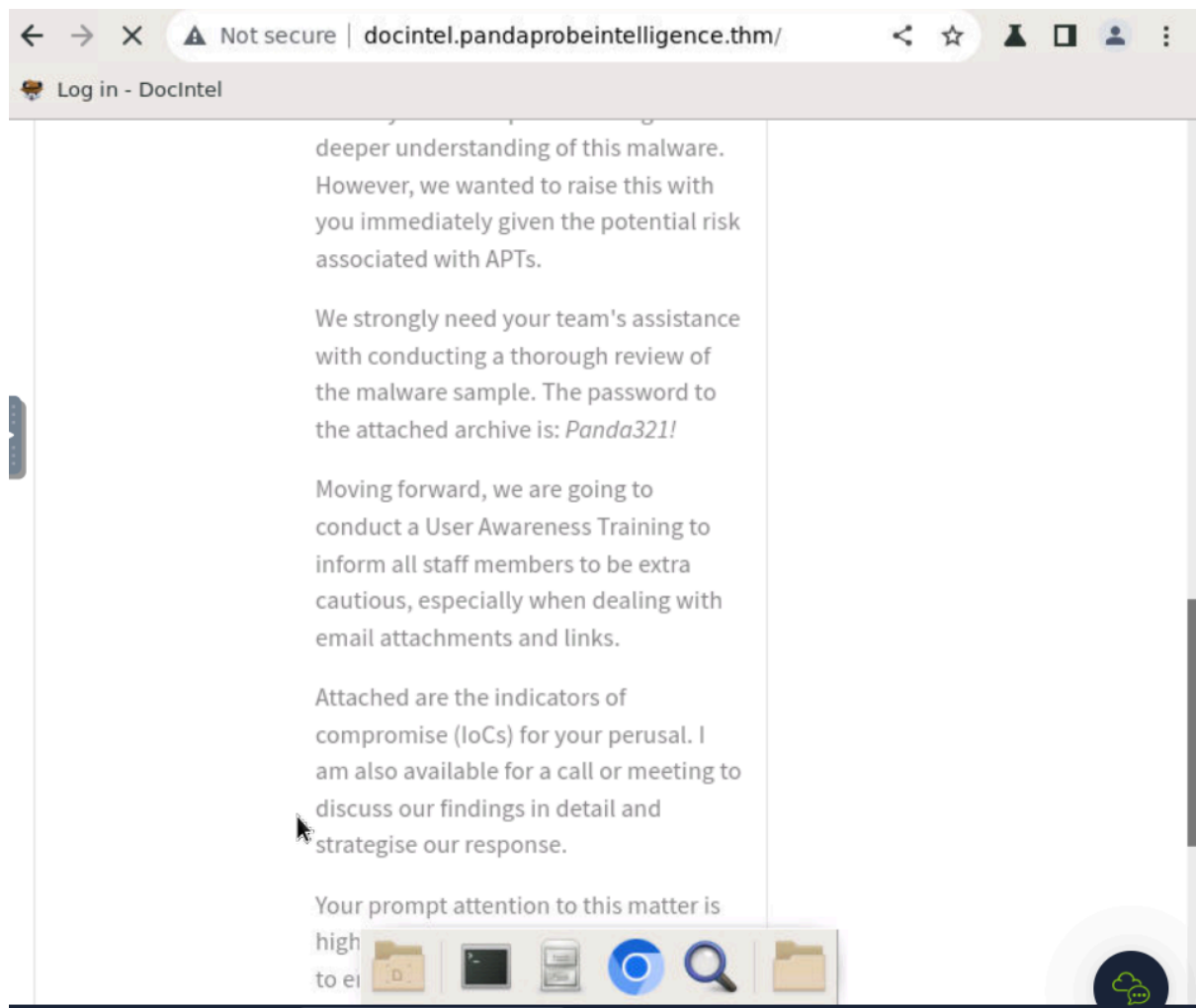


Friday Overtime

this is a challenge , after i learned misp, opecti and yara.
this is classified under the category of threat intelligence.

inside the doc intel platform, and after reading what's needed to be read, I see a password for an archive , so I will save it for later .



I download the samples.zip file to begin my analysis.

after i unzipped it, i found several files.

```

ericatracy@ip-10-10-183-41 ~]$ ls
esktop Downloads
ericatracy@ip-10-10-183-41 ~]$ cd Downloads/
ericatracy@ip-10-10-183-41 Downloads]$ ls
amples.zip
ericatracy@ip-10-10-183-41 Downloads]$ unzip samples.zip
Archive:  samples.zip
  inflating: samples.zip
  inflating: cbmrpa.dll password:
password incorrect--reenter:
password incorrect--reenter:
  inflating: cbmrpa.dll
  inflating: maillfpassword.dll
  inflating: pRsm.dll
  inflating: qmsdp.dll
  inflating: wcdbrk.dll
ericatracy@ip-10-10-183-41 Downloads]$ ls
cbmrpa.dll maillfpassword.dll pRsm.dll qmsdp.dll samples.zip wcdbrk.dll
ericatracy@ip-10-10-183-41 Downloads]$

```

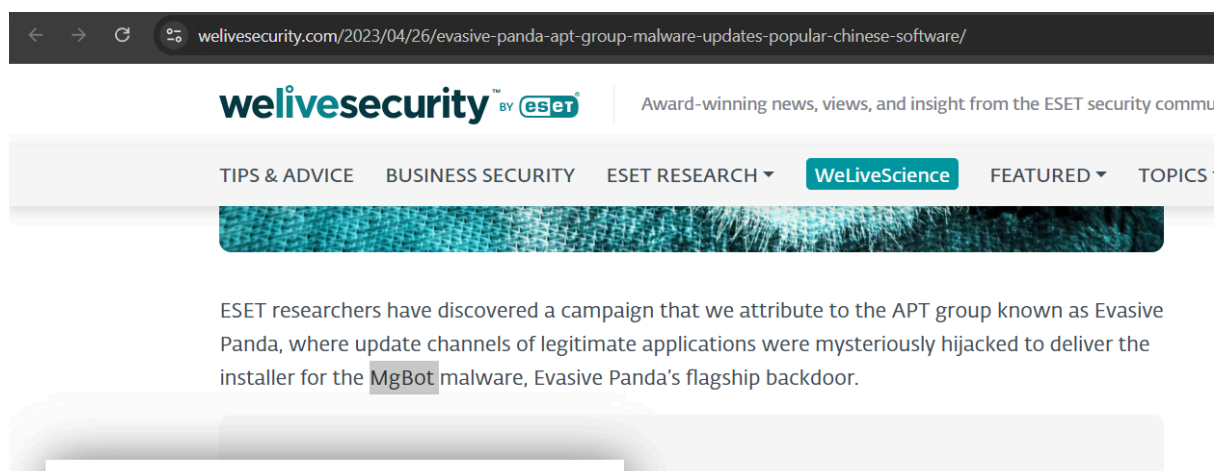
first task is to know the sha1 hash of the file pRsm.dll ,
I will use the the command 'sha1sum'

```

File Edit View Terminal Tabs Help
[ericatracy@ip-10-10-183-41 Downloads]$ sha1sum pRsm.dll
9d1ecbbe8637fed0d89fca1af35ea821277ad2e8  pRsm.dll
[ericatracy@ip-10-10-183-41 Downloads]$

```

the next task is to find which malware framework utilizes these
DLLs as add-on modules?
after some research , i found this article :



← → ↺ 🔍 welivesecurity.com/2023/04/26/evasive-panda-apt-group-malware-updates-popular-chinese-software/

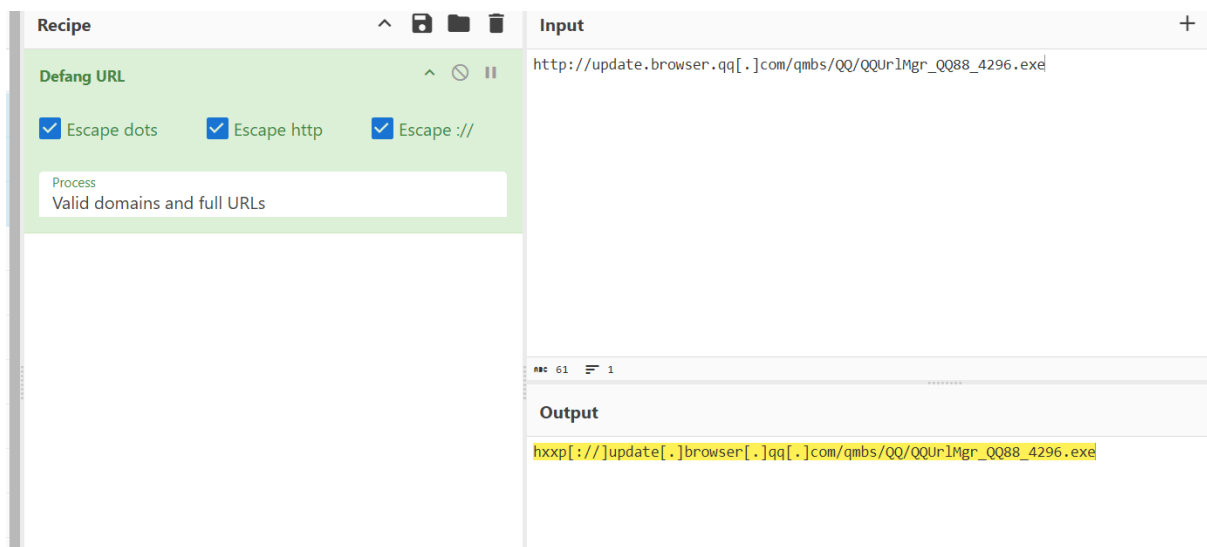
welivesecurity™ BY **ESET** | Award-winning news, views, and insight from the ESET security community

TIPS & ADVICE BUSINESS SECURITY ESET RESEARCH ▾ **WeLiveScience** FEATURED ▾ TOPICS ▾

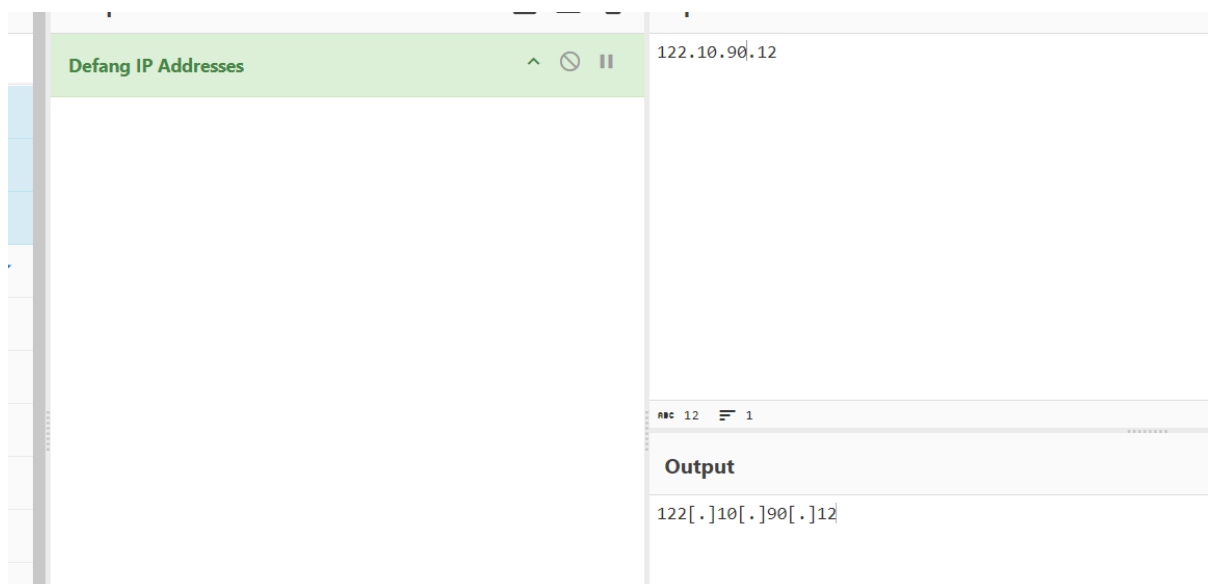
ESET researchers have discovered a campaign that we attribute to the APT group known as Evasive Panda, where update channels of legitimate applications were mysteriously hijacked to deliver the installer for the **MgBot** malware, Evasive Panda's flagship backdoor.

in the same page i will find the next answer.

next answer



defanged IP address of the C&C server first detected on 2020-09-14



Now i open VirusTotal , i search with '122.10.90.12' , the goal is to find the spyagent family spyware hosted on the same IP targeting Android devices on November 16, 2022.

well i found Android but the date changed :

/ 94

Community Score

1

122.10.90.12 (122.10.90.0/24)

AS 134548 (DXTL Tseung Kwan O Service)

DETECTION

DETAILS

RELATIONS

COMMUNITY 2

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Passive DNS Replication (1)

Date resolved	Detections	Resolver	Domain
2023-04-26	2 / 94	VirusTotal	feiyuxiao01.oicp.net

Communicating Files (4)

Scanned	Detections	Type	Name
2024-08-10	48 / 75	Win32 EXE	flashplayerax_install.exe
2024-02-13	42 / 71	Win32 EXE	ald_j.exe
2024-08-10	56 / 75	Win32 EXE	flashplayer_install_cn.exe
2024-10-27	43 / 67	Android	951F41930489A88FE963FCED5D8DFD79

Files Referring (2)

Scanned	Detections	Type	Name
---------	------------	------	------

I open it and i find the sha1 value .