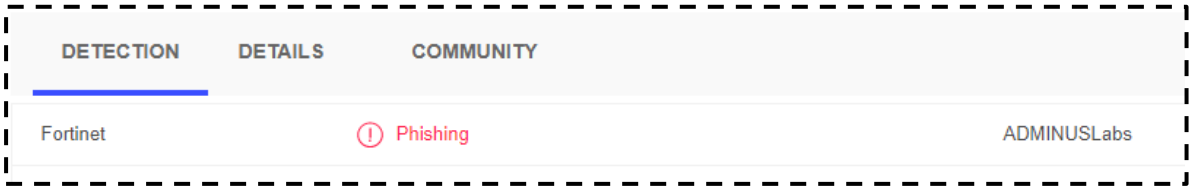
3



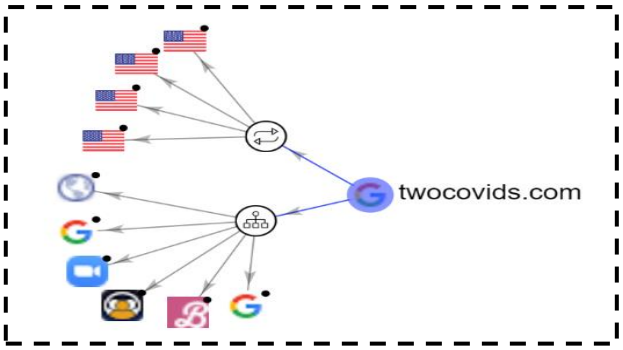
Al continuar con lo solicitado, te da la bienvenida por hacer uso del sitio web y muestra opciones de ajustes de la cuenta Gmail.

11. Las URL Maliciosas, fueron analizadas en las diferentes plataformas virtuales de seguridad digital, obteniendo el siguiente resultado:

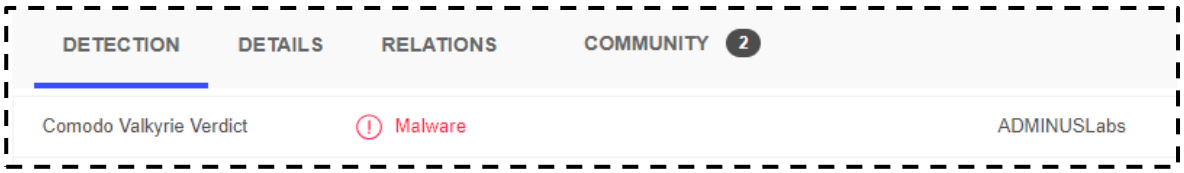
- hxxps://accounts.google.co.- No fue catalogada como Phishing.
- hxxp://twocovids.com .- Catalogada como Phishing.



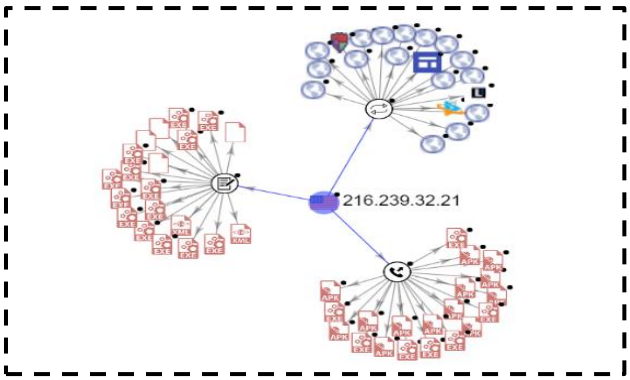
Topología URL:



- IP: 216[.]239[.]32[.]21



Topología IP: 216[.]239[.]32[.]21



12. Algunas Recomendaciones

- Verifica la información en los sitios web oficiales.
- No introduzcas datos personales en páginas sospechosas.
- Siempre ten presente que los ciberdelincuentes, quieren obtener siempre tus datos personales.

Fuentes de información	Análisis propio de redes sociales y fuente abierta

asbanc ASOCIACIÓN DE BANCOS DEL PERÚ	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 066	Fecha: 09-06-2020
		Página: 18 de 21

Componente que reporta	ÁREA DE OPERACIONES DE LA ASOCIACIÓN DE BANCOS DEL PERÚ			
Nombre de la alerta	Smishing – Banco de Crédito del Perú			
Tipo de ataque	Phishing		Abreviatura	Phishing
Medios de propagación	Mensaje de texto.			
Código de familia	G	Código de subfamilia	G02	
Clasificación temática familia	Fraude			

Descripción

1. Comportamiento

   El Área de Operaciones de ASBANC advierte sobre una campaña de smishing que se está difundiendo desde el número de celular +51 988 500 181 conteniendo el enlace *hxxts://bit.ly/BCP_VALIDAR*, redirigiendo a una página web fraudulenta del Banco Crédito del Perú *hxxp://142[.]11[.]229[.]252/iniciar-sesion*

2. Indicadores de compromiso

   - URL de alojamiento: hxxp://142.11.229.252/iniciar-sesion
   - IP: 142[.]11[.]229[.]252
   - Dominio: -
   - Localización: Seattle – Estados Unidos
   - URL de redirección: hxxts://bit.ly/BCP_VALIDAR
   - Número de celular: +51 988 500 181

3. Imágenes

4. Recomendaciones

   - Promover el uso de una solución de seguridad en todos los dispositivos finales (Antivirus, EDR).
   - Bloquear las direcciones URL fraudulentas en sus plataformas de seguridad.
   - Mantener actualizados los sistemas operativos de los equipos utilizados (Servidores, computadoras, smartphones).
   - Realizar concientización constante a los usuarios sobre:
     - Ataques cibernéticos.
     - Esquemas de Ingeniería social.
     - Aprenda a reconocer las características de los portales de su entidad financiera.
   - Considerar la conveniencia, o no, de utilizar enlaces web en los mensajes SMS enviados a sus clientes.

Fuentes de información	Área de Operaciones de ASBANC

asbanc ASOCIACIÓN DE BANCOS DEL PERÚ	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 066**	**Fecha: 09-06-2020**
		Página: 19 de 21

Componente que reporta	**ÁREA DE OPERACIONES DE LA ASOCIACIÓN DE BANCOS DEL PERÚ**			
Nombre de la alerta	Smishing – BBVA Perú			
Tipo de ataque	Phishing		Abreviatura	Phishing
Medios de propagación	Mensaje de texto.			
Código de familia	G	Código de subfamilia	G02	
Clasificación temática familia	Fraude			

Descripción

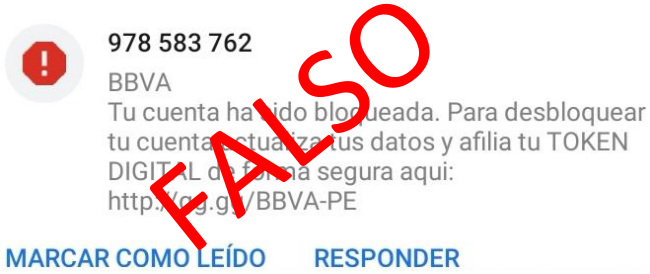
1. Comportamiento

   El Área de Operaciones de ASBANC advierte sobre una campaña de smishing que se está difundiendo desde el número de celular 978 583 762 conteniendo el enlace *hxxt://gg.gg/BBVA-PE*, redirigiendo a una página web fraudulenta del Banco BBVA Perú *hxxps://bancaporinternet.bbva.pe.blusteps.com/bdntux_pe_web/bdntux_pe_web*

2. Indicadores de compromiso

   - URL de alojamiento: hxxps://bancaporinternet.bbva.pe.blusteps.com/bdntux_pe_web/bdntux_pe_web
   - IP: 192[.]185[.]48[.]161
   - Dominio: bancaporinternet.bbva.pe.blusteps.com
   - Localización: Houston – Estados Unidos
   - URL de redirección: hxxts://gg.gg/BBVA-PE
   - Número de celular: 978 583 762

3. Imágenes



4. Recomendaciones

   - Promover el uso de una solución de seguridad en todos los dispositivos finales (Antivirus, EDR).
   - Bloquear las direcciones URL fraudulentas en sus plataformas de seguridad.
   - Mantener actualizados los sistemas operativos de los equipos utilizados (Servidores, computadoras, smartphones).
   - Realizar concientización constante a los usuarios sobre:
     - Ataques cibernéticos.
     - Esquemas de Ingeniería social.
     - Aprenda a reconocer las características de los portales de su entidad financiera.
   - Considerar la conveniencia, o no, de utilizar enlaces web en los mensajes SMS enviados a sus clientes.

Fuentes de información	Área de Operaciones de ASBANC

asbanc ASOCIACIÓN DE BANCOS DEL PERÚ	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 066	Fecha: 09-06-2020
		Página: 20 de 21

Componente que reporta	**ÁREA DE OPERACIONES DE LA ASOCIACIÓN DE BANCOS DEL PERÚ**			
Nombre de la alerta	Página web falsa del Banco de Crédito del Perú			
Tipo de ataque	Phishing		Abreviatura	Phishing
Medios de propagación	Redes sociales y correo electrónico.			
Código de familia	G	Código de subfamilia	G02	
Clasificación temática familia	Fraude			

Descripción

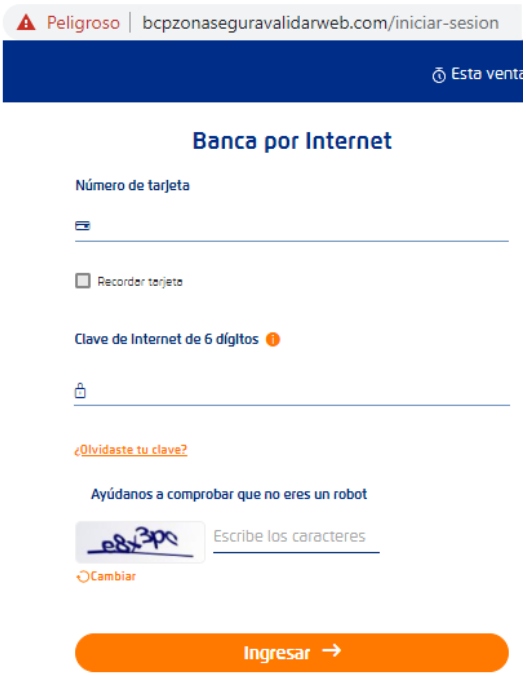
1. Comportamiento

   El Área de Operaciones de ASBANC advierte sobre una campaña de phishing que se está difundiendo desde redes sociales y correo electrónico.

2. Indicadores de compromiso

   - URL de alojamiento: hxxps://bcpzonaseguravalidarweb.com/iniciar-sesion
   - IP: 142[.]11[.]211[.]20
   - Dominio: bcpzonaseguravalidarweb.com
   - Localización: Seattle – Estados Unidos

3. Imágenes



4. Recomendaciones

   - Promover el uso de una solución de seguridad en todos los dispositivos finales (Antivirus, EDR).
   - Bloquear las direcciones URL fraudulentas en sus plataformas de seguridad.
   - Mantener actualizados los sistemas operativos de los equipos utilizados (Servidores, computadoras, smartphones).
   - Realizar concientización constante a los usuarios sobre:
     - Ataques cibernéticos.
     - Esquemas de Ingeniería social.
     - Aprenda a reconocer las características de los portales de su entidad financiera.

Fuentes de información	Área de Operaciones de ASBANC

Índice alfabético