


Friday Overtime

quarta-feira, 29 de outubro de 2025 14:52

- **Propósito do desafio:**
 - O desafio consiste em fazer uma análise de malware enviado por uma organização via e-mail.
 - Para essa análise, ferramentas CTI serão de suma importância.
- **Task 1:**
 - A primeira questão estava querendo saber quem era o responsável da organização que nos enviou o malware para análise, facilmente isso é decifrado lendo o conteúdo do e-mail.

Latest documents from your subscriptions



Urgent: Malicious Malware Artefacts Detected
by **SwiftSpend Finance** - Registered 2023-12-07T23:10:51.5503900

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

Latest documents

Urgent: Malicious Malware Art...
by **SwiftSpend Finance** - Registered 2023-12-07T23:10:51.5503900

- Oliver Bennett é nossa resposta.

- **Task 2:**
 - A segunda questão estava querendo saber o hash sha1 de um dos arquivos .dll que compõem esse suposto software malicioso, denominado "pRsm.dll", para tal, basta fazermos download da pasta que contém o software suspeito que nos foi enviado via e-mail, e puxar via terminal o hash do arquivo desejado.

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

Reference	DI-2023-12-002
Classification	TLP:RED
Document Date	2 years ago
Registration Date	2 years ago
Last Modification	2 years ago

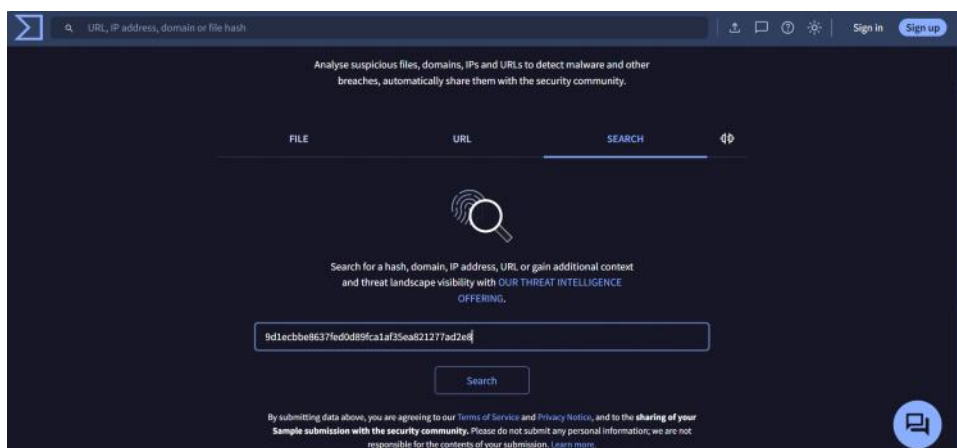
Files Attachments [View all](#)

 **samples.zip**
2 years ago

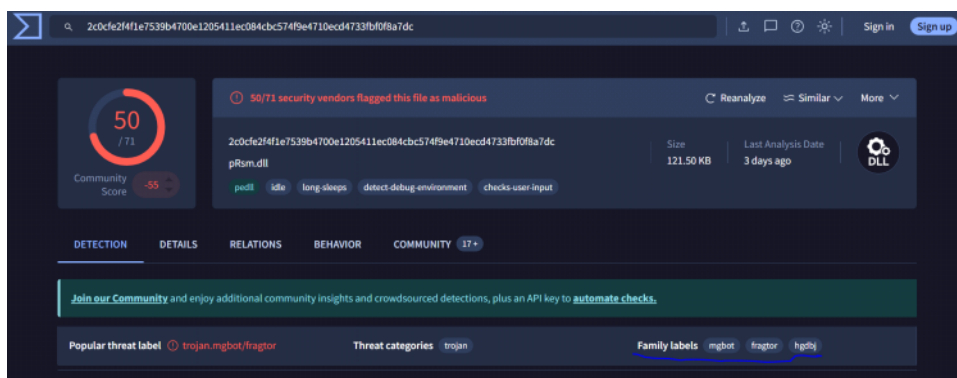
Source information

```
Terminal - ericatracy@ip-10-201-91-161:~/Desktop/samples
File Edit View Terminal Tabs Help
[ericatracy@ip-10-201-91-161 samples]$ sha1sum pRsm.dll
9d1ecbbe8637fed0d89fca1af35ea821277ad2e8  pRsm.dll
[ericatracy@ip-10-201-91-161 samples]$
```

- Task 3:
 - A terceira questão estava querendo saber qual é o framework malicioso que está por trás dos arquivos .dll que compõem o arquivo, nessa etapa, foi necessário consultar uma CTI para buscar informações sobre esse framework, então utilizei a aplicação VirusTotal - CTI que analisa arquivos maliciosos por meio de URL, endereço IP, nome de domínio hash ou o próprio arquivo.



- Consultei o hash do arquivo .dll da questão anterior usando essa CTI, me foi retornado detalhes desse arquivo, e na aba de rótulos familiares relacionados a esse arquivo, haviam alguns nomes.



- Decidi pesquisar o primeiro rótulo no mitre att&ck - Framework de conhecimento utilizado para categorizar e descrever comportamentos de ataques cibernéticos, e houve retorno.

MITRE | ATT&CK

Matrices | Tactics | Techniques | Defenses | CTI | Resources | Benefactors | Blog | Search

ATT&CK v18 has been released! Check out the [blog post](#) or [changelog](#) for more information.

SOFTWARE

Meteor

MgBot

Micropsia

Milan

Mimikatz

MimiPenguin

Miner-C

MiniDuke

MirageFox

Home > Software > MgBot

MgBot

MgBot is a modular malware framework exclusively associated with Daggerfly operations since at least 2012. MgBot was developed in C++ and features a module design with multiple available plugins that have been under active development through 2024.^{[1][2][3]}

ID: S1146

Type: MALWARE

Platforms: Windows

Version: 1.0

Created: 25 July 2024

Last Modified: 10 October 2024

[Version Permalink](#)

- Com base nisso, conseguimos descobrir o framework malicioso relacionado aos arquivos .dll, MgBot.

Task 4:

- A quarta questão queria saber o id da técnica relacionada ao arquivo "pRsm.dll", com um simples google e algumas rolagens de tela, encontrei a informação que queria no WeLiveSecurity - CTI que fornece soluções, artigos e análises sobre as mais recentes ameaças cibernéticas e tendências de segurança.

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

File stealer.

Has a configuration file that enables the collection of files from different sources: HDDs, USB thumb drives, and CD-ROMs; as well as criteria based on the file properties: filename must contain a keyword from a predefined list, file size must be between a defined minimum and maximum size.

Cbrmpa.dll Captures text copied to the clipboard and logs information from the USBSTOR registry key.

pRsm.dll Captures input and output audio streams.

Credential stealer.

Steals credentials from Outlook and Foxmail email client software.

Credential stealer.

Steals credentials from Chrome, Opera, Firefox, Foxmail, QQBrowser, FileZilla, and WinSCP, among others.

A complex plugin designed to steal the content from the Tencent QQ database that stores the user's message history. This is achieved by in-memory patching of the software component KernelDns.dll and dropping a fake userenv.dll DLL.

Evasive Panda profile

Campaign overview

Attribution

Technical analysis

Conclusion

IoCs

MITRE ATT&CK techniques

eset THREAT INTELLIGENCE

GET A DEMO

- Com essa informação, voltamos ao mitre att&ck e identificamos que a técnica relacionada a capturar entrada/saída de áudio a esse software é o T1123.

MgBot

MgBot is a modular malware framework exclusively associated with Daggerfly operations since at least 2012. MgBot was developed in C++ and features a module design with multiple available plugins that have been under active development through 2024.^{[1][2][3]}

ID: S1146

Type: MALWARE

Platforms: Windows

Version: 1.0

Created: 25 July 2024

Last Modified: 10 October 2024

[Version Permalink](#)

Techniques Used

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	<u>T1123</u>	<u>Audio Capture</u>	<u>MgBot can capture input and output audio streams from infected devices.</u> ^{[2][4]}

ATT&CK Navigator Layers

Task 5:

- A quinta questão queria saber qual foi o primeiro link URL para download desse software malicioso em 11 de fevereiro de 2020, felizmente, consegui essa informação

também no WeLiveSecurity.

welivesecurity by ESET Award-winning news, views, and insight from the ESET security community

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

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
		123.151.72[.]7
<u>http://update.browser.qq[.]com/qmbs/QQ/QQUrlMgr_QQ88_4296.exe</u>	2020-11-02	
		183.232.96[.]1
		61.129.7[.]35

Table of Contents

- Evasive Pand
- Campaign ov
- Attribution
- Technical ana
- Conclusion
- IoCs
- MITRE ATT&A

- Mas a questão pediu que o URL fosse entregue desarmado para não correr o risco de clicar sobre, para isso então, utilizaremos o Cyberchef - Aplicação web que contém várias ferramentas úteis para a cibersegurança, principalmente no quesito codificação/decodificação de elementos.

Recipe

Defang URL

☒ Escape dots ☒ Escape http ☒ Escape //

Process
Valid domains and full URLs

Input

http://update.browser.qq[.]com/qmbs/QQ/QQUrlMgr_QQ88_4296.exe

Output

hxxp[[:]update[.]browser[.]qq[.]com/qmbs/QQ/QQUrlMgr_QQ88_4296.exe

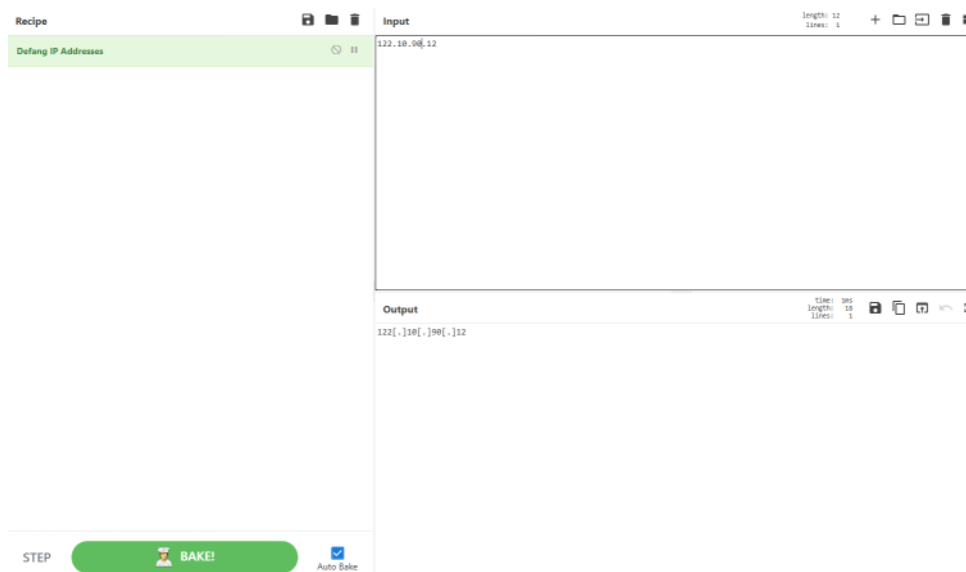
STEP **BAKE!** Auto Bake

- Com a URL desarmada, podemos entregá-la com segurança.
- Task 6:
 - A sexta questão queria saber o endereço IP C&C do servidor desse software que foi detectado no dia 14 de setembro de 2020, e mais uma vez o WeLiveSecurity me salvando oferecendo essa informação de bandeja.

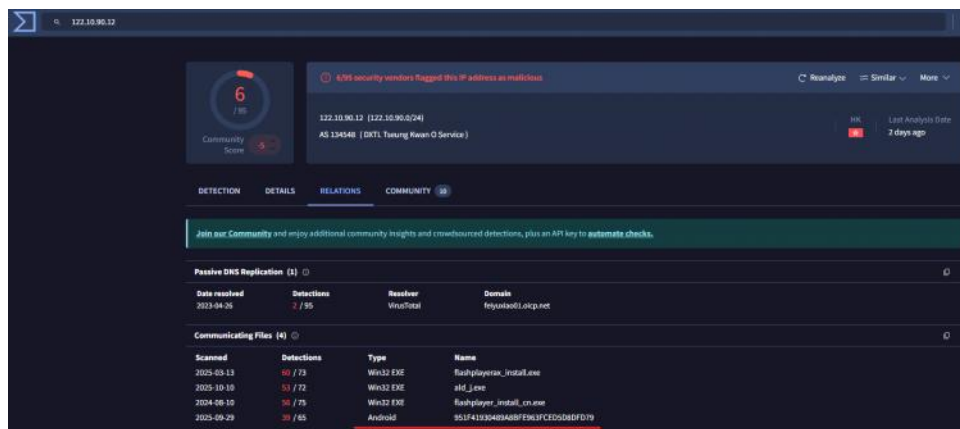
Network

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

- Por mais que uma parte desse IP esteja desarmada, vamos utilizar o Cyberchef para deixá-lo totalmente desarmado, por garantia.



- Task 7:
 - A sétima questão queria saber o hash md5 do spyware que estava hospedado no IP C&C direcionando a dispositivos Android.
 - Para isso, joguei o endereço IP C&C no VirusTotal, e consegui a informação que queria na aba de relacionamentos da análise.



- Aprendizados desse desafio:
 - Sempre ter um grande leque possível de fontes (e que sejam confiáveis) para se buscar informações, uma única não será suficiente suprir tudo.