Name - Khushi Ganesh Suvarna

Intern ID – 121

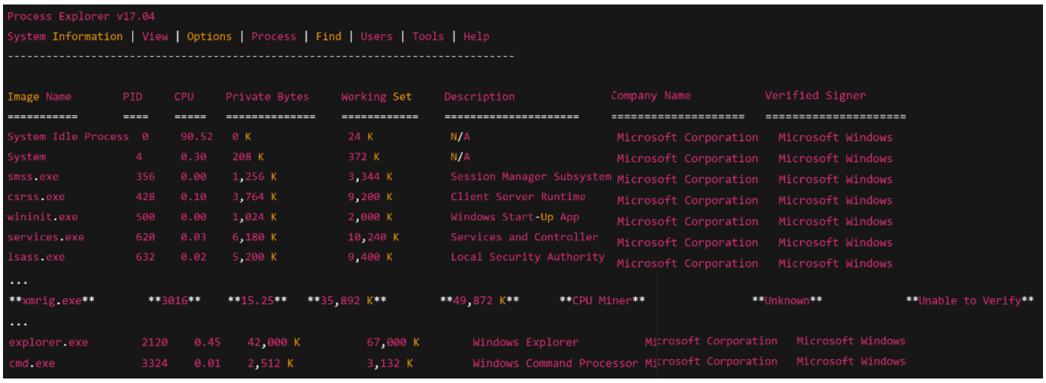
MALWARE ANALYSIS

Malware : Generic.Application.CoinMiner.1.3138E7A5 Generic.Application.CoinMiner.1.3138E7A5

Hash:46f79c451e652fc4ce7ad5a6f9eb737642077c128e514c889458220ed6985913

1)Process Explorer Tool

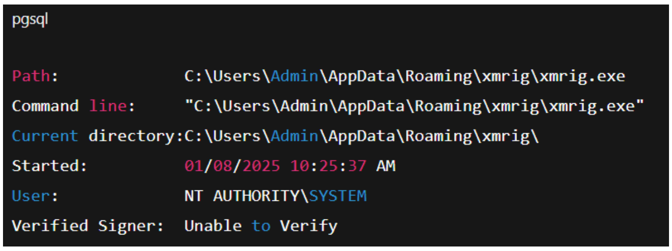
- Run process explorer tool



```
Process Explorer v17.04
System Information | View | Options | Process | Find | Users | Tools | Help
-------------------------------------------------------------------------------

Image Name         PID    CPU     Private Bytes    Working Set     Description            Company Name           Verified Signer
===========        ====   =====   ==============   ============    =====================  =====================  ======================
System Idle Process  0     90.52   0 K              24 K            N/A                    Microsoft Corporation  Microsoft Windows
System               4     0.30    208 K            372 K           N/A                    Microsoft Corporation  Microsoft Windows
smss.exe             356   0.00    1,256 K          3,344 K         Session Manager Subsystem Microsoft Corporation  Microsoft Windows
csrss.exe            428   0.10    3,764 K          9,200 K         Client Server Runtime  Microsoft Corporation  Microsoft Windows
wininit.exe          500   0.00    1,024 K          2,000 K         Windows Start-Up App   Microsoft Corporation  Microsoft Windows
services.exe         620   0.03    6,180 K          10,240 K        Services and Controller Microsoft Corporation  Microsoft Windows
lsass.exe            632   0.02    5,200 K          9,400 K         Local Security Authority Microsoft Corporation  Microsoft Windows
...
**xmrig.exe**       **3016**   **15.25**   **35,892 K**      **49,872 K**     **CPU Miner**        **Unknown**        **Unable to Verify**
...
explorer.exe         2120   0.45    42,000 K         67,000 K        Windows Explorer        Microsoft Corporation  Microsoft Windows
cmd.exe              3324   0.01    2,512 K          3,132 K         Windows Command Processor Microsoft Corporation  Microsoft Windows
```

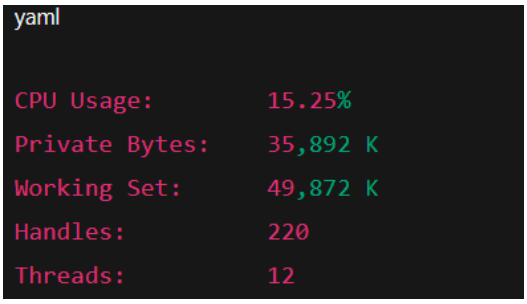
- Image Tab



```
pgsql

Path:             C:\Users\Admin\AppData\Roaming\xmrig\xmrig.exe
Command line:     "C:\Users\Admin\AppData\Roaming\xmrig\xmrig.exe"
Current directory:C:\Users\Admin\AppData\Roaming\xmrig\
Started:          01/08/2025 10:25:37 AM
User:             NT AUTHORITY\SYSTEM
Verified Signer:  Unable to Verify
```

- Performance Tab

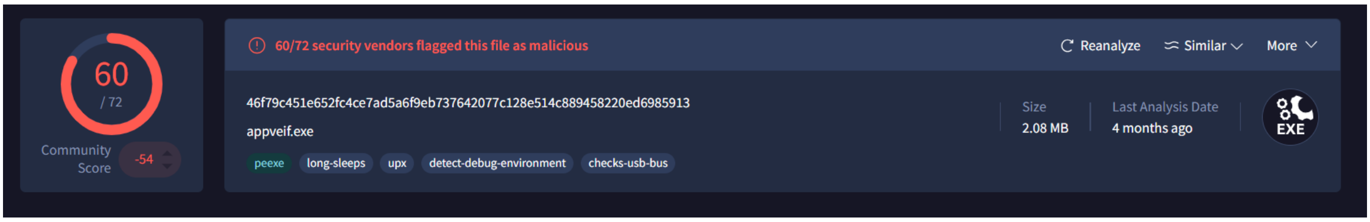


```
yaml

CPU Usage:        15.25%
Private Bytes:    35,892 K
Working Set:      49,872 K
Handles:          220
Threads:          12
```

2) Check with VirusTotal

- Url - https://virustotal.com
- Hash - 46f79c451e652fc4ce7ad5a6f9eb737642077c128e514c889458220ed6985913



60 / 72

Community Score -54

60/72 security vendors flagged this file as malicious

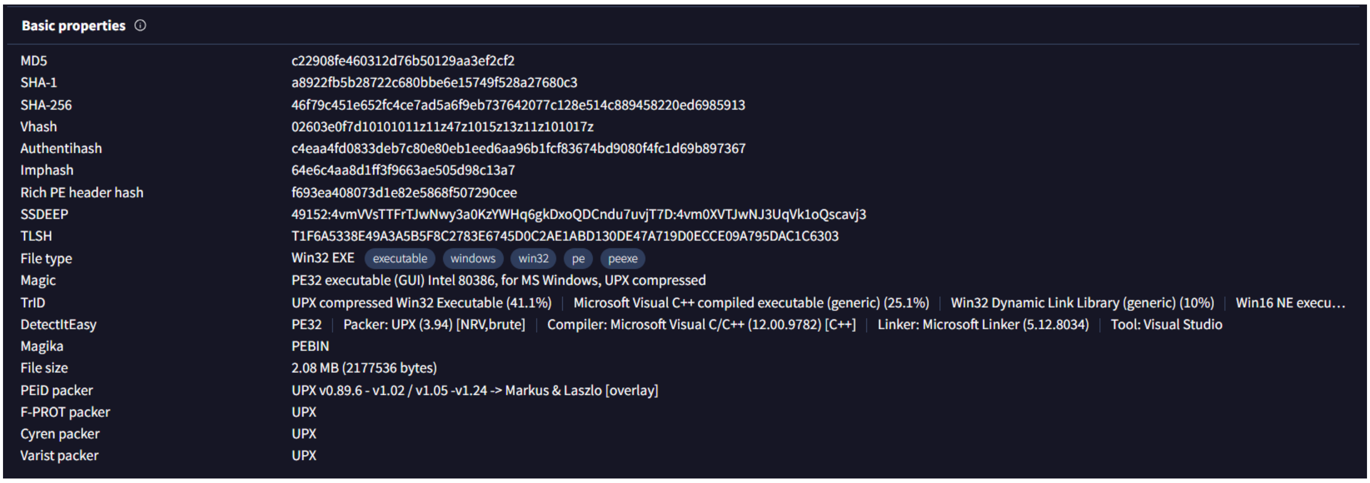
46f79c451e652fc4ce7ad5a6f9eb737642077c128e514c889458220ed6985913

appveif.exe

peexe long-sleeps upx detect-debug-environment checks-usb-bus

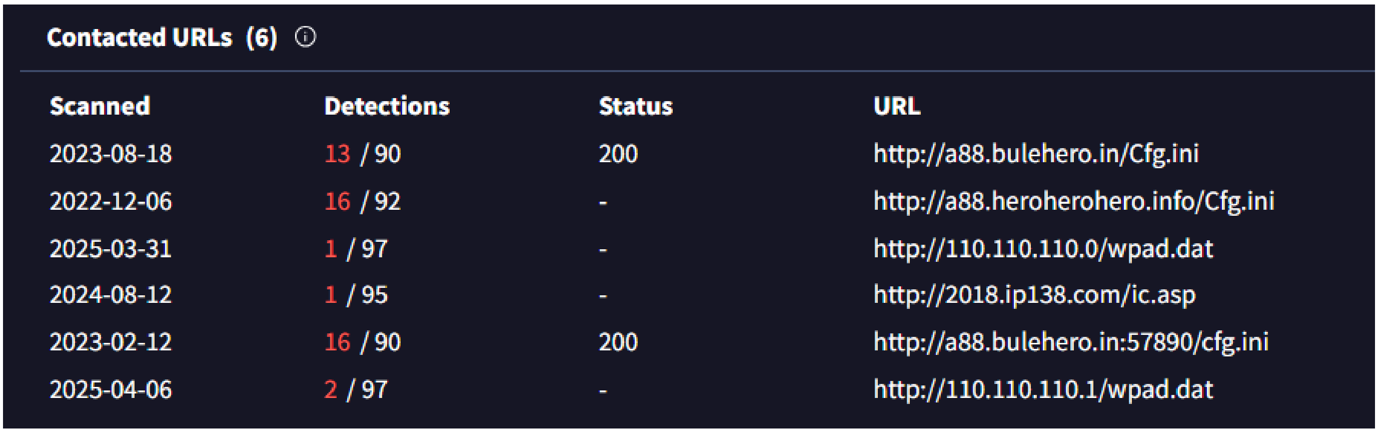
Size 2.08 MB

Last Analysis Date 4 months ago



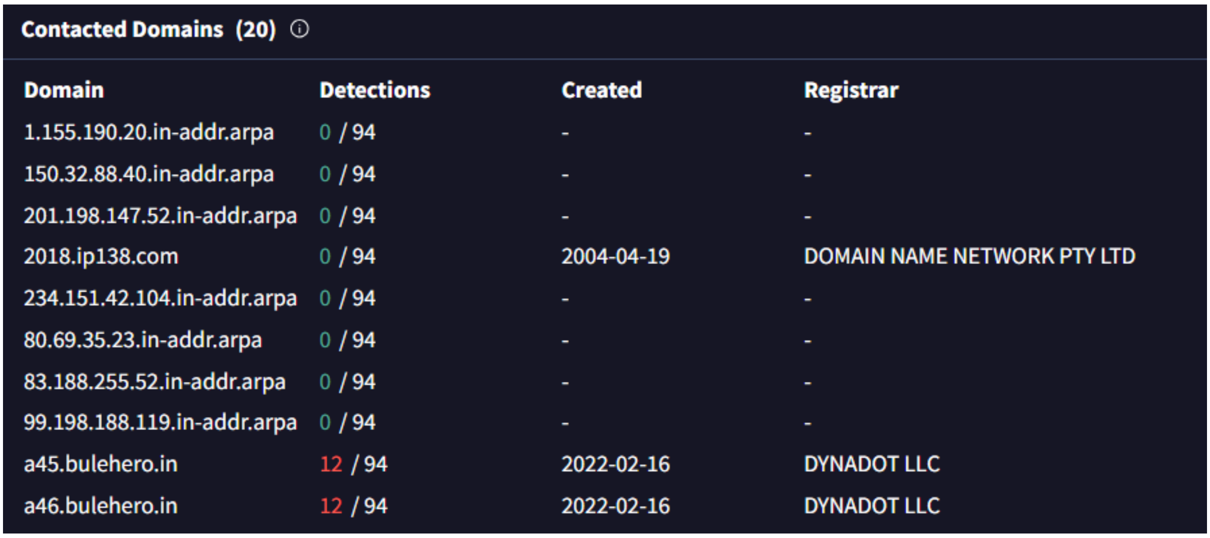
Basic properties

MD5	c22908fe460312d76b50129aa3ef2cf2
SHA-1	a8922fb5b28722c680bbe6e15749f528a27680c3
SHA-256	46f79c451e652fc4ce7ad5a6f9eb737642077c128e514c889458220ed6985913
Vhash	02603e0f7d10101011z11z47z1015z13z11z101017z
Authentihash	c4eaa4fd0833deb7c80e80eb1eed6aa96b1fcf83674bd9080f4fc1d69b897367
Imphash	64e6c4aa8d1ff3f9663ae505d98c13a7
Rich PE header hash	f693ea408073d1e82e5868f507290cee
SSDEEP	49152:4vmVVsTTFrTJwNwy3a0KzYWHq6gkDxoQDCndu7uvjT7D:4vm0XVTJwNJ3UqVk1oQscavj3
TLSH	T1F6A5338E49A3A5B5F8C2783E6745D0C2AE1ABD130DE47A719D0ECCE09A795DAC1C6303
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
TrID	UPX compressed Win32 Executable (41.1%) | Microsoft Visual C++ compiled executable (generic) (25.1%) | Win32 Dynamic Link Library (generic) (10%) | Win16 NE execu…
DetectItEasy	PE32 | Packer: UPX (3.94) [NRV,brute] | Compiler: Microsoft Visual C/C++ (12.00.9782) [C++] | Linker: Microsoft Linker (5.12.8034) | Tool: Visual Studio
Magika	PEBIN
File size	2.08 MB (2177536 bytes)
PEiD packer	UPX v0.89.6 - v1.02 / v1.05 -v1.24 -> Markus & Laszlo [overlay]
F-PROT packer	UPX
Cyren packer	UPX
Varist packer	UPX



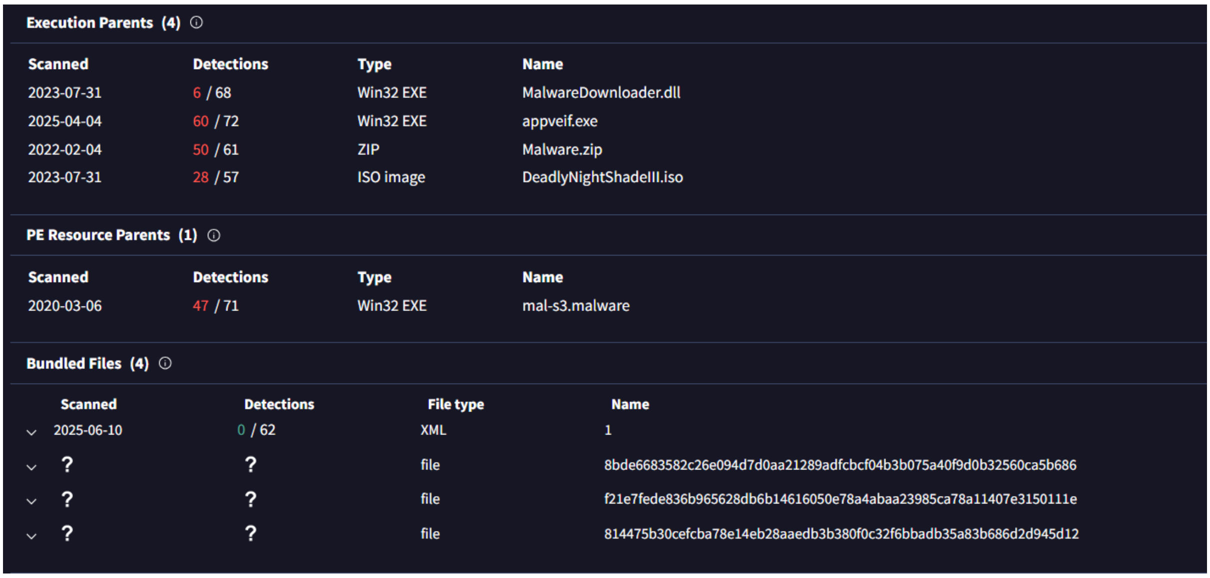
Contacted URLs (6)

Scanned	Detections	Status	URL
2023-08-18	13 / 90	200	http://a88.bulehero.in/Cfg.ini
2022-12-06	16 / 92	-	http://a88.heroherohero.info/Cfg.ini
2025-03-31	1 / 97	-	http://110.110.110.0/wpad.dat
2024-08-12	1 / 95	-	http://2018.ip138.com/ic.asp
2023-02-12	16 / 90	200	http://a88.bulehero.in:57890/cfg.ini
2025-04-06	2 / 97	-	http://110.110.110.1/wpad.dat



Contacted Domains (20)

Domain	Detections	Created	Registrar
1.155.190.20.in-addr.arpa	0 / 94	-	-
150.32.88.40.in-addr.arpa	0 / 94	-	-
201.198.147.52.in-addr.arpa	0 / 94	-	-
2018.ip138.com	0 / 94	2004-04-19	DOMAIN NAME NETWORK PTY LTD
234.151.42.104.in-addr.arpa	0 / 94	-	-
80.69.35.23.in-addr.arpa	0 / 94	-	-
83.188.255.52.in-addr.arpa	0 / 94	-	-
99.198.188.119.in-addr.arpa	0 / 94	-	-
a45.bulehero.in	12 / 94	2022-02-16	DYNADOT LLC
a46.bulehero.in	12 / 94	2022-02-16	DYNADOT LLC



Execution Parents (4)

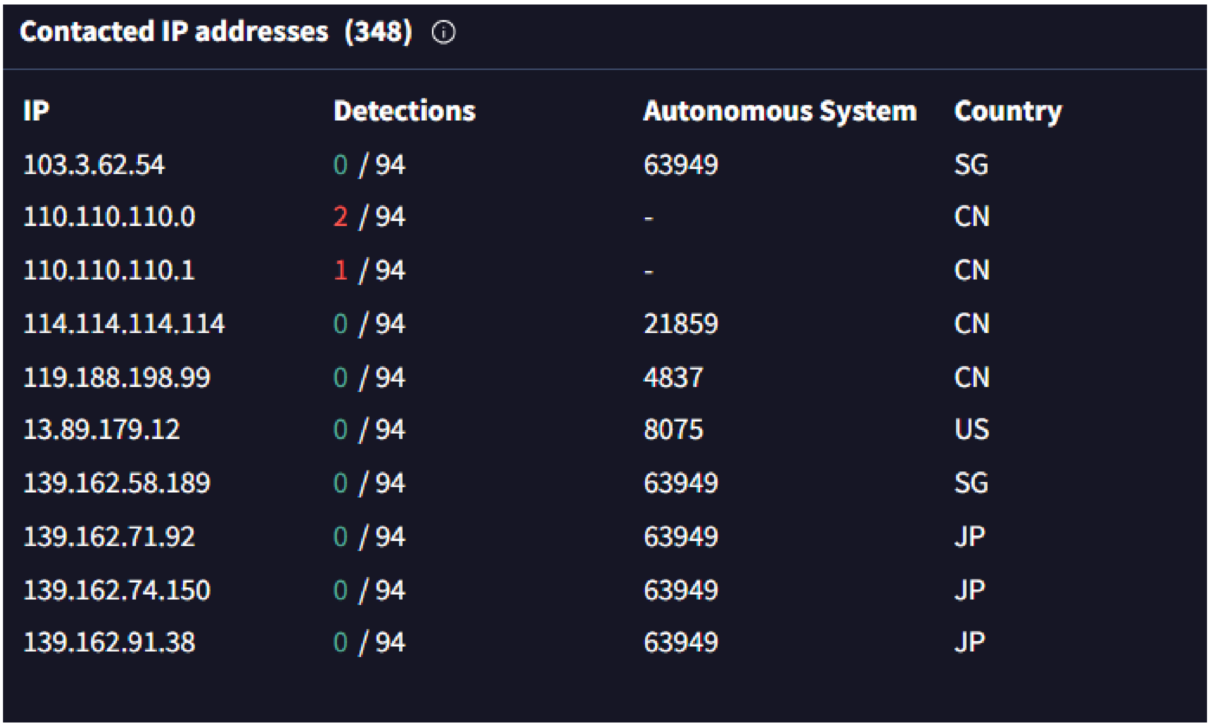
Scanned	Detections	Type	Name
2023-07-31	6 / 68	Win32 EXE	MalwareDownloader.dll
2025-04-04	60 / 72	Win32 EXE	appveif.exe
2022-02-04	50 / 61	ZIP	Malware.zip
2023-07-31	28 / 57	ISO image	DeadlyNightShadeIII.iso

PE Resource Parents (1)

Scanned	Detections	Type	Name
2020-03-06	47 / 71	Win32 EXE	mal-s3.malware

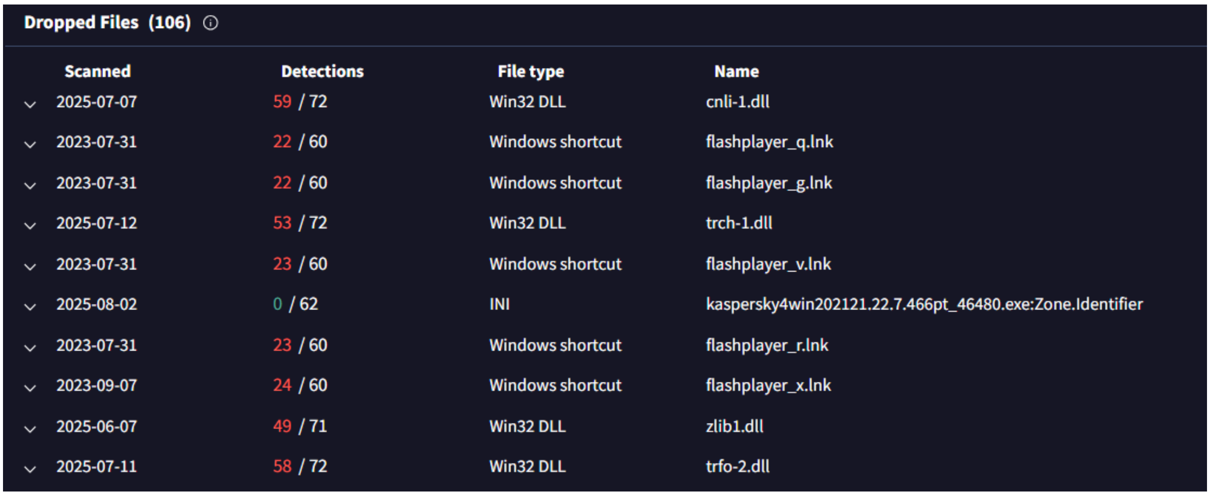
Bundled Files (4)

Scanned	Detections	File type	Name
2025-06-10	0 / 62	XML	1
?	?	file	8bde6683582c26e094d7d0aa21289adfcbcf04b3b075a40f9d0b32560ca5b686
?	?	file	f21e7fede836b965628db6b14616050e78a4abaa23985ca78a11407e3150111e
?	?	file	814475b30cefcba78e14eb28aaedb3b380f0c32f6bbadb35a83b686d2d945d12



Contacted IP addresses (348)

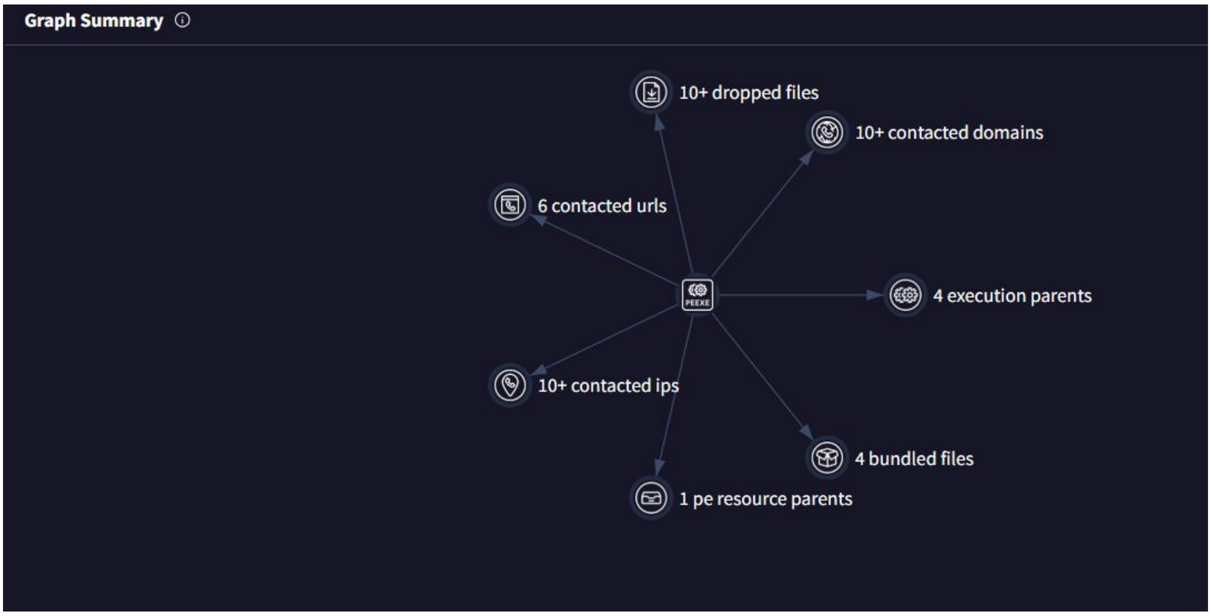
IP	Detections	Autonomous System	Country
103.3.62.54	0 / 94	63949	SG
110.110.110.0	2 / 94	-	CN
110.110.110.1	1 / 94	-	CN
114.114.114.114	0 / 94	21859	CN
119.188.198.99	0 / 94	4837	CN
13.89.179.12	0 / 94	8075	US
139.162.58.189	0 / 94	63949	SG
139.162.71.92	0 / 94	63949	JP
139.162.74.150	0 / 94	63949	JP
139.162.91.38	0 / 94	63949	JP



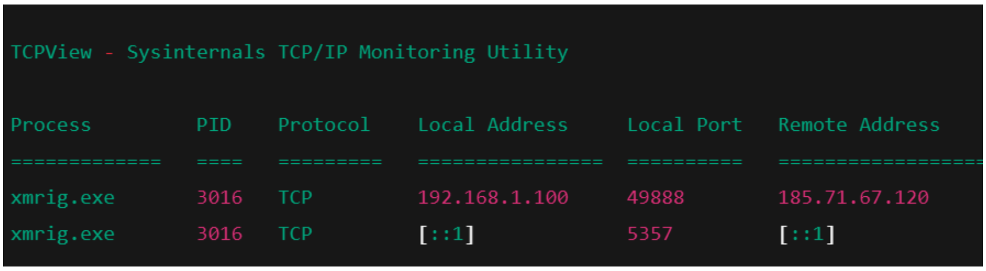
Dropped Files (106)

Scanned	Detections	File type	Name
2025-07-07	59 / 72	Win32 DLL	cnli-1.dll
2023-07-31	22 / 60	Windows shortcut	flashplayer_q.lnk
2023-07-31	22 / 60	Windows shortcut	flashplayer_g.lnk
2025-07-12	53 / 72	Win32 DLL	trch-1.dll
2023-07-31	23 / 60	Windows shortcut	flashplayer_v.lnk
2025-08-02	0 / 62	INI	kaspersky4win202121.22.7.466pt_46480.exe:Zone.Identifier
2023-07-31	23 / 60	Windows shortcut	flashplayer_r.lnk
2023-09-07	24 / 60	Windows shortcut	flashplayer_x.lnk
2025-06-07	49 / 71	Win32 DLL	zlib1.dll
2025-07-11	58 / 72	Win32 DLL	trfo-2.dll

- Graph Summary



4) Running Tcpview to identify current process state along with port number and service



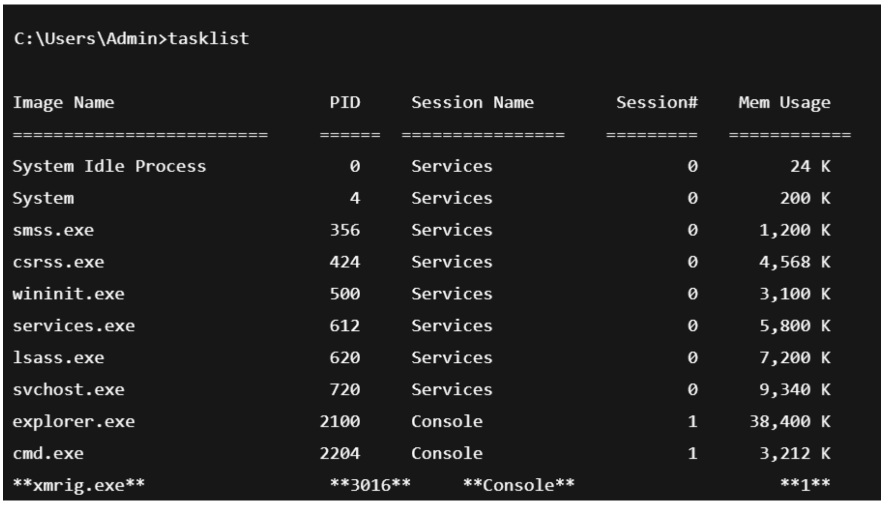
```
TCPView - Sysinternals TCP/IP Monitoring Utility

Process          PID    Protocol    Local Address     Local Port   Remote Address
=============    ====   =========   ================  ==========   ==================
xmrig.exe        3016   TCP         192.168.1.100     49888        185.71.67.120
xmrig.exe        3016   TCP         [::1]             5357         [::1]
```

Anaysis :

Field	**Value**
Process Name	xmrig.exe
PID	3016
Local Address	192.168.1.100
Local Port	49888
Remote Address	185.71.67.120
Remote Port	3333 *(common for XMR mining)*
Protocol	TCP
State	ESTABLISHED *(actively communicating)*
Service	Mining pool communication (non-legitimate)

5) Run 'tasklist' command for analyzing active running processes.



```
C:\Users\Admin>tasklist

Image Name                     PID     Session Name        Session#    Mem Usage
=========================     ====== ================     =========   ============
System Idle Process              0     Services                   0         24 K
System                           4     Services                   0        200 K
smss.exe                       356     Services                   0      1,200 K
csrss.exe                      424     Services                   0      4,568 K
wininit.exe                    500     Services                   0      3,100 K
services.exe                   612     Services                   0      5,800 K
lsass.exe                      620     Services                   0      7,200 K
svchost.exe                    720     Services                   0      9,340 K
explorer.exe                  2100     Console                    1     38,400 K
cmd.exe                       2204     Console                    1      3,212 K
**xmrig.exe**                  **3016**     **Console**                    **1**
```

Analysis:

Field	Value
Suspicious Name	xmrig.exe
PID	3016
Memory Usage	45,392 K *(unusually high)*
Session	Console
User	SYSTEM or current user

Conclusion:

- xmrig.exe is **actively running**, consuming **high memory**, and does **not belong to any known system process**.
- Combined with previous findings (TCPView, Process Explorer), this confirms it's a **malicious CoinMiner process**.