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

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 18 de junio de 2022

N° 163-2022-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 Aérea del 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 las empresas 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

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 163	Fecha: 18-06-2022
		Página 4 de 12

Componente que reporta	**EL CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Cierran la botnet rusa RSOCKS que hackeó millones de dispositivos		
Tipo de ataque	Botnets	Abreviatura	Botnets
Medios de propagación	IRC, USB, Disco, Red, Correo, navegación por Internet		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código Malicioso		

Descripción

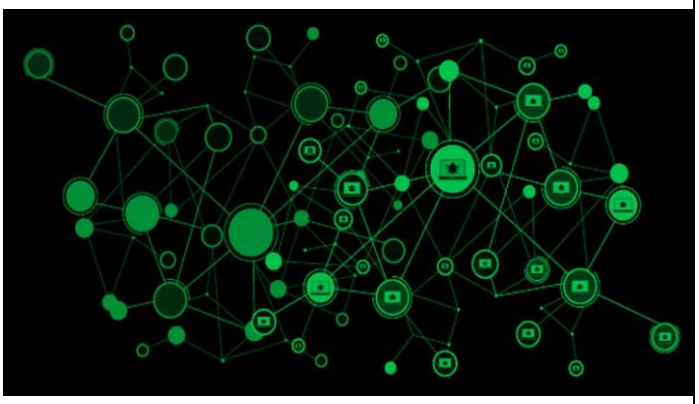
1. **Fecha del evento:**

- A través del monitoreo y búsqueda de amenazas en el ciberespacio el 17 de junio del 2022 se tomó conocimiento de la publicación realizada en https://thehackernews.com/ sobre botnet rusa conocida como RSOCKS en colaboración con socios encargados de hacer cumplir la ley en Alemania, los Países Bajos y el Reino Unido.

2. **Antecedentes:**

- Se cree que la red de bots, operada por una organización sofisticada de delitos cibernéticos, atrapó a millones de dispositivos conectados a Internet, incluidos dispositivos de Internet de las cosas (IoT), teléfonos Android y computadoras para usar como un servicio de proxy.

3. **Detalles:**



- Los botnets, una amenaza en constante evolución, son redes de dispositivos informáticos secuestrados que están bajo el control de una sola parte atacante y se utilizan para facilitar una variedad de intrusiones cibernéticas a gran escala, como ataques de denegación de servicio distribuido (DDoS), correo electrónico spam y criptojacking.
- "La botnet RSOCKS ofreció a sus clientes acceso a direcciones IP asignadas a dispositivos que habían sido pirateados", dijo el Departamento de Justicia en un comunicado de prensa. "Los propietarios de estos dispositivos no otorgaron a los operadores de RSOCKS la autoridad para acceder a sus dispositivos con el fin de utilizar sus direcciones IP y enrutar el tráfico de Internet"
- Además de las empresas domésticas y los individuos, varias entidades públicas y privadas grandes, incluida una universidad, un hotel, un estudio de televisión y un fabricante de productos electrónicos, han sido víctimas de la botnet hasta la fecha, dijeron los fiscales.
- Los clientes que deseen aprovechar los proxy de RSOCKS pueden alquilar el acceso a través de una tienda basada en la web durante diferentes períodos de tiempo a varios puntos de precio que van desde $ 30 por día para acceder a 2000 proxy y hasta $ 200 por día para acceder a 90 000 proxy.
- Una vez comprados, los delincuentes podrían redirigir el tráfico de Internet malicioso a través de las direcciones IP asociadas con los dispositivos de las víctimas comprometidas para ocultar su verdadera intención, que era llevar a cabo ataques de relleno de credenciales, acceder a cuentas de redes sociales comprometidas y enviar mensajes de phishing. La acción es la culminación de una operación encubierta montada por la Oficina Federal de Investigaciones (FBI) a principios de 2017, cuando realizó compras encubiertas a RSOCKS para mapear su infraestructura y sus víctimas, lo que le permitió determinar aproximadamente 325,000 dispositivos infectados.
- "A través del análisis de los dispositivos de las víctimas, los investigadores determinaron que la botnet RSOCKS comprometió el dispositivo de la víctima al realizar ataques de fuerza bruta", dijo el Departamento de Justicia. "Los servidores back-end de RSOCKS mantuvieron una conexión persistente con el dispositivo comprometido".
- La interrupción de RSOCKS llega menos de dos semanas después de que se apoderara de un mercado en línea ilícito conocido como SSNDOB para traficar información personal como nombres, fechas de nacimiento,

números de tarjetas de crédito y números de Seguro Social de aproximadamente 24 millones de personas en los EE. UU.

4. Recomendaciones:

- Habilitar el cortafuegos:

  Dentro de todas las herramientas de seguridad que tenemos a nuestra disposición, el firewall o cortafuegos es una de las más importantes para prevenir ataques en red. Si queremos protegernos de ataques de botnet, una de las primeras medidas que debemos tomar es la de habilitar el cortafuegos.

  Hoy en día la mayoría de los usuarios de equipos de escritorio utilizan Windows 10 como sistema operativo. Esto significa que de manera gratuita cuentan con el firewall de Windows. Es una buena opción, aunque existen más. Eso sí, es clave que ese cortafuegos esté configurado correctamente.

- Limitar el compartir red con otros equipos:

  Es cierto que vivimos en una época en la que puede ser importante que todos nuestros dispositivos estén unidos en la misma red. Es una manera de poder compartir archivos o funciones rápidamente. Ahora bien, esto también puede ser un problema para nuestra seguridad.

  Nuestro consejo para protegernos de ataques botnet es que limitemos el hecho de que los dispositivos estén compartidos en la red. Esto hay que aplicarlo lógicamente cuando este tipo de servicios no vamos a necesitarlo.

- Utilizar el filtrado de datos:

  El malware de botnet generalmente funciona estableciendo interacciones con al menos un servidor de comando y control remoto, que los piratas informáticos también usan para extraer información confidencial. Para bloquear las interacciones maliciosas y evitar así ataques, podemos utilizar el filtrado de datos en la información que sale de la red.

- Asegurar con capas extras nuestra red:

  Algo que no puede faltar es asegurar por completo nuestra red. Pero si queremos realmente aumentar la seguridad frente a ataques botnet, es importante que pongamos en práctica funciones adicionales. Esto hay que aplicarlo especialmente si queremos proteger una empresa de ataques de este tipo.

- Mejorar el monitoreo de red:

  Tener un control sobre el uso de la red, los dispositivos que están conectados, es algo también muy importante. El monitoreo las 24 horas de la actividad de la red debería ser algo a tener en cuenta. Para ello podemos hacer uso de herramientas de recolección de datos que detecten comportamientos anómalos y bloqueen los intentos de infiltrarse en el sistema

- Tener actualizado correctamente el sistema:

  Otro punto vital es el tema de las actualizaciones y parches de seguridad. Muchos tipos de amenazas llegan a través de vulnerabilidades existentes. Es muy importante que tengamos instaladas las últimas versiones. De esta forma podremos evitar que posibles piratas informáticos se aprovechen de esos fallos de seguridad para llevar a cabo sus ataques

- Utiliza contraseñas fuertes y complejas:

  En muchas ocasiones los ataques de botnet llegan a través de dispositivos que utilizan contraseñas genéricas. Esto es un problema muy importante y hay que evitar. Nuestro consejo es cambiar siempre las claves que vienen de fábrica, tanto del router como de cualquier otro equipo.

  Una buena contraseña es aquella que es totalmente aleatoria y única. Tiene que contar con letras (mayúsculas y minúsculas), números y otros símbolos especiales.

- Cuidado con las descargas:

  A la hora de descargar de Internet es una de las puertas de entrada para malware. Hay que tener cuidado en este sentido y descargar únicamente software legítimo y desde sitios oficiales. Especialmente hay que tener cuidado con las descargas P2P, ya que es uno de los medios para llevar a cabo este tipo de ataques.

Fuentes de información	▪ https://thehackernews.com/2022/06/authorities-shut-down-russian-rsocks.html ▪ https://www.redeszone.net/tutoriales/seguridad/evitar-ataques-botnet-dispositivos/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 163	Fecha: 18-06-2022
		Página 6 de 12

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Los piratas informáticos chinos aprovecharon la falla de día cero de Sophos Firewall para apuntar a una entidad		
Tipo de ataque	Botnets	Abreviatura	Botnets
Medios de propagación	IRC, USB, Disco, Red, Correo, navegación por Internet		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código Malicioso		

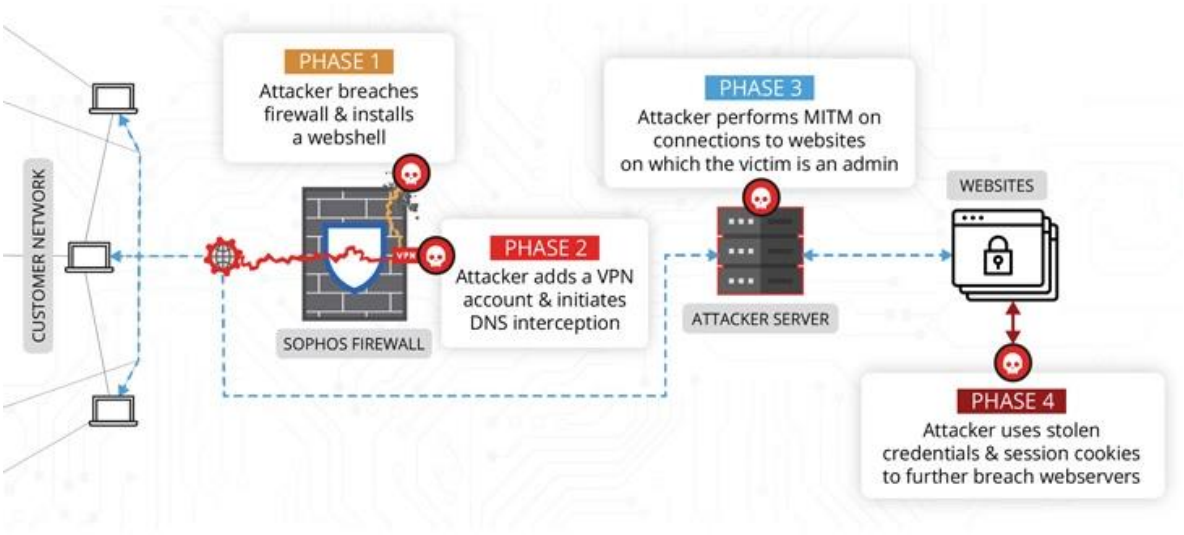
Descripción

FECHA DEL EVENTO:

A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 10 de junio del 2022, se tomó conocimiento a través de la publicación realizada en la página web de **"thehackernews.com"**, sobre piratas informáticos chinos aprovecharon la falla de día cero de Sophos Firewall para apuntar a una entidad.

ANTECEDENTES:

- Un sofisticado actor chino de amenazas persistentes avanzadas (APT) explotó una vulnerabilidad de seguridad crítica en el producto de firewall de Sophos que salió a la luz a principios de este año para infiltrarse en un objetivo no identificado del sur de Asia como parte de un ataque altamente dirigido.



DETALLES:

- El atacante implementó una puerta trasera de shell web interesante, creó [d] una forma secundaria de persistencia y, en última instancia, lanzó ataques contra el personal del cliente", dijo Volexity en un informe. "Estos ataques tenían como objetivo violar aún más los servidores web alojados en la nube que alojan los sitios web públicos de la organización".
- La falla de día cero en cuestión se rastrea como CVE-2022-1040 (puntuación CVSS: 9.8) y se refiere a una vulnerabilidad de omisión de autenticación que puede armarse para ejecutar código arbitrario de forma remota. Afecta a las versiones de Sophos Firewall 18.5 MR3 (18.5.3) y anteriores.
- La empresa de ciberseguridad, que emitió un parche para la falla el 25 de marzo de 2022, señaló que se abusó de ella para "apuntar a un pequeño conjunto de organizaciones específicas principalmente en la región del sur de Asia" y que había notificado directamente a las entidades afectadas.
- Ahora, según Volexity, las primeras pruebas de explotación de la falla comenzaron el 5 de marzo de 2022, cuando detectó una actividad de red anómala que se originaba en el Sophos Firewall de un cliente anónimo que ejecutaba la versión actualizada, casi tres semanas antes de la divulgación pública de la falla. vulnerabilidad.

- "El atacante estaba usando el acceso al firewall para realizar ataques de intermediario (MitM)", dijeron los investigadores. "El atacante usó los datos recopilados de estos ataques MitM para comprometer sistemas adicionales fuera de la red donde residía el firewall".
- La secuencia de infección posterior a la violación del firewall implicó además la puerta trasera de un componente legítimo del software de seguridad con el shell web Behinder al que se podía acceder de forma remota desde cualquier URL que el actor de la amenaza eligiera.

- Es de destacar que el shell web Behinder también fue aprovechado a principios de este mes por grupos APT chinos en un conjunto separado de intrusiones que explotan una falla de día cero en los sistemas Atlassian Confluence Server (CVE-2022-26134).
- Además, se dice que el atacante creó cuentas de usuario de VPN para facilitar el acceso remoto, antes de pasar a modificar las respuestas de DNS para sitios web especialmente dirigidos, principalmente el sistema de gestión de contenido (CMS) de la víctima, con el objetivo de interceptar las credenciales de usuario y las cookies de sesión.

- Posteriormente, el acceso a las cookies de sesión equipó a la parte malintencionada para tomar el control del sitio de WordPress e instalar un segundo shell web denominado IceScorpion, y el atacante lo usó para implementar tres implantes de código abierto en el servidor web, incluidos PupyRAT, Pantegana y Sliver.
- "DriftingCloud es un actor de amenazas efectivo, bien equipado y persistente que apunta a objetivos relacionados con cinco venenos. Pueden desarrollar o comprar exploits de día cero para lograr sus objetivos, inclinando la balanza a su favor cuando se trata de obtener acceso a redes objetivo".

RECOMENDACIONES

- Para evitar este tipo de ataques, Akamai sugiere que los objetivos potenciales utilicen contraseñas complejas, agreguen MFA en todas las cuentas, limiten el acceso SSH y supervisen constantemente la actividad de los recursos de las máquinas virtuales.
- Mantén actualizado tu antivirus y asegúrate de contar con protección anti-malware.

Fuentes de información	▪ https://thehackernews.com/2022/06/chinese-hackers-exploited-sophos.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 163	Fecha: 18-06-2022
		Página 8 de 12

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Botnet Panchan Golang P2P dirigida a servidores Linux en campaña de criptominería		
Tipo de ataque	Botnets	Abreviatura	Botnets
Medios de propagación	IRC, USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código Malicioso		

Descripción

FECHA DEL EVENTO:

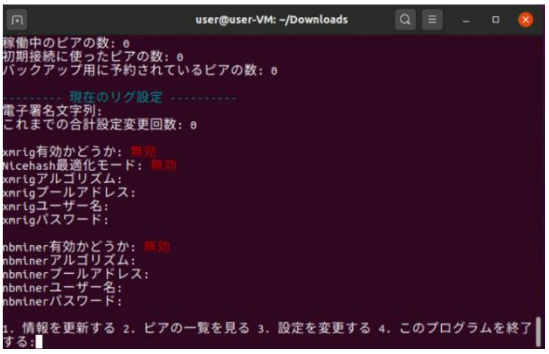
A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 10 de junio del 2022, se tomó conocimiento a través de la publicación realizada en la página web de **"SECURITY AFFAIRS"**, sobre una nueva botnet peer-to-peer llamada Panchan apareció en la naturaleza alrededor de marzo de 2022, apuntando a servidores Linux en el sector educativo para extraer criptomonedas.

ANTECEDENTES:

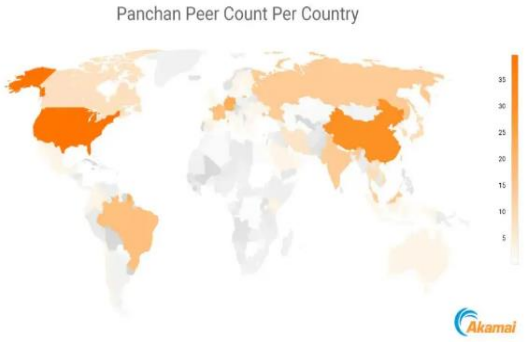
- Panchan está equipado con funciones de gusano SSH como ataques de diccionario y abuso de claves SSH para realizar un movimiento lateral rápido a las máquinas disponibles en la red comprometida.
- Al mismo tiempo, tiene potentes capacidades de prevención de detección, como el uso de mineros mapeados en memoria y la detección dinámica de monitoreo de procesos para detener el módulo de minería de inmediato.

DETALLES:

- La botnet se dedica a la actividad de criptominería, el código malicioso ha sido diseñado para secuestrar los recursos de la computadora para extraer criptomonedas. El bot se observó utilizando mineros XMRig y nbhash que no se extraen al disco para evitar la detección.



- El malware despliega dos mineros: xmrig y nbhash. Ambos binarios mineros vienen codificados en base64 dentro del propio binario de malware y se extraen y ejecutan durante el tiempo de ejecución. Sin embargo, hay alguna novedad en la ejecución, ya que los mineros no se extraen en el disco en absoluto.
- Para evitar la detección y reducir la trazabilidad, el malware deja caer sus criptomineros como archivos mapeados en memoria, sin ninguna presencia de disco. También mata los procesos de los criptomineros si detecta cualquier monitoreo de procesos.



- Los investigadores observaron que el malware implementaba un "godmode", un panel de administración que los operadores usan para editar la configuración de minería, que luego se distribuye a todos los nodos de la botnet. Se observaron actores de amenazas utilizando una clave privada para acceder a godmode con el fin de evitar la manipulación no deseada.
- El bot contiene una clave pública asociada con la clave privada anterior y se utiliza para autenticar conexiones. El panel de administración está escrito en japonés, una circunstancia que sugiere que los actores de la amenaza probablemente sean de origen japonés.

- Los expertos realizaron ingeniería inversa del bot, también pudieron desarrollar un script para mapear la botnet y extraer la lista completa de máquinas infectadas. En el momento del análisis, los investigadores descubrieron 209 pares, 40 de los cuales están actualmente activos.
- La mayoría de las infecciones se producen en Asia (64), seguida de Europa (52), América del Norte (45), América del Sur (11), África (1) y Oceanía (1).
- Para lograr la persistencia, el malware se copia a sí mismo en /bin/systemd-worker y crea un servicio systemd con el mismo nombre. Los expertos señalaron que es probable que los operadores imiten los servicios sistematizados legítimos para evitar detecciones.

RECOMENDACIONES

- Para evitar este tipo de ataques, Akamai sugiere que los objetivos potenciales utilicen contraseñas complejas, agreguen MFA en todas las cuentas, limiten el acceso SSH y supervisen constantemente la actividad de los recursos de las máquinas virtuales.
- Mantén actualizado tu antivirus y asegúrate de contar con protección anti-malware.

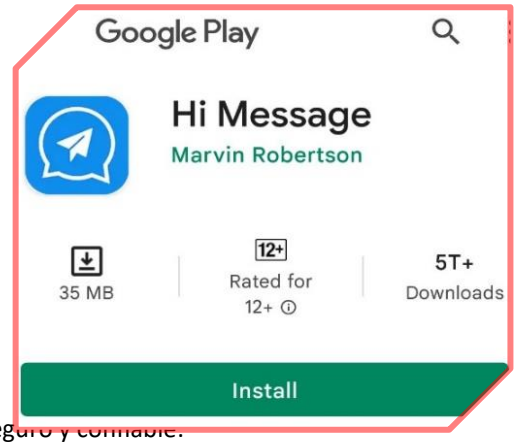
Fuentes de información	▪ https://securityaffairs.co/wordpress/132290/cyber-crime/panchan-p2p-botnet.html

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 163	Fecha: 18-06-2022
		Página 10 de 12

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de malware en la aplicación "Hi Message" de Android.		
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. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo avanzados ataques de malware que se propaga por medio de la plataforma de "Google Play", bajo la apariencia de una aplicación inofensiva de android denominada "Hi Message", que oculta el virus conocido como "Joker", que al ejecutarse provoca una automatización de suscripciones y códigos para servicios Premium, sin consentimiento de usuario.



- Detalles del aplicativo:
  - Versión: 4.01
  - Tamaño del archivo: 42,02 MB
  - Requiere: Android 4.4+
  - Nombre del paquete: com.young.messaging.hiya
  - Desarrollador: Marvin Robertson
  - Actualizado: 24 de febrero de 2022
  - Precio: Gratis

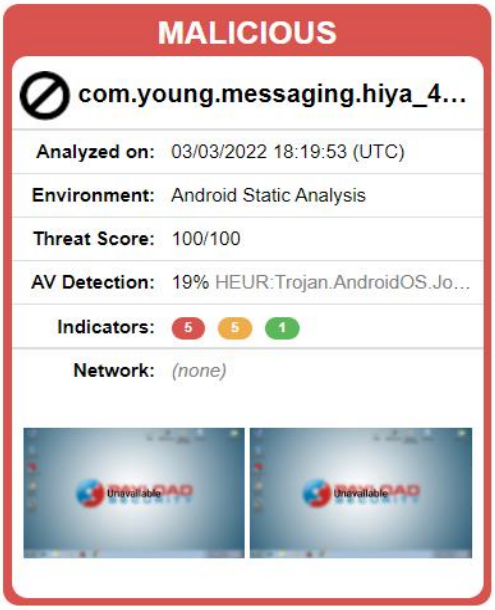
- Funciones gratuitas que ofrece el aplicativo:
  - Mensajes de texto, imágenes, voz, etc. Gratuitos.
  - Proteger la privacidad de los usuarios, absolutamente seguro y confiable.
  - Puede personalizar el interfaz y temas.
  - Puede enviar mensajes regularmente.
  - Búsqueda de palabras clave para mensajes de texto importantes.

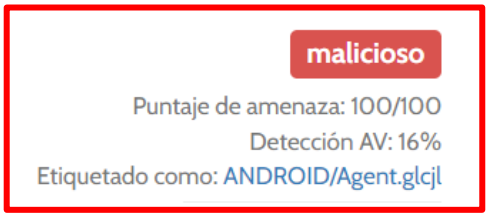
2. Se realizó el análisis del aplicativo en cuestión, en las diferentes plataformas virtuales de seguridad digital a fin de determinar el grado de confianza y la detección de algún malware que pudiera poner en riesgo a los dispositivos Android, obteniendo como resultado:

- Análisis del archivo (. *apk): com.young.messaging.hiya
  - MD5: 8b2e3075025385355956350b4c5ec8f5
  - SHA-256: 837e5a044ffb2721ab07430380c4089e3a6995c9f0663c5192ae76d3a92e4ac0
  - Tipo de archivo: Android
  - Tamaño del archivo: 42,02 MB (44063750 bytes)
  - Nombre de paquete: com.young.messaging.hiya

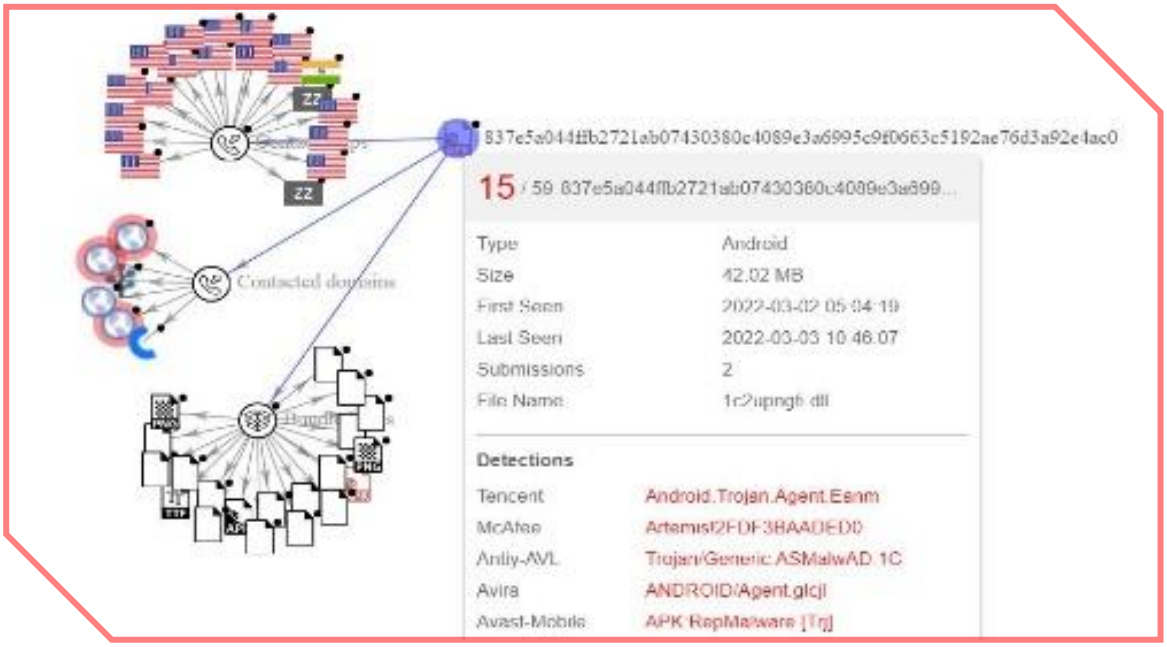
Observación: Se detecta que el archivo APK contiene Malware uno de ellos conocido como "Joker" que está diseñado para robar mensajes SMS, lista de contactos e información del dispositivo, además de suscribir de manera oculta a usuarios en servicios de pago.

- Otros resultados del análisis:





3. Topología de red:



4. Recomendaciones:

- Verificar la información de la app visitando el sitio web de los desarrolladores.
- Analizar los permisos que otorgas para la aplicación.
- No abrir archivos sospechosos.
- Actualizar el sistema de tu dispositivo constantemente.
- No compartir la información con terceras personas, amigos o familiares y otros.
- Mantener instalado un servicio de antivirus en el dispositivo.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta

Índice alfabético