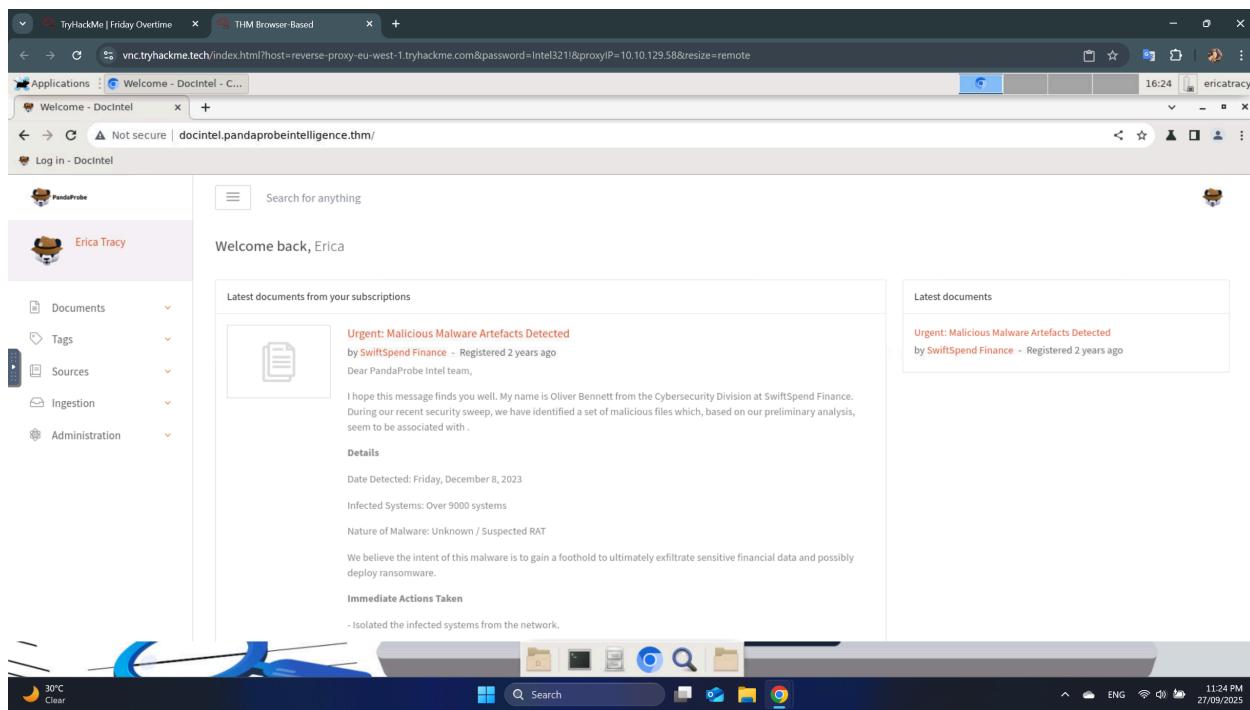


Friday Overtime

Step into the shoes of a Cyber Threat Intelligence Analyst and put your investigation skills to the test.

In this challenge, we will be assuming the role of a CTI (Cyber Threat Intelligence) analyst, investigating a ticket by a member of the security division at the company.

We start the challenge by inspecting the ticket we were left by the security department, which has the details of the attempted attack along with the malicious artefacts in a .zip file.



When we open the document, we see the full email, along with *samples.zip* that we can download to analyze.

Screenshot of a web browser showing an email from PandaProbe to Erica Tracy. The email subject is "Urgent: Malicious Malware Artefacts Detected".

Registration Information:

- Reference: DI-2023-12-002
- Classification: TLP:RED
- Document Date: 2023-12-07T23:10:00.0000000
- Registration Date: 2023-12-07T23:10:51.5503900
- Last Modification: 2024-01-12T21:40:35.0782360

Files/Attachments:

- samples.zip** (2023-12-07T23:10:51.8621190)

Source Information:

- SwiftSpend Finance
- Reliability:** A (Reliable)

Email Content:

Dear PandaProbe Intel team,

I hope this message finds you well. My name is Oliver Bennett from the Cybersecurity Division at SwiftSpend Finance. During our recent security sweep, we have identified a set of malicious files which, based on our preliminary analysis, seem to be associated with.

Details

Date Detected: Friday, December 8, 2023
 Infected Systems: Over 9000 systems.
 Nature of Malware: Unknown / Suspected RAT
 We believe the intent of this malware is to gain a foothold to ultimately exfiltrate sensitive financial data and possibly deploy ransomware.

Immediate Actions Taken

- Isolated the infected systems from the network.
- Initiated a comprehensive scan across all systems.
- Collected and stored malware samples securely for further analysis.
- We are currently collaborating with external cybersecurity agencies and our security solutions providers to get a deeper understanding of this malware. However, we wanted to raise this with you immediately given the potential risk associated with APTs.

We strongly need your team's assistance with conducting a thorough review of the malware sample. The password to the attached archive is: *Panda32!*

Moving forward, we are going to conduct a User Awareness Training to inform all staff members to be extra cautious, especially when dealing with email attachments and links.

Attached are the indicators of compromise (IoCs) for your perusal. I am also available for a call or meeting to discuss our findings in detail and strategise our response.

Your prompt attention to this matter is highly appreciated. Let's work together to ensure the safety and integrity of our systems and data.

Warm regards,
 Oliver Bennett
 Cybersecurity Division
 SwiftSpend Finance
 Phone: +123 456 7890
 Email: oliver.bennett@swiftpend.finance

Just by reading the email, we are presented with the answer of the first question.

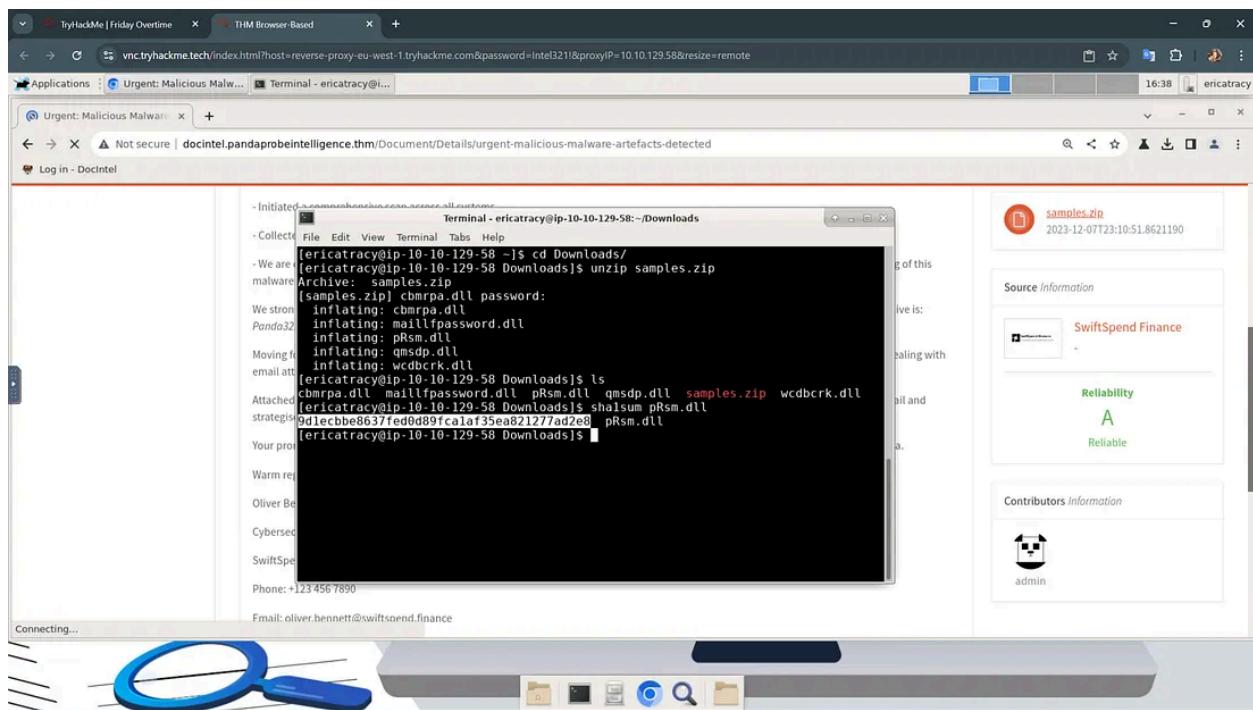
Who shared the malware samples?

Answer: **Oliver Bennett**

We then download the sample.zip folder, unzip it and inspect what we find. We got several .dll files. Simply put, a DLL (Dynamic-Link Library) file is a library that contains code and data that can be used by several programs and processes on the MS Windows OS. They are one of the most common file types to be used as malicious files.

What is the SHA1 hash of the file "pRsm.dll" inside samples.zip?

We can get the answer by unzipping the folder then calculating the SHA1 hash of this file.



Answer: **9d1ecbbe8637fed0d89fca1af35ea821277ad2e8**

Which malware framework utilizes these DLLs as add-on modules?

If we searched for pRsm.dll, we'll have this [article](#) be ESET as the first search result.

Going through it, we find the malware framework that used these DLLs.

weLiveSecurity™ by ESET Award-winning news, views, and insight from the ESET security community English

TIPS & ADVICE BUSINESS SECURITY ESET RESEARCH WeLiveScience FEATURED TOPICS ABOUT US

26 Apr 2023 • 12 min. read

Table of Contents

- Evasive Panda profile
- Campaign overview
- Attribution
- Technical analysis
- Conclusion
- IoCs
- MITRE ATT&CK techniques

Key points of the report:

Answer: **MgBot**

Which MITRE ATT&CK Technique is linked to using pRsm.dll in this malware framework?

Searching for pRsm.dll in the article using **Ctrl + F**, we find the MITRE ATT&CK Technique used by this file.

Discovery	T1016	System Network Configuration Discovery	MgBot has the capability to recover network information.
	T1083	File and Directory Discovery	MgBot has the capability of creating file listings.
	T1056.001	Input Capture: Keylogging	MgBot plugin module <code>kstres.dll</code> is a keylogger.
	T1560.002	Archive Collected Data: Archive via Library	MgBot's plugin module <code>sebasek.dll</code> uses aPLib to compress files staged for exfiltration.
	T1123	Audio Capture	MgBot's plugin module <code>prem.dll</code> captures input and output audio streams.
	T1119	Automated Collection	MgBot's plugin modules capture data from various sources.
Collection	T1115	Clipboard Data	MgBot's plugin module <code>Cbmrsa.dll</code> captures text copied to the clipboard.
	T1025	Data from Removable Media	MgBot's plugin module <code>sebasek.dll</code> collects files from removable media.
		Data Staged: Local Data	MgBot's plugin modules store data locally on

Answer: **T1123**

What is the CyberChef defanged URL of the malicious download location first seen on 2020-11-02?

If we go through the article, we will come across a “*Technical Analysis*” section that provides the URL from where the download originated, according to ESET telemetry data.

In Table 1, we provide the URL from where the download originated, according to ESET telemetry data, including the IP addresses of the servers, as resolved at the time by the user's system; therefore, we believe that these IP addresses are legitimate. According to passive DNS records, all of these IP addresses match the observed domains, therefore we believe that these IP addresses are legitimate.

Table 1. Malicious download locations according to ESET telemetry

URL	First seen	Domain IP
http://update.browser.qq[.]com/qmbs/QQ/QQUr1Mgr_QQ88_4296.exe	2020-II-02	123.151.72[.]7
		183.232.96[.]1
		61.129.7[.]35

We then copy the URL and go to [CyberChef](#) to defang it. To defang a URL is to modify a potentially harmful link, making it non-functional and safe to share.

Operations

def

Recipe

Defang URL

Input

http://update.browser.qq[.]com/qmbs/QQ/QQUr1Mgr_QQ88_4296.exe

Output

hxxp[://]update[.]browser[.]qq[.]com/qmbs/QQ/QQUr1Mgr_QQ88_4296.exe

Answer: **hxxp[://]update[.]browser[.]qq[.]com/qmbs/QQ/QQUr1Mgr_QQ88_4296[.]exe**

What is the CyberChef defanged IP address of the C&C server first detected on 2020-09-14 using these modules?

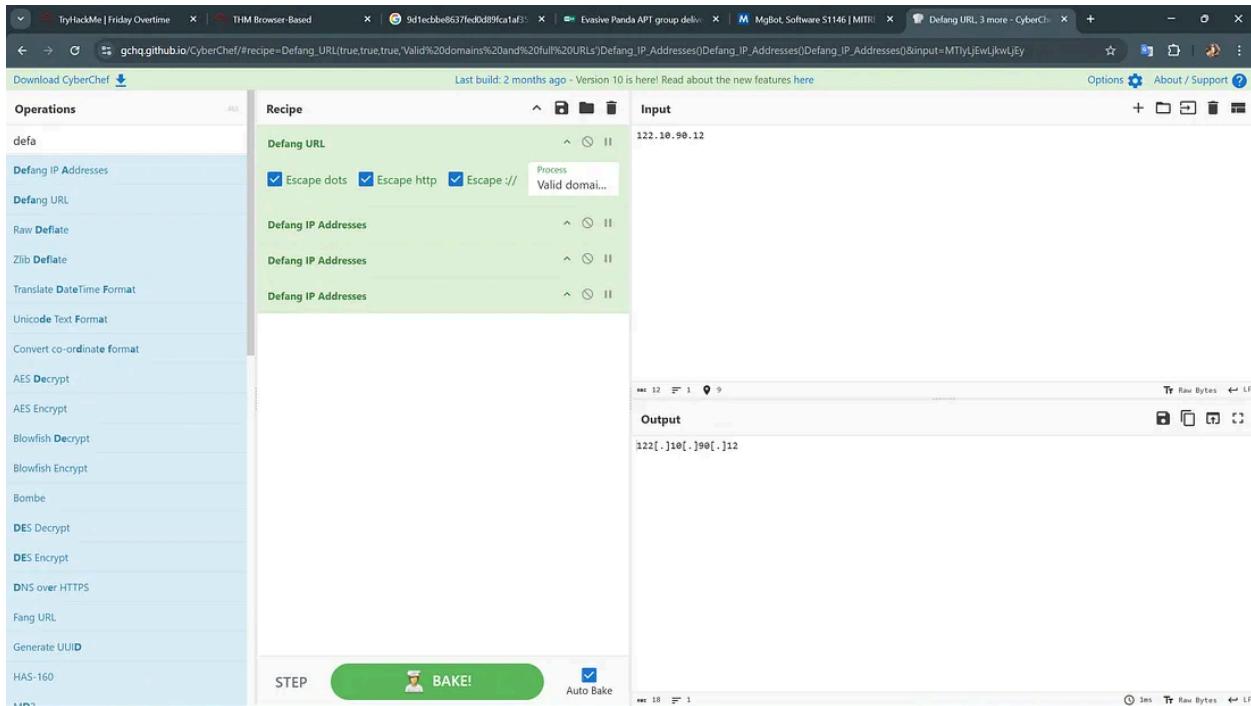
In the “IoCs” section of the article, we find a table of network IoCs, containing the IP address of the C2 server first detected on the specified date.

The screenshot shows a web browser window with multiple tabs open. The active tab is from [we-live-security.com](https://we-live-security.com/2023/04/26/evasive-panda-apt-group-malware-updates-popular-chinese-software/#mitre-attck-techniques), displaying information about Evasive Panda APT group malware. The page includes a navigation bar with links like TIPS & ADVICE, BUSINESS SECURITY, ESET RESEARCH, WeLiveScience, FEATURED, TOPICS, ABOUT US, and a search bar. On the left, there's a table titled "Network" with columns for IP, Provider, First seen, and Details. It lists two entries: one for 122.10.88[.]226 and another for 122.10.90[.]112, both associated with AS55933 Cloudie Limited and first seen on 2020-07-09. To the right of the table is a large advertisement for ESET Threat Intelligence, featuring a network diagram and a "GET A DEMO" button. Below the table, there's a section titled "MITRE ATT&CK techniques" with a note that it was built using version 12 of the framework. A table lists tactics, IDs, names, and descriptions, including T1583.004 for Acquire Infrastructure: Server and T1587.001 for Develop Capabilities: Malware.

IP	Provider	First seen	Details
122.10.88[.]226	AS55933 Cloudie Limited	2020-07-09	MgBot C&C server.
122.10.90[.]112	AS55933 Cloudie Limited	2020-09-14	MgBot C&C server.

Tactic	ID	Name	Description
Resource Development	T1583.004	Acquire Infrastructure: Server	Evasive Panda acquired servers to be used for C&C infrastructure.
	T1587.001	Develop Capabilities: Malware	Evasive Panda develops its custom MgBot backdoor and plugins, including obfuscated

We repeat the ‘defanging’ process using CyberChef, this time for the IP address.



Answer: **122[.]10[.]90[.]12**

What is the md5 hash of the spyagent family spyware hosted on the same IP targeting Android devices in Jun 2025?

For this question, we can use any reputation checker to see data related to this IP address. We'll use the one and only [VirusTotal](#). We search for the IP address on VT, and go to the "Relations" tab where we can find related info.

Press enter or click to view image in full size

Did you intend to search across the file corpus instead? [Click here](#)

5 / 95 security vendors flagged this IP address as malicious

122.10.90.12 (122.10.90.0/24)
AS 134548 (DXTL Tseung Kwan O Service)

Community Score: 5

Detection Details Relations Community 10

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendor's analysis	Do you want to automate checks?
alphaMountain.ai Malicious	CyRadar Malicious
Fortinet Malware	SOCRadar Malware
Webroot Malicious	Forcepoint ThreatSeeker Suspicious
Abusix Clean	Acronis Clean
ADMINUSLabs Clean	AI Labs (MONITORAPP) Clean

Did you intend to search across the file corpus instead? [Click here](#)

5 / 95 security vendors flagged this IP address as malicious

122.10.90.12 (122.10.90.0/24)
AS 134548 (DXTL Tseung Kwan O Service)

Community Score: 5

Detection Details Relations Community 10

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Passive DNS Replication (1) [View](#)

Date resolved	Detections	Resolver	Domain
2023-04-26	2 / 95	VirusTotal	felyuxiao01.oicp.net

Communicating Files (4) [View](#)

Scanned	Detections	Type	Name
2025-03-13	60 / 73	Win32 EXE	flashplayerax_install.exe
2025-01-22	54 / 71	Win32 EXE	ald_j.exe
2024-08-10	56 / 75	Win32 EXE	flashplayer_install_cn.exe
2025-08-31	42 / 67	Android	951F41930489A8BFE963FCED5D8DFD79

We find a file related to this IP address whose Type is Android. When we click on its name, we are directed to a separate page for this malware. On the "Details" tab, we find its MD5 hash and therefore our final answer.

42 / 67

42/67 security vendors flagged this file as malicious

bbebf5975a0483220cfec379c44a487ed4146e0af9205f00dbc0eb53de8a63533

951f41930489a8bfe963fcfd5d8df79.virus

Size: 1022.13 KB | Last Analysis Date: 27 days ago | APK

Community Score: -2

Basic properties

MD5	951f41930489a8bfe963fcfd5d8df79
SHA-1	1c1fe906e822012f6235cc53f601d006d15d7be
SHA-256	bbebf5975a0483220cfec379c44a487ed4146e0af9205f00dbc0eb53de8a63533
Vhash	ad4e496212bafb6522fd3d9a0e4f0711
SSDEEP	24576:\$SEEv0KfZ1SgjSpWA9kcE5BErKLZ9YMIj9nMdP99cnO8S:vw31SgIA9t0u2Z5+9nicnOV
TLSH	T18B25335227C1C689FA70A67E8F0BC07C3525341A3819C3D750E8A00C6653E4E9F9F6AE
Permalink	19366572235393940964ba4ea2501ba10eb0452b61fac715c3bb86078904b92e
File type	Android executable mobile android apk
Magic	Zip archive data, at least v2.0 to extract; compression method=deflate
TrID	Android Package (42.1%) Java Enterprise Archive (30.4%) Java Archive (21%) ZIP compressed archive (6.2%)
Magik	APK
File size	1022.13 KB (1046663 bytes)

Answer: **951F41930489A8BFE963FCED5D8DFD79**

Et Voilà!

You did it! 🎉 Friday Overtime complete!

Points earned	210
Completed tasks	1
Room type	Challenge
Difficulty	Medium
Streak	214

78,544 users are actively learning this week

This was a straightforward challenge with no need to use any special tools, only your Threat Intel mindset, and the mighty Virus Total!