

Friday Overtime Cazando Amenazas en el Último Turno

- *Andres Valdivieso Pinilla - Líder de Ciberseguridad (Consultor)*
- *www.linkedin.com/in/andres-valdivieso-pinilla*

*Análisis de Amenaza: Evaluación de Posible Malware en SwiftSpend Finance**

Introducción

En nuestro rubro nunca se duerme, y los que hemos estado en un puesto de analista de inteligencia de amenazas lo sabemos mejor que nadie. Mientras la mayoría se prepara para disfrutar del fin de semana, nosotros estamos atentos a las alertas que no cesan. Para este desafío nos ponen a interactuar como analista donde nos plantean que en **PandaProbe Intelligence**, se recibe una notificación de la plataforma CTI que interrumpe la tranquilidad del viernes por la tarde.

La alerta proviene de **SwiftSpend Finance**, una institución financiera reconocida por su estricta postura en seguridad, que ha detectado actividad sospechosa en sus sistemas. *Ante la posibilidad de una amenaza real, la empresa ha abierto un ticket de emergencia*, solicitando un análisis inmediato de los archivos adjuntos, presuntamente muestras de malware.

Como el único analista de CTI disponible, la responsabilidad recae sobre nuestros hombros. **La misión es clara: evaluar la naturaleza de estos archivos, determinar su alcance y proporcionar una respuesta que permita contener cualquier posible amenaza.** Para ello, se llevará a cabo un análisis estructurado en múltiples fases, desde el escaneo preliminar hasta la correlación de datos con fuentes de inteligencia sobre amenazas.

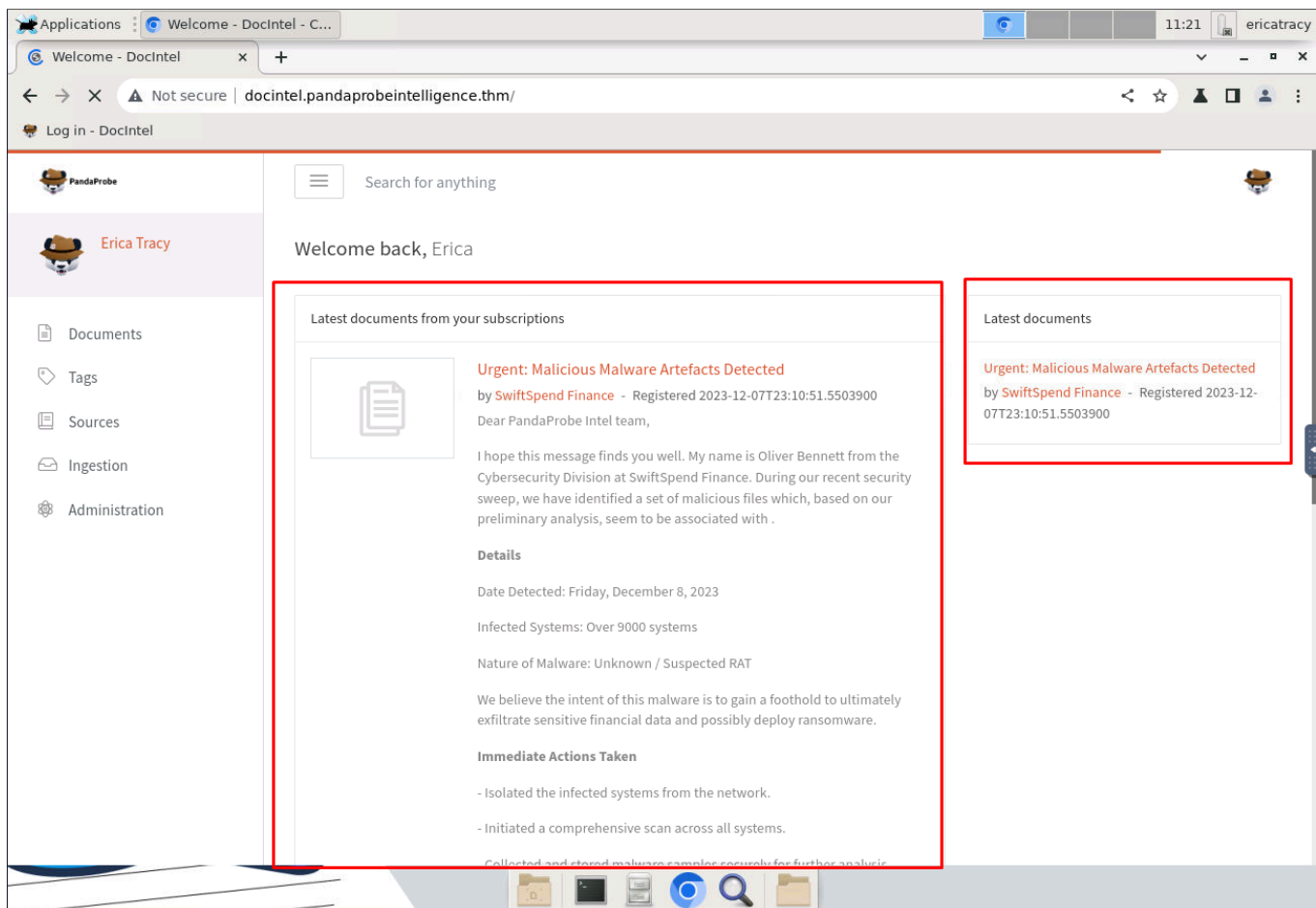
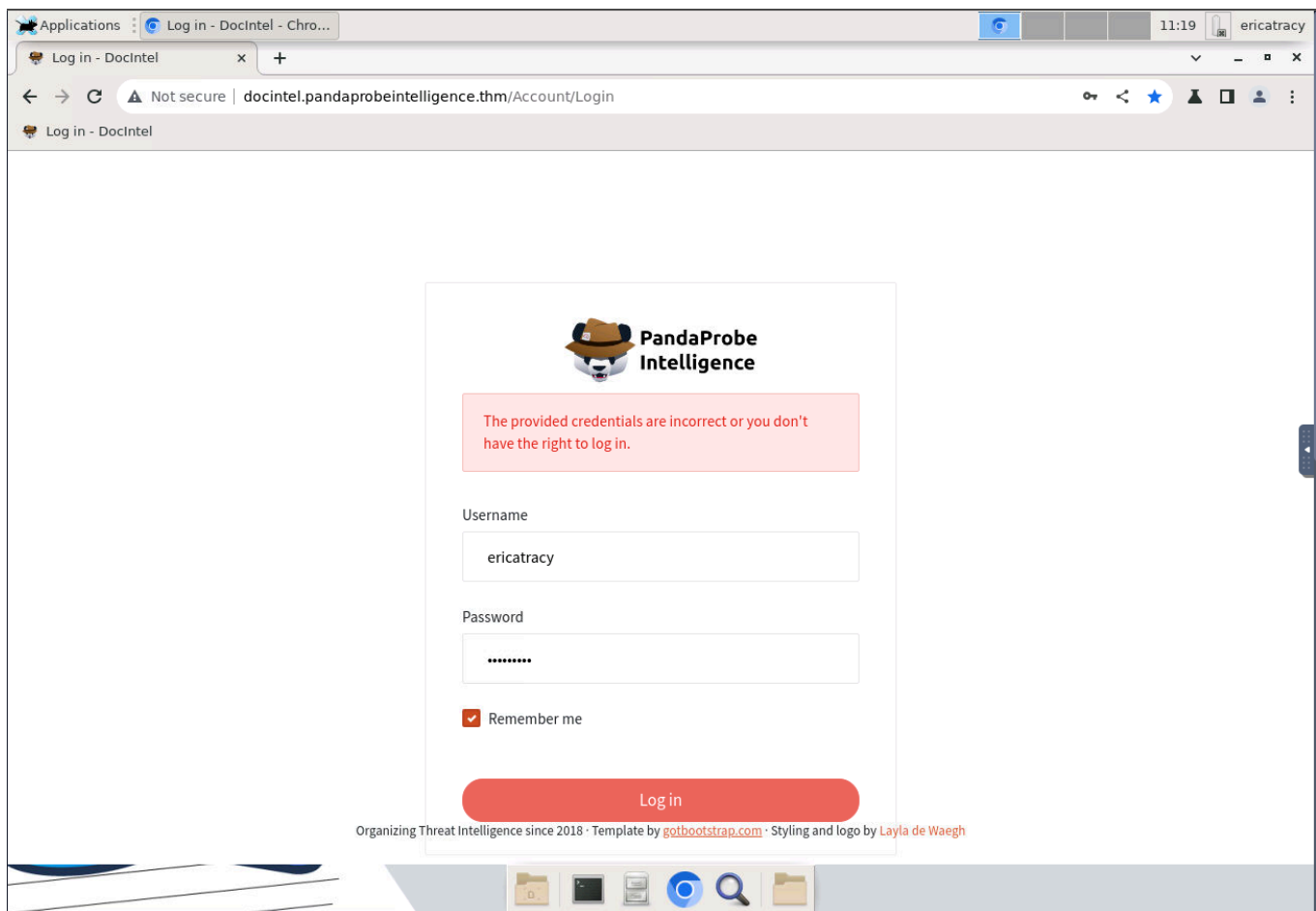
Este write-up documentará cada paso del análisis, incluyendo herramientas utilizadas, técnicas aplicadas y hallazgos clave. *El objetivo es ofrecer una visión técnica detallada sobre el posible malware involucrado y proporcionar recomendaciones efectivas para su mitigación y remediación.*

Con una respiración profunda, una mente concentrada y el anhelo de volver a casa, comenzamos el proceso de:

1. Descargar las muestras de malware proporcionadas en el ticket, *asegurándose de que estaban contenidas en un entorno seguro*.
2. *Ejecutar las muestras* a través de herramientas preliminares de análisis automatizado de malware *para obtener una descripción general rápida*.
3. *Profundizar en un análisis manual*, comprender el comportamiento del malware e identificar sus patrones de comunicación.
4. *Correlacionar hallazgos* con bases de datos de inteligencia sobre amenazas globales *para identificar firmas o comportamientos conocidos*.
5. *Elaborar un informe completo con medidas de mitigación y recuperación*, garantizando que SwiftSpend Finance pueda abordar rápidamente las posibles amenazas.

Desarrollo

Lo primero es ingresar a la plataforma para ver el correo con la información inicial del caso:



Al ingresar podemos ver que:

- la Fecha de la detección es el: viernes 8 de diciembre de 2023.
- los Sistemas infectados son: más de 9000 sistemas.
- Que la naturaleza del malware la catalogan como: desconocido y/o sospecha de RAT.

Las Acciones que fueron tomadas:

- Aislar los sistemas infectados de la red.
- inició un escaneo integral en todos los sistemas.
- *Muestras de malware recolectadas y almacenadas de forma segura para un análisis posterior.*
- Actualmente estamos colaborando con agencias de ciberseguridad externas y nuestros proveedores de soluciones de seguridad para obtener una comprensión más profunda de este malware. *Sin embargo, queríamos plantear esto con usted inmediatamente dado el riesgo potencial asociado con los APT.*

En el futuro, vamos a llevar a cabo una capacitación de concientización sobre el usuario para informar a todos los miembros del personal que sean más cautelosos, especialmente cuando se trata de archivos adjuntos y enlaces por correo electrónico.

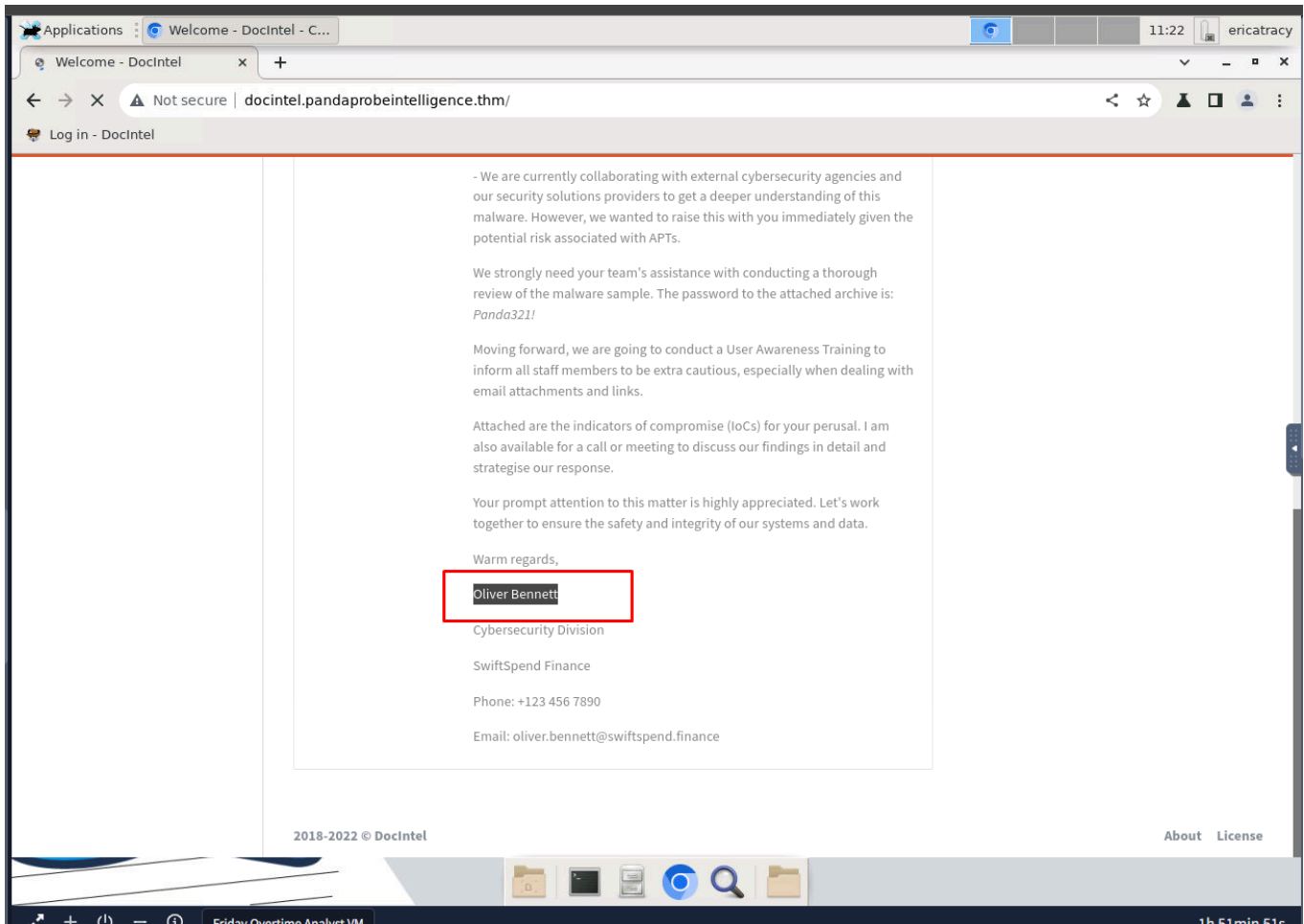
Se adjuntan los indicadores de compromiso (IOC) para su lectura. También estoy disponible para una llamada o reunión para discutir nuestros hallazgos en detalle y estrategia nuestra respuesta.

Con esto ya podemos arrancar a solucionar las diferentes preguntas planteadas se indica que creen que la intención de este malware es obtener un punto de apoyo para finalmente exfiltrar datos financieros confilados y posiblemente implementar ransomware.

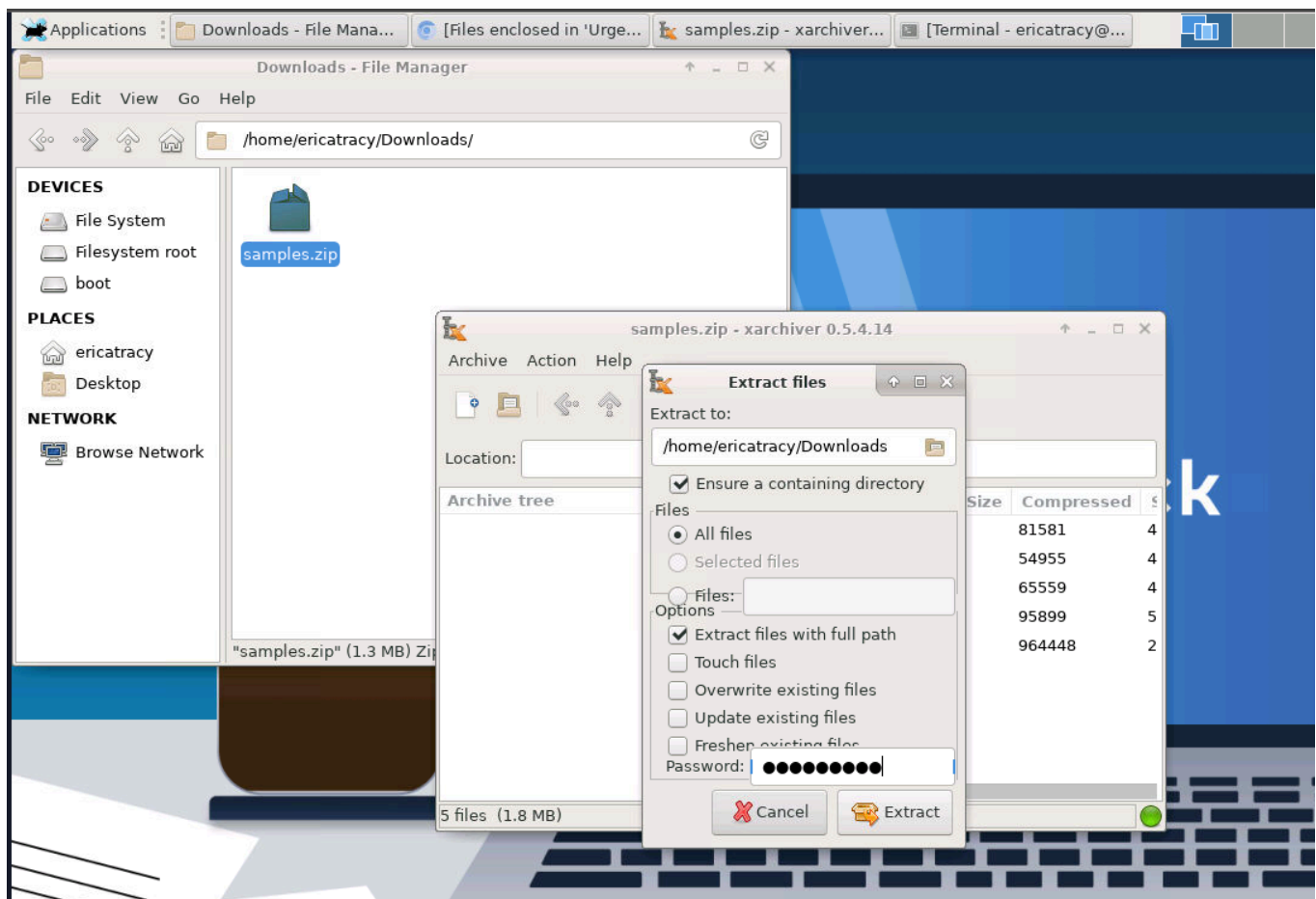
Preguntas

¿Quién compartió las muestras de malware?

Esta información esta a simple vista en el cuerpo del correo:

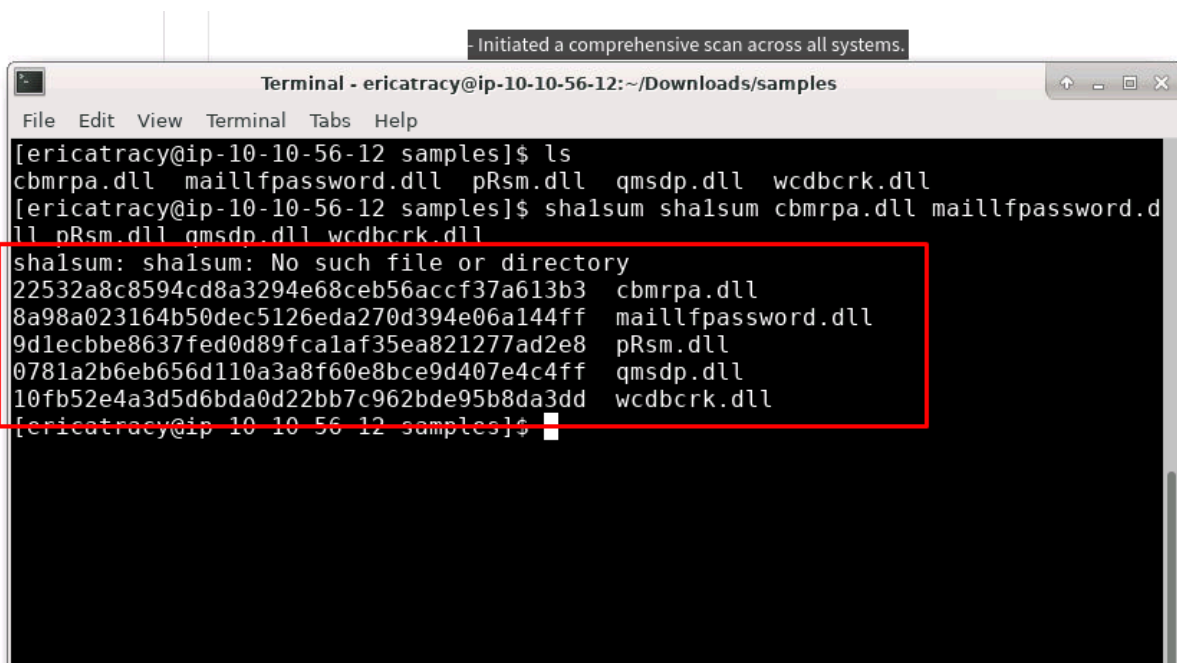


Posteriormente validamos los artefactos suministrados a lo que debemos descargarlos para poder sacar los hash de los diferentes archivos primero procedemos a descargar la muestra y posteriormente debemos extraer los archivos sin manipularlos con la clave proporcionada:

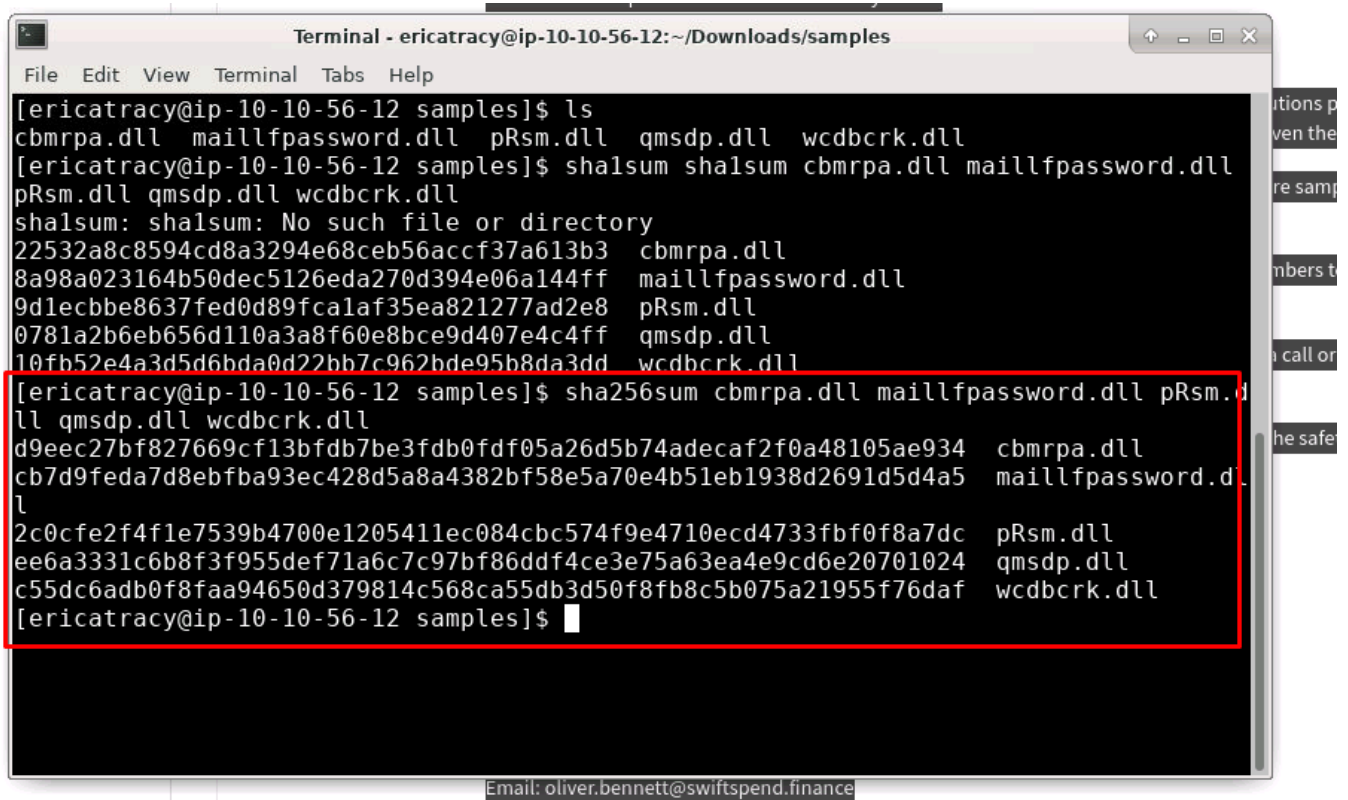


Cuando ya los tenemos todos lo que debemos a hacer es usar el comando:

```
shasum cbmrpa.dll maillfpassword.dll pRsm.dll qmsdp.dll
wcdbrck.dll
```



Con esto ya obtenemos todos los sha1 de las muestra aplica para sha256 también:



```
Terminal - ericatracy@ip-10-10-56-12: ~/Downloads/samples
File Edit View Terminal Tabs Help
[ericatracy@ip-10-10-56-12 samples]$ ls
cbmrpa.dll maillfpassword.dll pRsm.dll qmsdp.dll wdbcrk.dll
[ericatracy@ip-10-10-56-12 samples]$ sha1sum sha1sum cbmrpa.dll maillfpassword.dll
pRsm.dll qmsdp.dll wdbcrk.dll
sha1sum: sha1sum: No such file or directory
22532a8c8594cd8a3294e68ceb56accf37a613b3 cbmrpa.dll
8a98a023164b50dec5126eda270d394e06a144ff maillfpassword.dll
9d1ecbbe8637fed0d89fca1af35ea821277ad2e8 pRsm.dll
0781a2b6eb656d110a3a8f60e8bce9d407e4c4ff qmsdp.dll
10fb52e4a3d5d6bda0d22bb7c962bde95b8da3dd wdbcrk.dll
[ericatracy@ip-10-10-56-12 samples]$ sha256sum cbmrpa.dll maillfpassword.dll pRsm.d
ll qmsdp.dll wdbcrk.dll
d9eec27bf827669cf13bfdb7be3fdb0fdf05a26d5b74adecaf2f0a48105ae934 cbmrpa.dll
cb7d9feda7d8ebfba93ec428d5a8a4382bf58e5a70e4b51eb1938d2691d5d4a5 maillfpassword.d
ll
2c0cfe2f4f1e7539b4700e1205411ec084cbc574f9e4710ecd4733fbf0f8a7dc pRsm.dll
ee6a3331c6b8f3f955def71a6c7c97bf86ddf4ce3e75a63ea4e9cd6e20701024 qmsdp.dll
c55dc6adb0f8faa94650d379814c568ca55db3d50f8fb8c5b075a21955f76daf wdbcrk.dll
[ericatracy@ip-10-10-56-12 samples]$
```

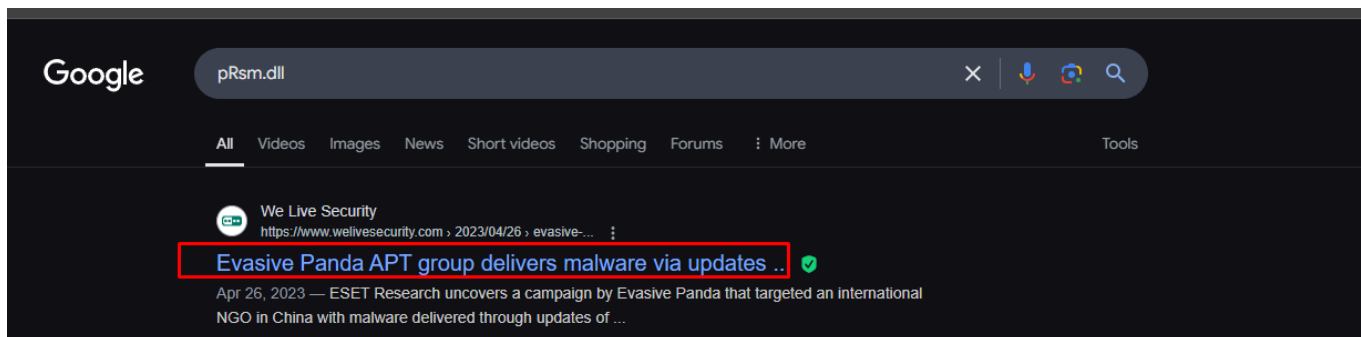
Email: oliver.bennett@swiftspend.finance

Ahora la consulta solicitada es ¿Cuál es el hash SHA1 del archivo "pRsm.dll" dentro de samples.zip?

```
sha1sum pRsm.dll
```

```
Terminal - ericatracy@ip-10-10-56-12:~/Downloads/samples
File Edit View Terminal Tabs Help
[ericatracy@ip-10-10-56-12 ~]$ cd Samples
bash: cd: Samples: No such file or directory
[ericatracy@ip-10-10-56-12 ~]$ cd Downloads/samples
[ericatracy@ip-10-10-56-12 samples]$ ls
cbmrpa.dll  maillfpassword.dll  pRsm.dll  qmsdp.dll  wcdberk.dll
[ericatracy@ip-10-10-56-12 samples]$ sha1sum qmsdp.dll
0781a2b6eb656d110a3a8f60e8bce9d407e4c4ff  qmsdp.dll
[ericatracy@ip-10-10-56-12 samples]$ sha1sum pRsm.dll
9d1ecbbe8637fed0d89fca1af35ea821277ad2e8  pRsm.dll
[ericatracy@ip-10-10-56-12 samples]$
```

Posteriormente nos preguntan ¿Qué marco de malware utiliza estas DLL como módulos complementarios?. Por lo que primero hice una validación en la web y encontré el siguiente [link](#):



ESET researchers have discovered a campaign that we attribute to the APT group known as Evasive Panda, where update channels of legitimate applications were mysteriously hijacked to deliver the installer for the **MgBot malware**, Evasive Panda's flagship backdoor.

En este podemos ver que **ESET** presenta una campaña del grupo APT conocido como Evasive Panda la cual fue dirigida a una ONG, en esta los investigadores descubrieron una campaña que atribuyen al grupo APT conocido como Evasive Panda, donde los canales de actualización de aplicaciones legítimas fueron secuestrados misteriosamente para entregar el instalador del **malware MgBot**, que es la Backdoor insignia de Evasive Panda.

Ahora quieren saber ¿Qué técnica de MITRE ATT&CK está vinculada al uso de pRsm.dll en este marco de malware?, por lo que podemos validarlo de dos formas una es sobre el mismo link que proporcione si buscamos la dll especifica nos mostrara en primera instancia que esta asociada a captura de entrada y salida de audio:

pRsm.dll	Captures input and output audio streams.
----------	--

Y un poco mas abajo nos muestra que esta asociada a la técnica T1123:

Collection	T1123	Audio Capture	MgBot's plugin module pRsm.dll captures input and output audio streams.
	T1119	Automated Collection	MgBot's plugin modules capture data from various sources.
	T1115	Clipboard Data	MgBot's plugin module Cbmrpa.dll captures text copied to the clipboard.
	T1025	Data from Removable Media	MgBot's plugin module sebasek.dll collects files from removable media.
	T1074.001	Data Staged: Local Data Staging	MgBot's plugin modules stage data locally on disk.
	T1114.001	Email Collection: Local Email Collection	MgBot's plugin modules are designed to steal credentials and email information from several applications.
	T1113	Screen Capture	MgBot can capture screenshots.

Pero tambien podemos encontrar esta informacion buscando directamente en la mitre el MgBot

Domain	ID	Name	Use
Enterprise	T1087	.001 Account Discovery: Local Account	MgBot includes modules for identifying local administrator accounts on victim systems. ^[4]
		.002 Account Discovery: Domain Account	MgBot includes modules for collecting information on Active Directory domain accounts. ^[4]
Enterprise	T1123	Audio Capture	MgBot can capture input and output audio streams from infected devices. ^{[2][4]}
Enterprise	T1115	Clipboard Data	MgBot can capture clipboard data. ^{[2][4]}
Enterprise	T1555	Credentials from Password Stores	MgBot includes modules for stealing stored credentials from Outlook and Foxmail email client software. ^{[2][4]}
		.003 Credentials from Web Browsers	MgBot includes modules for stealing credentials from various browsers and applications, including Chrome, Opera, Firefox, Foxmail, QOBrowser, FileZilla, and WinSCP. ^{[2][4]}

ATT&CKoon 6.0 returns October 14-15, 2025 in McLean, VA. More details about tickets and our CFP can be found here
MgBot (\$1146)
+

Selection Controls

Layer Controls

Technique Controls

🔍

✕

🔒

⋮

🔗

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	14 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	9 techniques
Active Scanning	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Cloud Account	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration
Gather Victim Host Information	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Account Discovery	Domain Account	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limit
Gather Victim Identity Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution	BITS Jobs	Build Image on Host	Cloud Secrets Management Stores	Email Account	Internal Spearphishing	Automated Collection	Content Injection	Exfiltrate Over Alternate Protocol
Gather Victim Network Information	Compromise Infrastructure	External Remote Services	Deploy Container	Account Manipulation	Debugger Evasion	Credentials from Web Browsers	Credentials from Web Browsers	Local Account	Audio Capture (H1123)	Automated Collection	Data Encoding	Exfiltrate Over C2 Channel
Gather Victim Org Information	Develop Capabilities	Hardware Additions	Browser Extensions	Boot or Logon Autostart Execution	Decfuscate/Decode Files or Information	Deploy Container	Keychain	Score: 1	Comment: MgBot	Browser Session Hijacking	Data Obfuscation	Exfiltrate Over C2 Channel
Phishing for Information	Establish Accounts	Phishing	Compromise Host Software Binary	Boot or Logon Initialization Scripts	Direct Volume Access	Exploitation for Credential Access	Password Managers	https://att&ckoon.org/gp/MgBot/\$1146	can capture input and output keys	Clipboard Data	Dynamic Resolution	Exfiltrate Over OT Network Medium
Search Closed Sources	Obtain Capabilities	Replication Through Removable Media	Create Account	Boot or Logon Initialization Scripts	Domain or Tenant Policy Modification	Execution Guardrails	Security Memory	Cloud Infrastructure Discovery	ESB: Businessphish 2023:315 Media Symantec: Droggerly 2023:315	Data from Cloud Storage	Encrypted Channel	Exfiltrate Over Web Service
Search Open Technical Databases	Stage Capabilities	Supply Chain Compromise	Scheduled Task/job	Create or Modify System Process	Exploitation for Defense Evasion	Forge Web Credentials	Windows Credential Manager	Cloud Service Dashboard	Application Through Removable Media	Software Deployment Tools	Fallback Channels	Multi-Stage Transfer
Search Open Websites/Domains	Valid Accounts	Trusted Relationship	Event Triggered Execution	Domain or Tenant Policy Modification	File and Directory Permission Modification	Input Capture	Credential API Hooking	Cloud Service Discovery	Container and Resource Discovery	Debugger Evasion	Use Alternate Authentication Material	Non-Standard Port
Search Victim-Owned Websites	Software Deployment Tools	External Remote Services	Hijack Execution Flow	Escape to Host	Hide Artifacts	Hijack Execution Flow	Keylogging	Device Driver Discovery	Domain Trust Discovery	File and Directory Discovery	Data from Network Shared Drive	Transfer Data to Cloud Account
	System Services	User Execution	Implant Internal Image	Exploitation for Privilege Escalation	Indicator Removal	Impersonation	Web Portal Capture	Group Policy Discovery	Log Enumeration	Network Service Discovery	Data Staged	Protocol Tunneling
	Windows Management Instrumentation	Modify Authentication	Hijack	Indirect Command Execution								

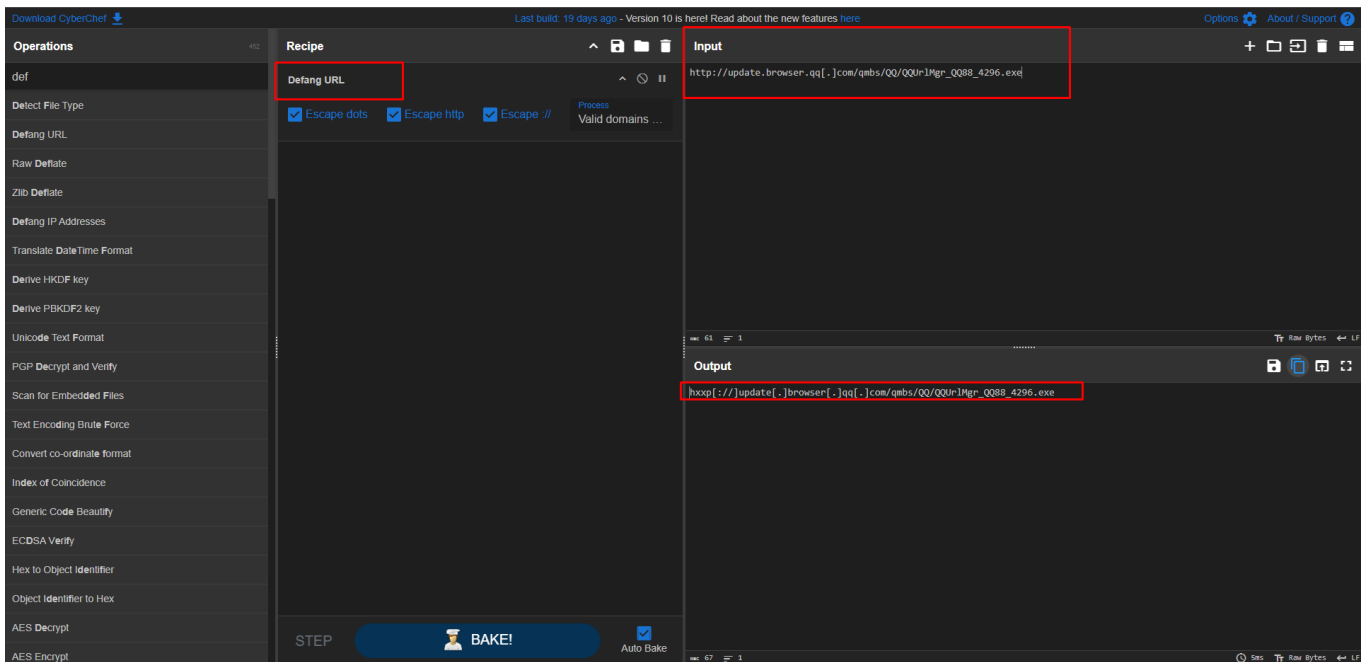
⬆
Legend

Ahora quieren saber ¿Cuál es la URL deshabilitada de CyberChef de la ubicación de descarga maliciosa vista por primera vez el 2 de noviembre de 2020? , en el informe podemos ver un apartado con la tabla de descargas maliciosas asociadas y la URL por lo que debemos copiarla:

Table 1. Malicious download locations according to ESET telemetry

URL	First seen	Domain IP
		123.151.72[.]7
<code>http://update.browser.qq[.]com/qmbs/QQ/QUrlMgr_QQ88_4296.exe</code>	2020-11-02	
		183.232.96[.]1
		61.129.7[.]35

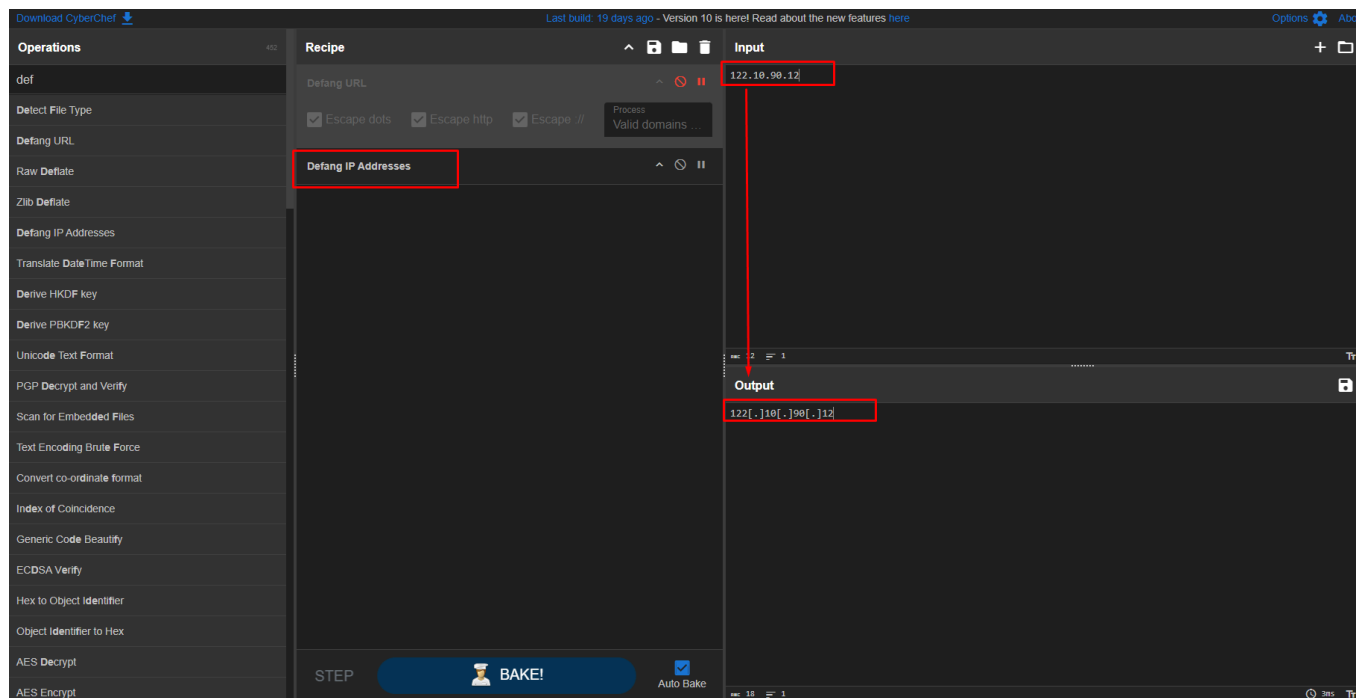
Y para verla en modo deshabilitada usar la opción de Defang URL esta opción la debemos usar debido a que al compartir una URL, direcciones IP y direcciones de correo electrónico sospechosas o maliciosas, no queremos que la persona que reciba el informe haga clic en esos enlaces accidentalmente. Para evitarlo, debemos **desactivar** las URL o direcciones IP para que el software no las convierta en enlaces clicables, debido a esto usamos la función de Cyberchef:



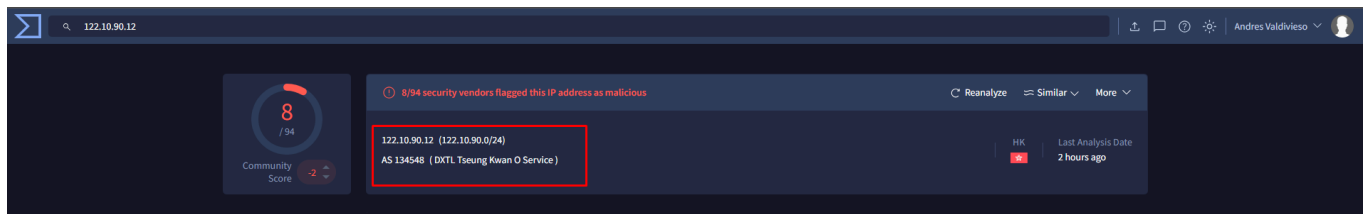
Ahora nos piden saber ¿Cuál es la dirección IP del servidor C&C detectado por primera vez el 14 de septiembre de 2020 utilizando estos módulos?, si vemos el informe encontraremos la parte de Network en la cual vemos dos IP asociadas a el C&C la que nos solicitan es la .12 a lo cual volvemos a aplicar el mismo principio de la pregunta anterior usando el Cyberchef:

Network

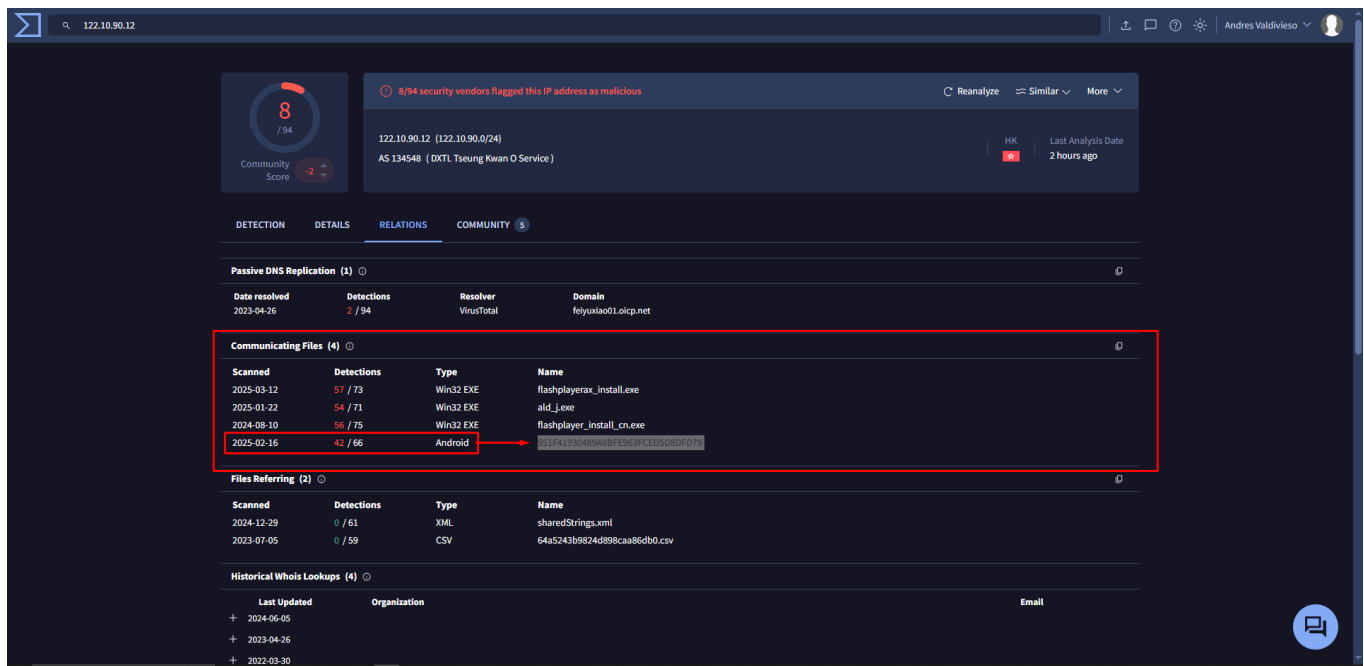
IP	Provider	First seen	Details
122.10.88[.]226	AS55933 Cloudie Limited	2020-07-09	MgBot C&C server.
122.10.90[.]12	AS55933 Cloudie Limited	2020-09-14	MgBot C&C server.



Si bien ya tenemos bastante información sobre el artefacto nos piden identificar ¿Cuál es el hash SHA1 del software espía de la familia *SpyAgent* alojado en la misma IP que apunta a dispositivos Android el 16 de noviembre de 2022?, con esta información lo que debemos hacer es buscar en fuentes de inteligencia a lo cual busque la IP 122[.]10[.]90[.]12 en VirusTotal y encontramos lo siguiente:



Ahora si ingresamos a las Relations en la parte de Communication Files vemos 4 uno de ellos es de tipo android:



Este tiene asociado un link al artefacto por lo que debemos ir a este:

Link al Artefacto

951F41930489A8BFE963FCED5D8DFD79

bbf5975a0483220fec379c44a487ed4146e0af9205f00dbc0eb53de8a63533

42/66 security vendors flagged this file as malicious

Community Score: 42 / 66

Size: 1022.13 KB | Last Analysis Date: 24 days ago | APK

android obfuscated contains-elf checks-gps runtime-modules apk reflection telephony sends-sms

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 3

Popular threat label: trojan.spyagent/fhv | Threat categories: trojan spyware | Family labels: spyagent fhv

Security vendors' analysis

AhnLab-V3	Spyware.Android.BgService.557579	Alibaba	TrojanSpy.Android.Injector.f8d60db
ALYac	Trojan.Linux.Generic.4497	Antiy-AVL	Trojan.Android.Injector.e
Arcabit	Trojan.Linux.Generic.D1191	Avast	Android.SpyAgent-UT [Trj]
Avast-Mobile	Android:Evo-gen [Trj]	AVG	Android.SpyAgent-UT [Trj]
Avira (no cloud)	ANDROID/SpyAgent.FJHV.Gen	BitDefender	Trojan.Linux.Generic.4497
BitDefenderFalx	Android.Trojan.SpyAgent.A	CTX	Apk.trojan.spyagent
Cynet	Malicious (score: 99)	DrWeb	Android.SmsSpy.1973
Emsisoft	Trojan.Linux.Generic.4497 (B)	eScan	Trojan.Linux.Generic.4497
ESET-NOD32	Multiple Detections	Fortinet	Android/Agent.JLitr.spy
GData	Trojan.Linux.Generic.4497	Google	Detected

En este ya podemos ir a la Details y encontraremos el Sha1 del artefacto de tipo Android indicado. Con esto logramos recabar toda la información sobre el artefacto y nos podemos dar una idea del mismo.

Conclusión

El análisis detallado de las muestras de malware proporcionadas por nos reveló una serie de hallazgos críticos que apuntaban a la actividad del grupo **Evasive Panda**, donde pudimos determinar un APT con antecedentes de comprometer sistemas a través de secuestro de canales de actualización de software legítimos. Que contaba con la presencia de la DLL **pRsm.dll**, que es utilizada en el malware **MgBot**, estos nos permitió identificar su asociación con la técnica **T1123 (Screen Capture)** de MITRE ATT&CK, confirmando que tenía la capacidad para capturar y exfiltrar información de audio.

Además, con la correlación de los indicadores de compromiso (IOC) pudimos descubrir que la infraestructura maliciosa está activa desde el 2020, incluyendo una **URL utilizada para la distribución del malware** y una **dirección IP asociada a un servidor de comando y control (C2)**. Posteriormente y bajo el análisis en VirusTotal, identificamos también un **software espía de la familia SpyAgent**, alojado en la misma infraestructura maliciosa y dirigido a dispositivos Android, lo que sugiere un ecosistema de amenazas multidispositivo con objetivos diversos.

Estos hallazgos nos refuerzan la importancia de implementar controles preventivos y estrategias de defensa proactiva, tales como:

- **Segmentación y monitoreo de tráfico** para detectar patrones anómalos de comunicación con servidores sospechosos.
- **Análisis de comportamiento en endpoints** para identificar actividades maliciosas relacionadas con técnicas de captura y exfiltración de datos.
- **Políticas de restricción y verificación de actualizaciones de software** para evitar el secuestro de paquetes legítimos.

Este análisis nos muestra cómo los actores de amenazas continúan evolucionando sus tácticas para comprometer los sistemas de alto valor. Por lo que al tener una detección temprana y contar con correlación de inteligencia de amenazas podemos mitigar el impacto de estos ataques y reforzar la seguridad de las organizaciones frente a grupos APT.