LetsDefend

THE BEST SOC ANALYST TOOLS

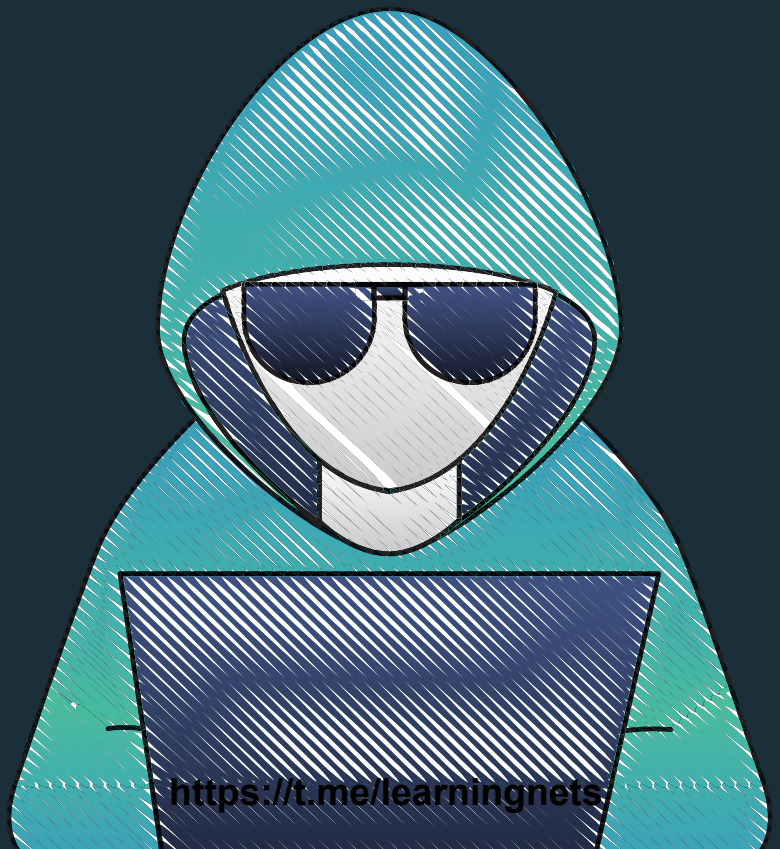
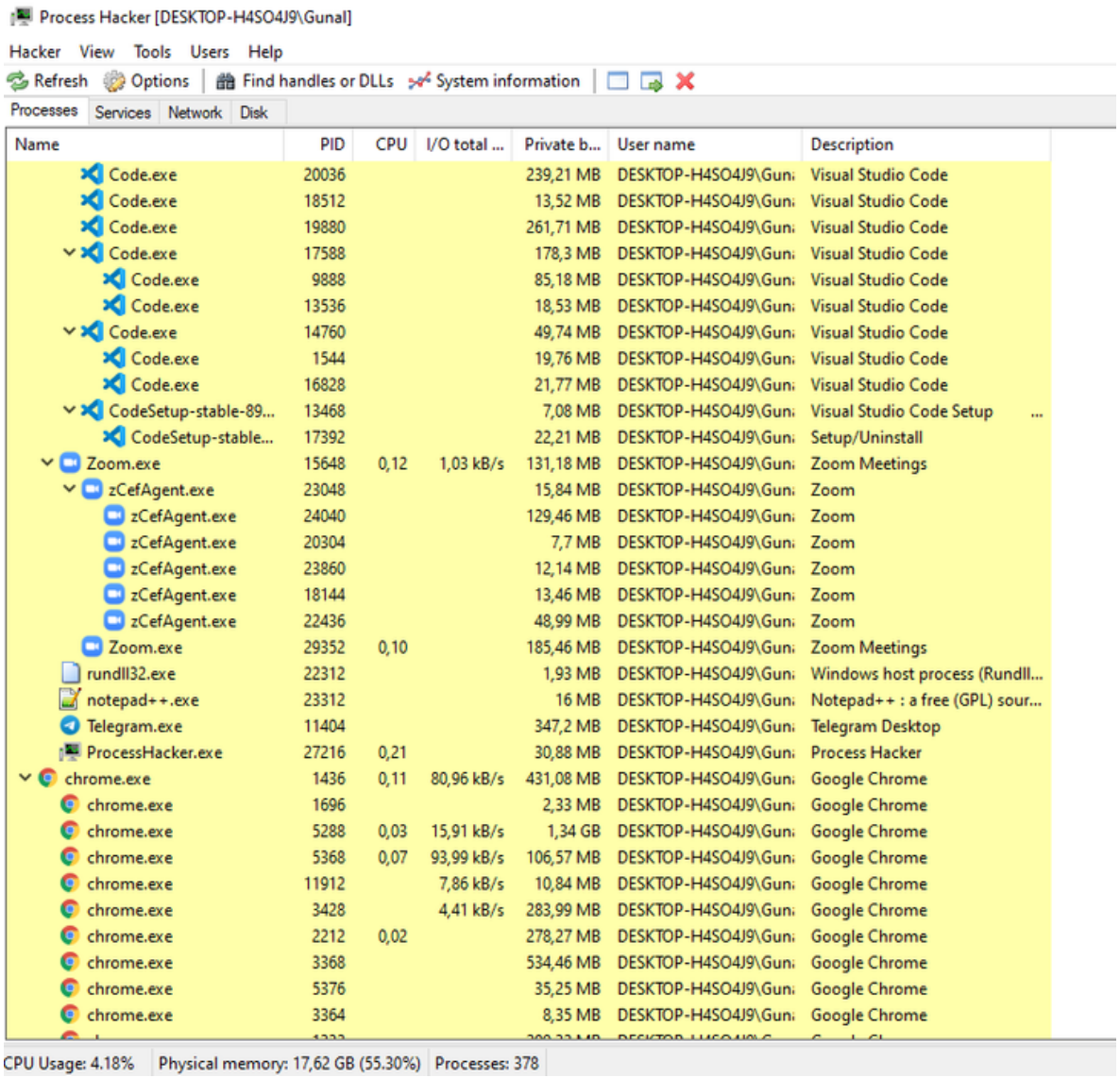


TABLE OF CONTENTS

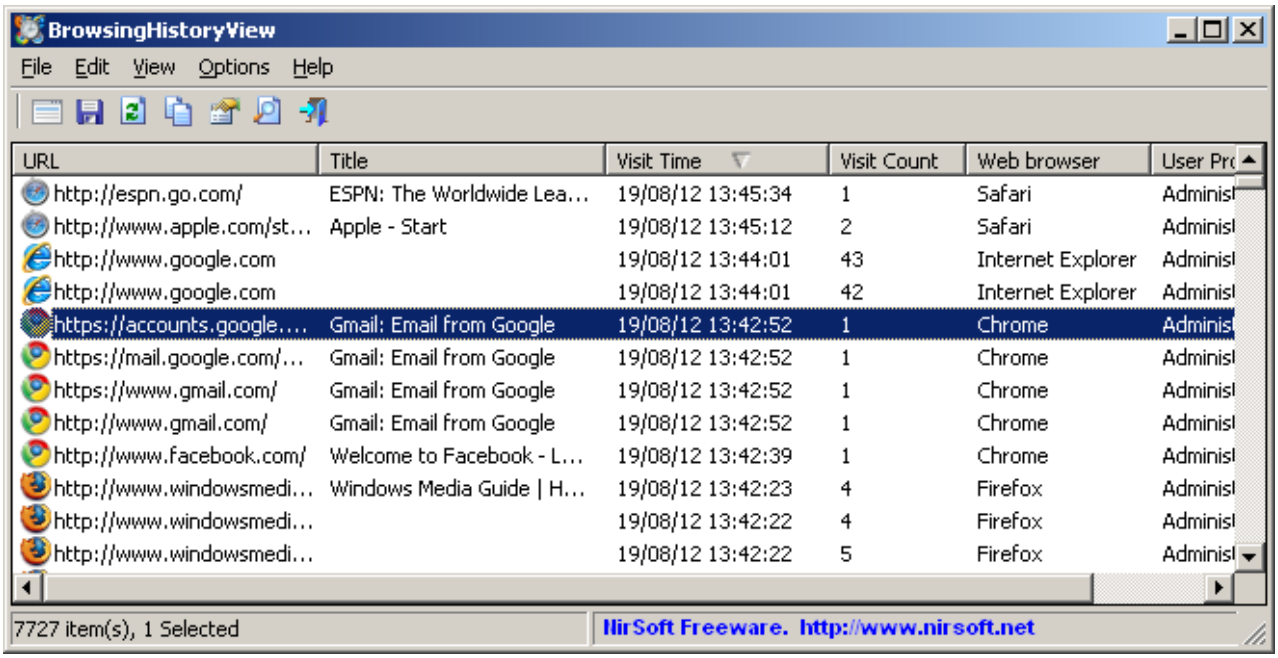
Process Hacker

Great tool for monitoring the system and detecting suspicious situations. It's also free.



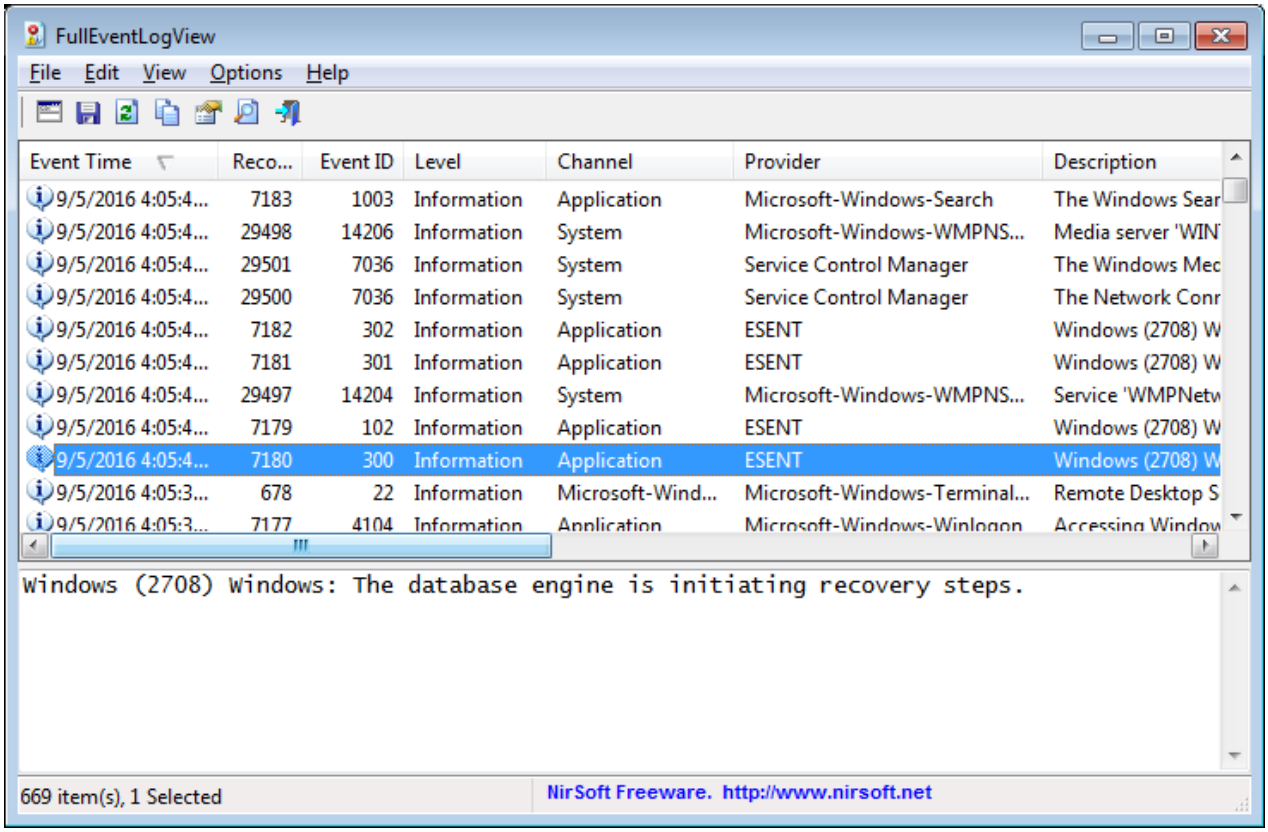
BrowsingHistoryView

It gives you the history of different browsers in one table.



FullEventLogView

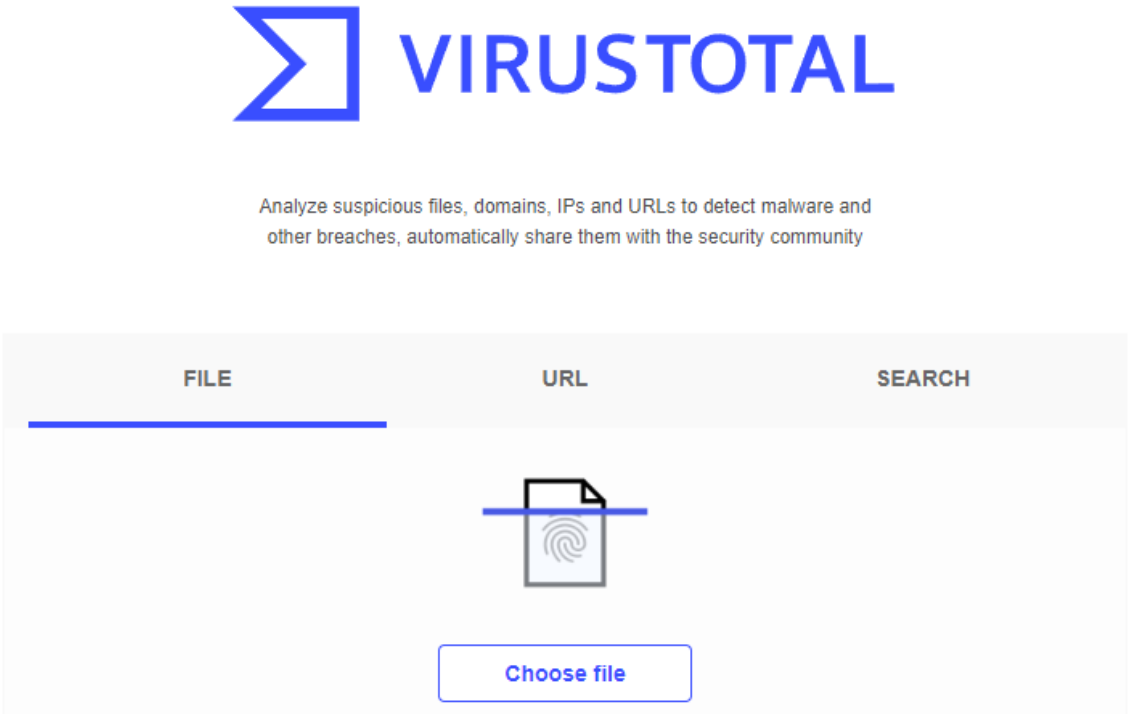
It displays all event logs in a table, which helps to decrease the investigation time.



Checking Reputation

VirusTotal

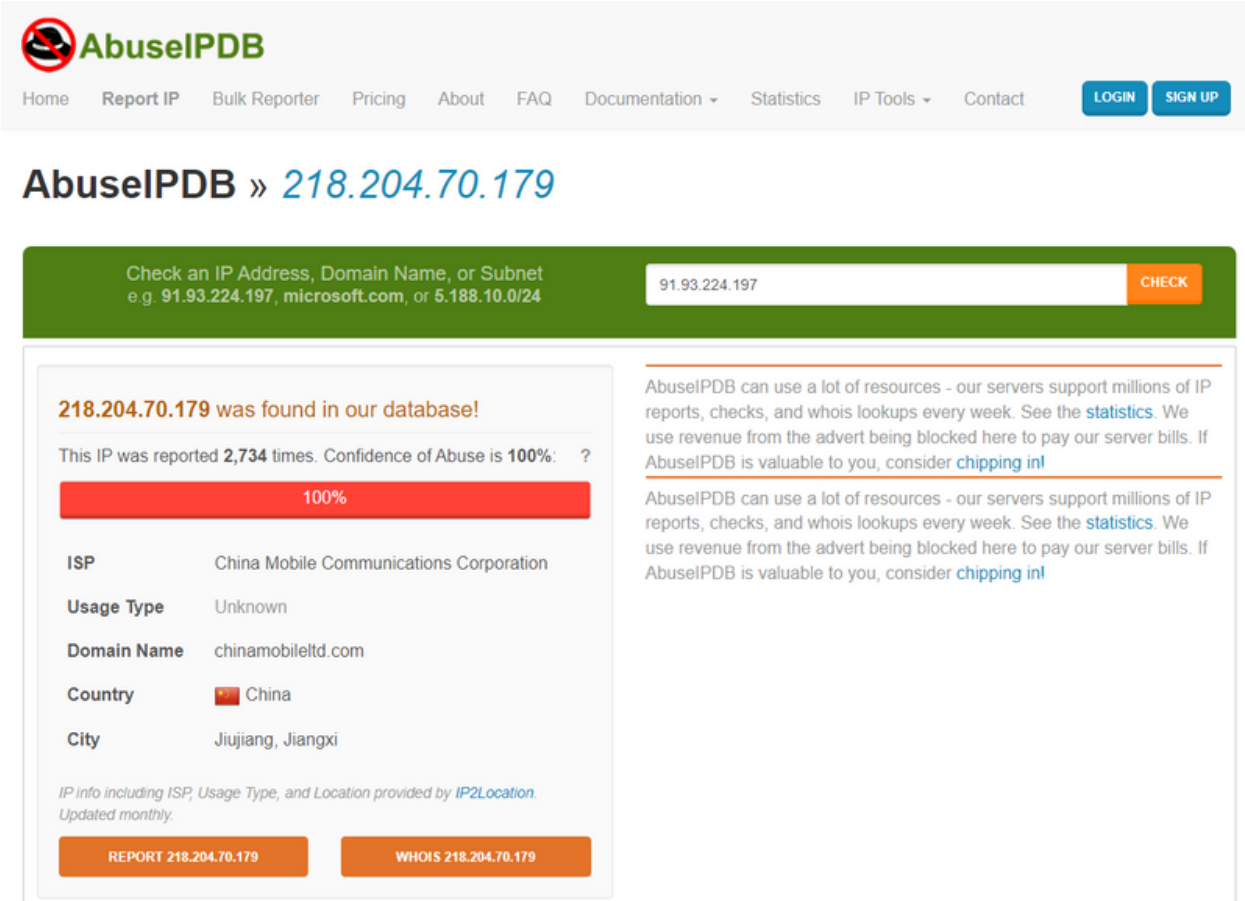
You can both IP and hash search on VT database. and find relationships about suspicious IP/files



Checking Reputation

Abuse IPDb

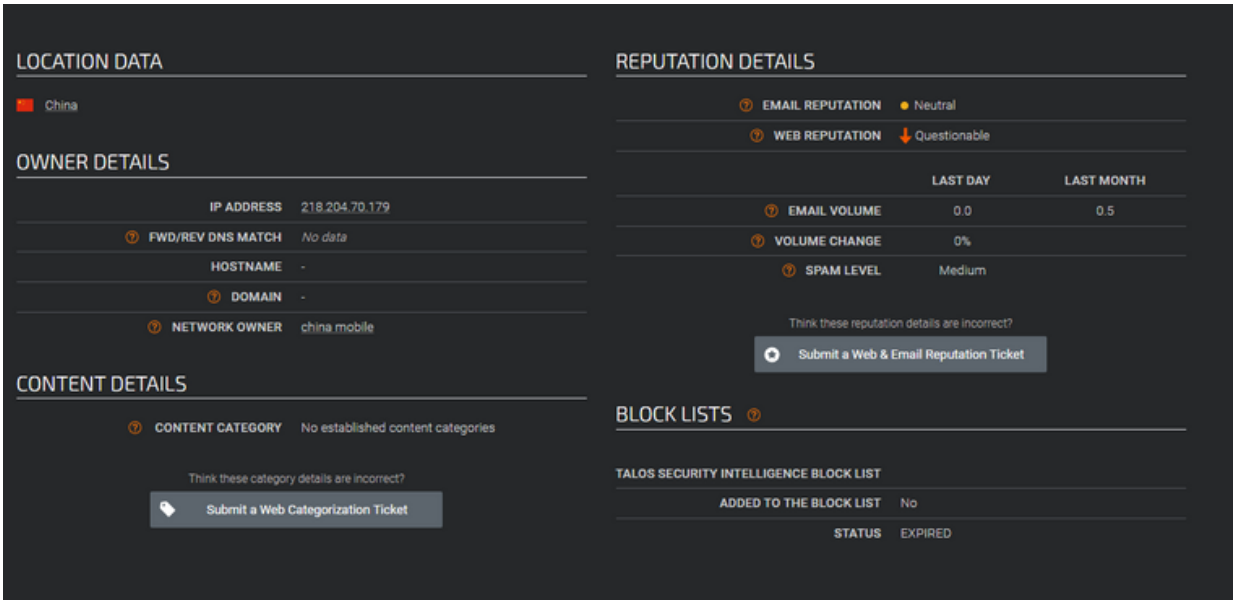
You can check if the IP address has been reported before. Let's say you found a suspicious IP address on your firewall logs and want to ensure is IP address did something bad before.



Checking Reputation

Cisco Talos

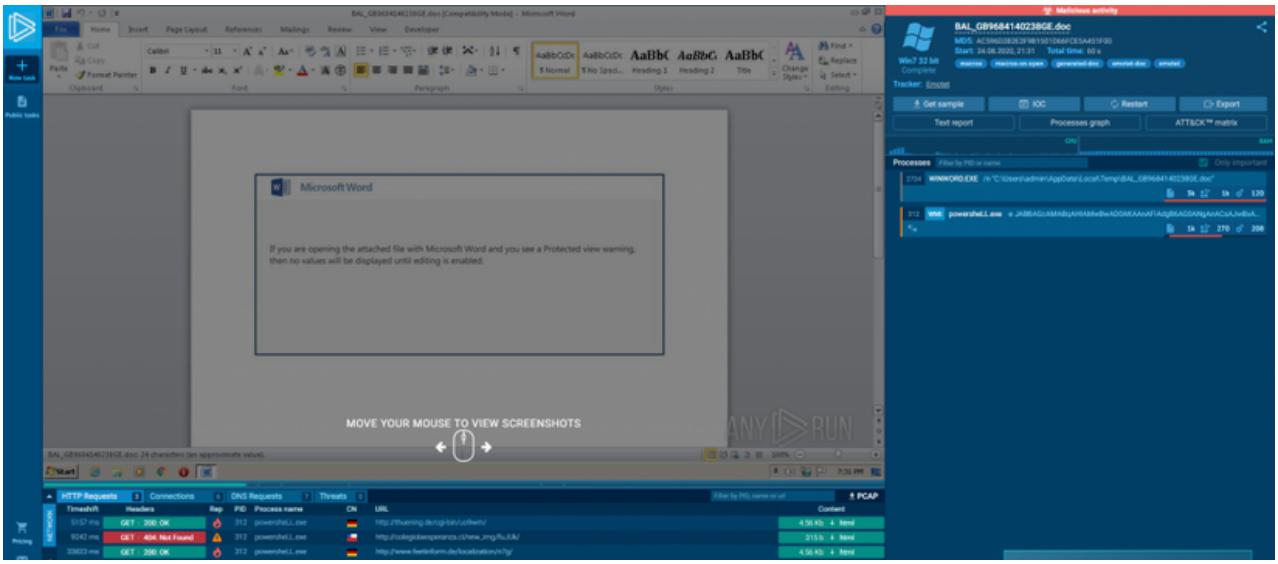
You can search by IP, domain, or network owner for real-time threat data.



Online Sandbox

AnyRun

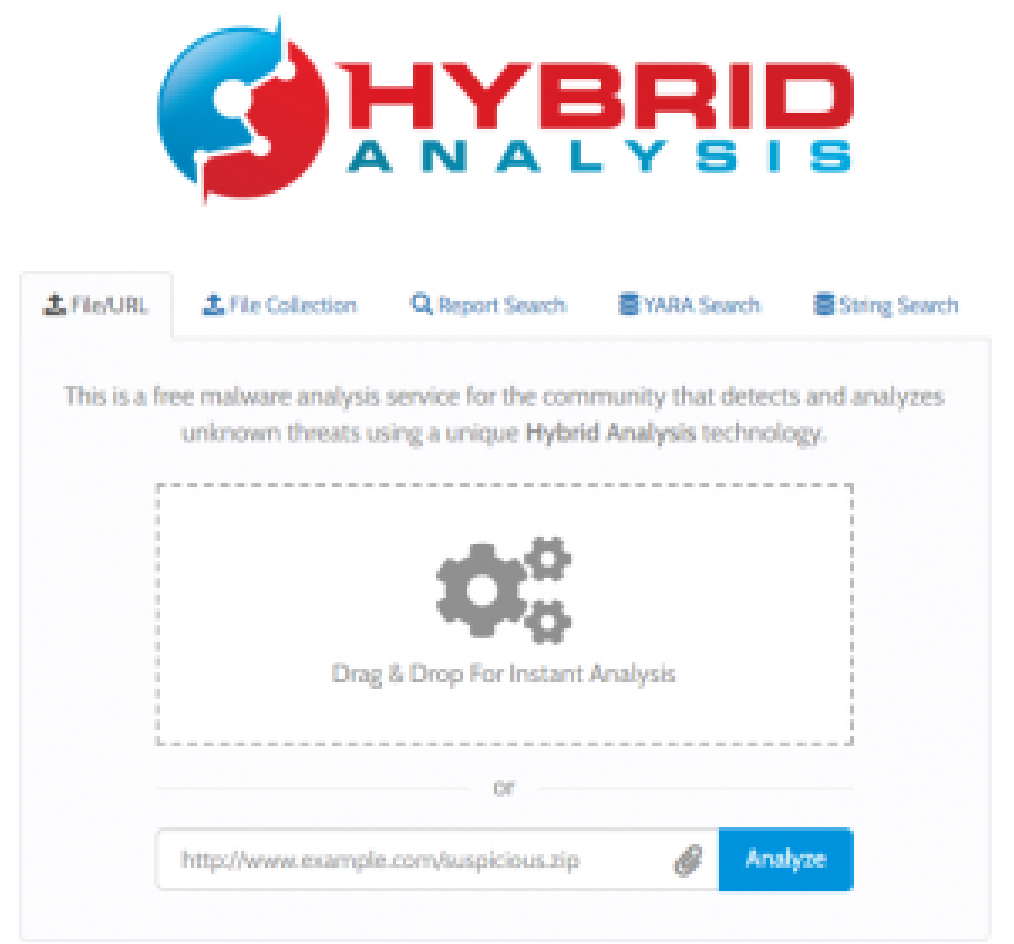
This is an interactive malware analysis platform. Very useful for finding command and control addresses of malware and understanding the purpose. You can use it with the free version.



Online Sandbox

Hybrid-Analysis

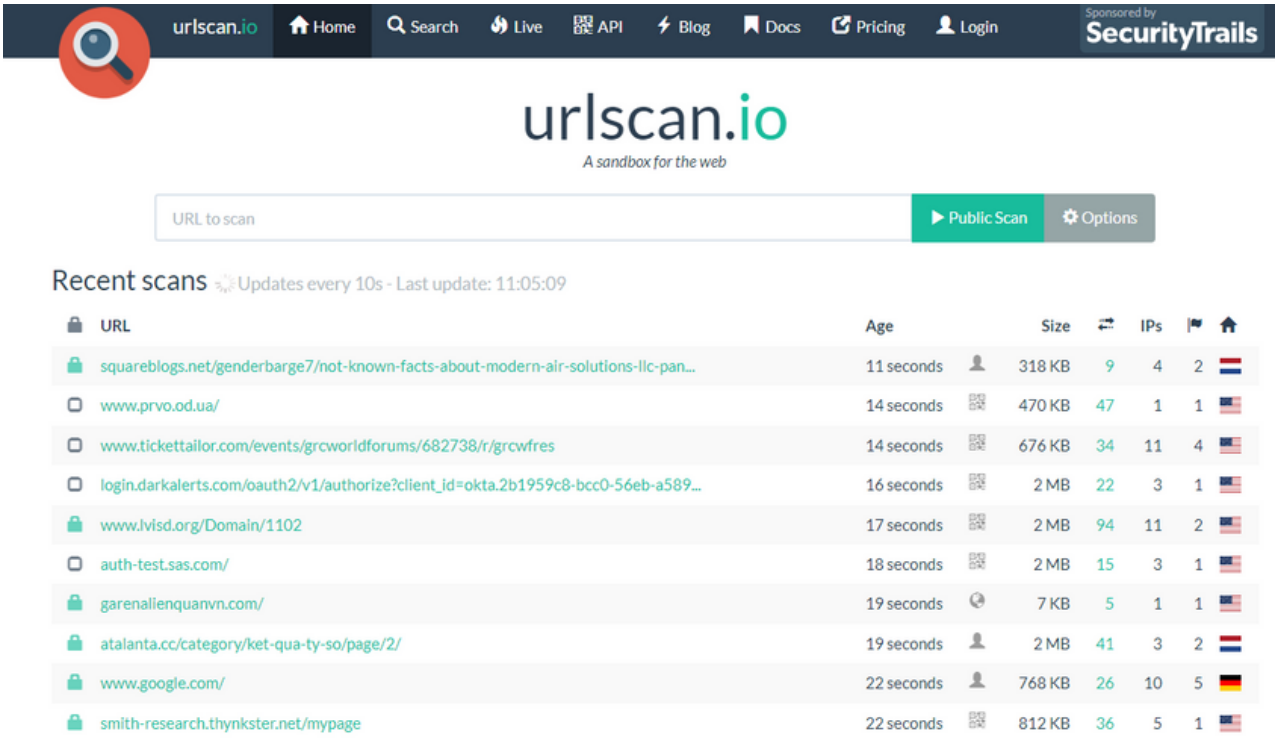
It provides an analysis report with Falcon Sandbox and Hybrid Analysis technology.



Online Sandbox

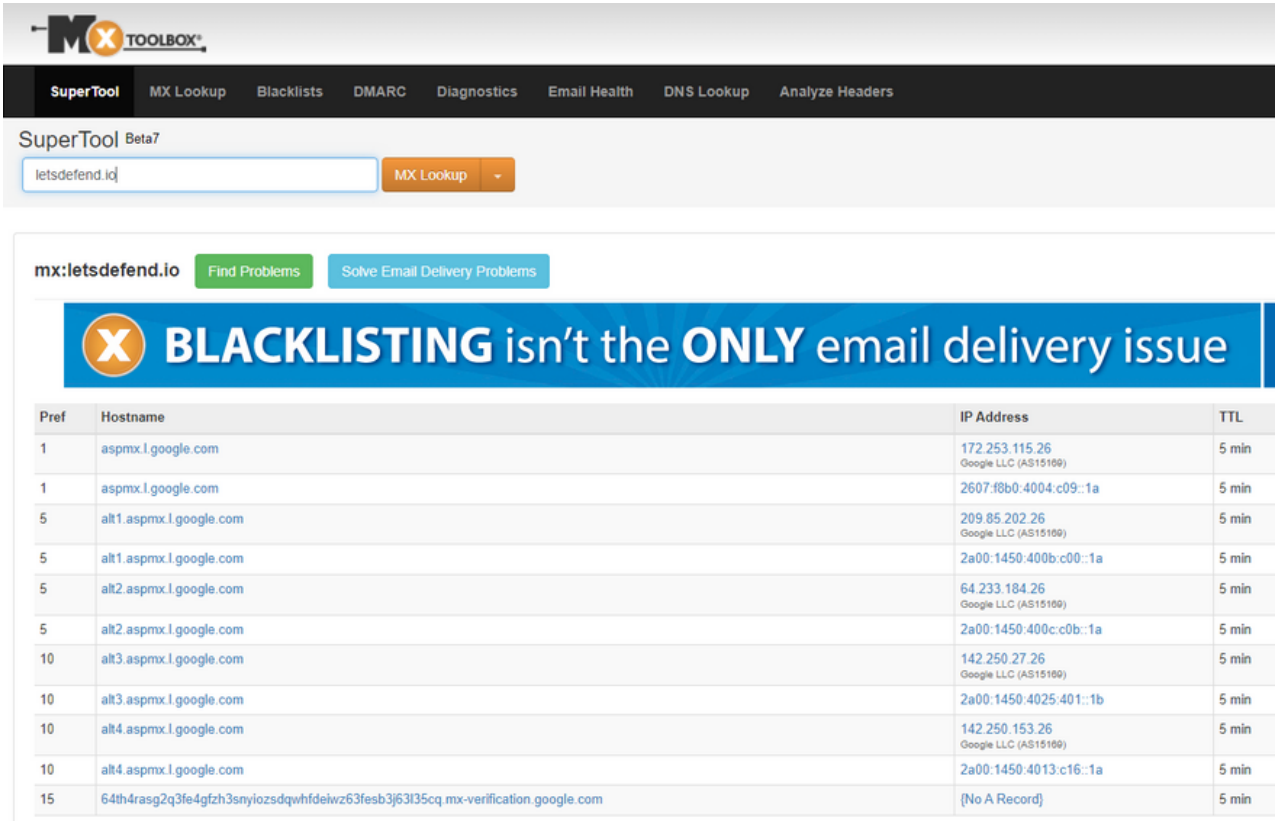
urlscan

If you specifically want to scan URL addresses, it's useful tool for you.



MXToolBox

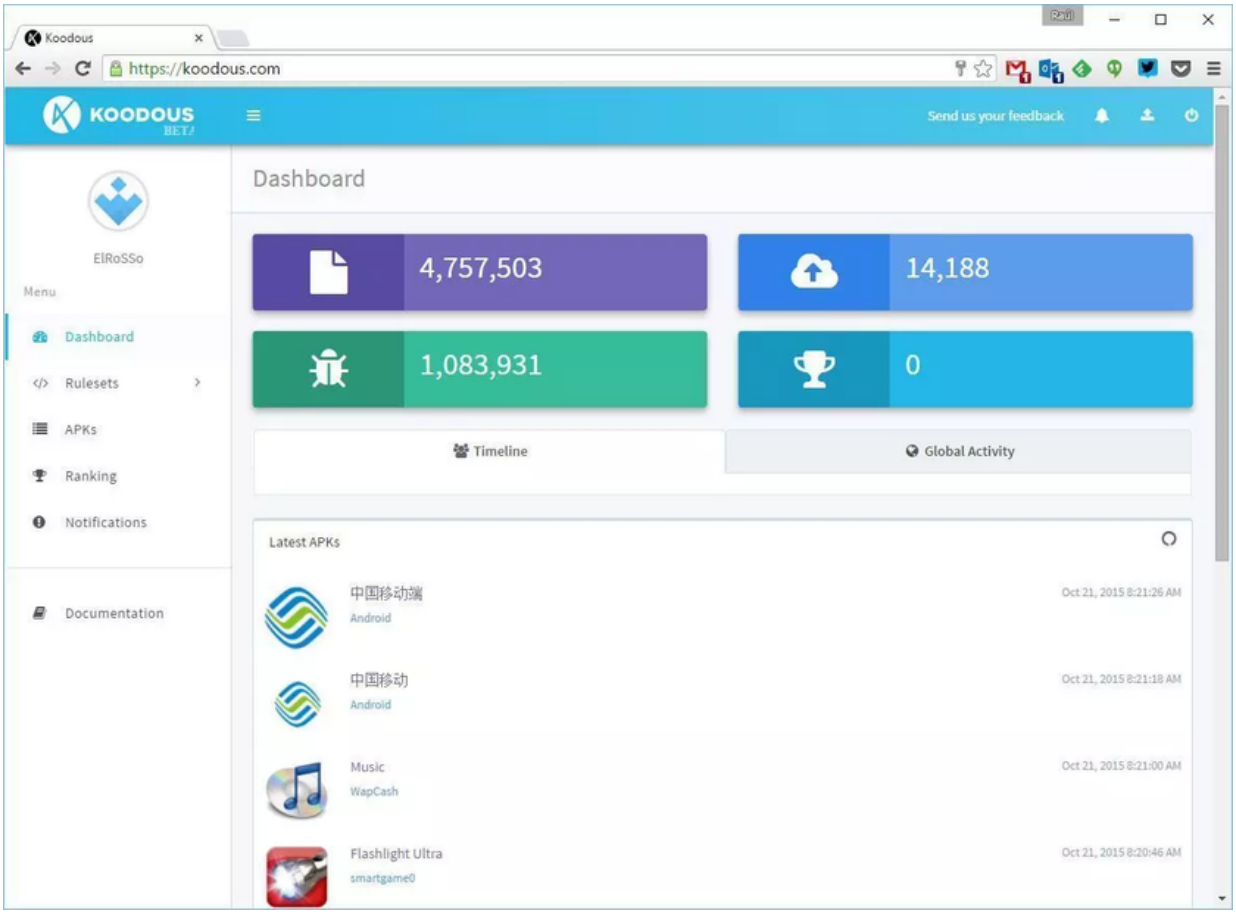
During the phishing campaign analysis, it would be helpful for spoofing analysis. You can compare the SMTP addresses.



Pref	Hostname	IP Address	TTL
1	aspmx.l.google.com	172.253.115.26 Google LLC (AS15169)	5 min
1	aspmx.l.google.com	2607:f8b0:4004:c09::1a	5 min
5	alt1.aspmx.l.google.com	209.85.202.26 Google LLC (AS15169)	5 min
5	alt1.aspmx.l.google.com	2a00:1450:400b:c00::1a	5 min
5	alt2.aspmx.l.google.com	64.233.184.26 Google LLC (AS15169)	5 min
5	alt2.aspmx.l.google.com	2a00:1450:400c:c0b::1a	5 min
10	alt3.aspmx.l.google.com	142.250.27.26 Google LLC (AS15169)	5 min
10	alt3.aspmx.l.google.com	2a00:1450:4025:401::1b	5 min
10	alt4.aspmx.l.google.com	142.250.153.26 Google LLC (AS15169)	5 min
10	alt4.aspmx.l.google.com	2a00:1450:4013:c16::1a	5 min
15	64th4rasg2q3fe4gfzh3snyiozsdqwhfdeiwz63fesb3j63l35cq.mx-verification.google.com	{No A Record}	5 min

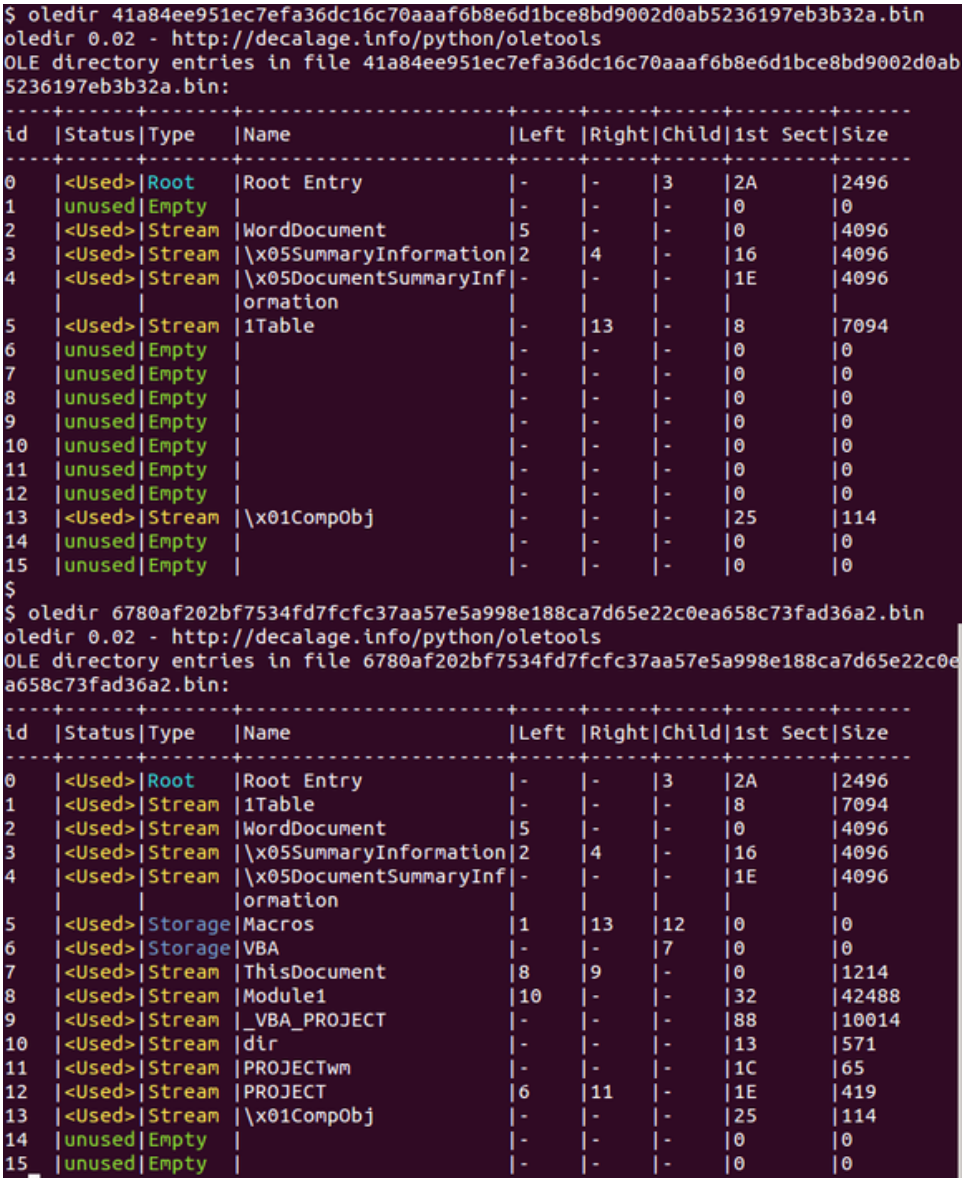
Koodous

Provides malicious APK data



python-oletools

It helps to analyze the Microsoft OLE2 files (Office documents, Outlook messages, etc.)



```
$ oledir 41a84ee951ec7efa36dc16c70aaaf6b8e6d1bce8bd9002d0ab5236197eb3b32a.bin
oledir 0.02 - http://decalage.info/python/oletools
OLE directory entries in file 41a84ee951ec7efa36dc16c70aaaf6b8e6d1bce8bd9002d0ab
5236197eb3b32a.bin:
----+------+-------+---------------------+-----+-----+-----+--------+------
id  |Status|Type   |Name                 |Left |Right|Child|1st Sect|Size
----+------+-------+---------------------+-----+-----+-----+--------+------
0   |<Used>|Root   |Root Entry           |-    |-    |3    |2A      |2496
1   |unused|Empty  |                     |-    |-    |-    |0       |0
2   |<Used>|Stream |WordDocument         |5    |-    |-    |0       |4096
3   |<Used>|Stream |\x05SummaryInformation|2    |4    |-    |16      |4096
4   |<Used>|Stream |\x05DocumentSummaryInf|-    |-    |-    |1E      |4096
    |      |       |ormation             |     |     |     |        |
5   |<Used>|Stream |1Table               |-    |13   |-    |8       |7094
6   |unused|Empty  |                     |-    |-    |-    |0       |0
7   |unused|Empty  |                     |-    |-    |-    |0       |0
8   |unused|Empty  |                     |-    |-    |-    |0       |0
9   |unused|Empty  |                     |-    |-    |-    |0       |0
10  |unused|Empty  |                     |-    |-    |-    |0       |0
11  |unused|Empty  |                     |-    |-    |-    |0       |0
12  |unused|Empty  |                     |-    |-    |-    |0       |0
13  |<Used>|Stream |\x01CompObj          |-    |-    |-    |25      |114
14  |unused|Empty  |                     |-    |-    |-    |0       |0
15  |unused|Empty  |                     |-    |-    |-    |0       |0
$
$ oledir 6780af202bf7534fd7fcfc37aa57e5a998e188ca7d65e22c0ea658c73fad36a2.bin
oledir 0.02 - http://decalage.info/python/oletools
OLE directory entries in file 6780af202bf7534fd7fcfc37aa57e5a998e188ca7d65e22c0e
a658c73fad36a2.bin:
----+------+-------+---------------------+-----+-----+-----+--------+------
id  |Status|Type   |Name                 |Left |Right|Child|1st Sect|Size
----+------+-------+---------------------+-----+-----+-----+--------+------
0   |<Used>|Root   |Root Entry           |-    |-    |3    |2A      |2496
1   |<Used>|Stream |1Table               |-    |-    |-    |8       |7094
2   |<Used>|Stream |WordDocument         |5    |-    |-    |0       |4096
3   |<Used>|Stream |\x05SummaryInformation|2    |4    |-    |16      |4096
4   |<Used>|Stream |\x05DocumentSummaryInf|-    |-    |-    |1E      |4096
    |      |       |ormation             |     |     |     |        |
5   |<Used>|Storage|Macros               |1    |13   |12   |0       |0
6   |<Used>|Storage|VBA                  |-    |-    |7    |0       |0
7   |<Used>|Stream |ThisDocument         |8    |9    |-    |0       |1214
8   |<Used>|Stream |Module1              |10   |-    |-    |32      |42488
9   |<Used>|Stream |_VBA_PROJECT         |-    |-    |-    |88      |10014
10  |<Used>|Stream |dir                  |-    |-    |-    |13      |571
11  |<Used>|Stream |PROJECTwm            |-    |-    |-    |1C      |65
12  |<Used>|Stream |PROJECT              |6    |11   |-    |1E      |419
13  |<Used>|Stream |\x01CompObj          |-    |-    |-    |25      |114
14  |unused|Empty  |                     |-    |-    |-    |0       |0
15  |unused|Empty  |                     |-    |-    |-    |0       |0
```