

+
New analysis

Reports

TI

Pricing

Contacts

FAQ

Sign In

Recycle Bin

Skype

playingmark...

Acrobat Reader DC

VLC media player

rulewaste.jpg

CCleaner

bestll.png

startreqs...

FileZilla Client

commercet...

vedays.tif

Firefox

enbydocum...

zanevaga...

Google Chrome

government...

Opera

locatedr...

MOVE YOUR MOUSE TO VIEW SCREENSHOTS

ANYRUN

Malicious activity

payload.exe

Win7 32 bit Complete

Indicators: Tracker: [Trojan](#)

Get sample

IOC

MalConf

Restart

Text report

Graph

ATT&CK

AI Summary

beta

Export

CPU

RAM

Processes

Filter by PID or name

☒ Only important

3032

payload.exe

PE

260

30

40

3588

Nypezi.exe

PE

114

28

40

4080

cmd.exe

/a /c netsh advfirewall firewall add rule name="Z...

184

32

26

2500

netsh.exe

advfirewall firewall add rule name="Z0BAZ...

1k

1k

252

1544

nypezi.exe

PE

neutrino

336

358

100

3884

cmd.exe

/a /c ping 127.0.0.1 -n 3&del "C:\Users\admin\AppData...

232

32

26

4088

PING.EXE

127.0.0.1 -n 3

112

282

40

| | HTTP Requests | Connections | DNS Requests | Threats | Filter by PID, name or url | | | PCAP |
|---------|---------------|-----------------------|--------------|---------|----------------------------|----|--------------------------------------|---------|
| NETWORK | Timeshift | Headers | Rep | PID | Process name | CN | URL | Content |
| | 11224 ms | POST 404: Not Found | ? | 1544 | nypezi.exe | | http://3.124.104.244:58755/tasks.php | 7 |
| | 12203 ms | POST 404: Not Found | ? | 1544 | nypezi.exe | | http://3.124.104.244:58755/tasks.php | 18 |
| FILES | 41950 ms | POST 404: Not Found | ? | 1544 | nypezi.exe | | http://3.124.104.244:58755/tasks.php | 18 |
| DEBUG | | | | | | | | |

Info

[1544] nypezi.exe [YARA] Firewall manipulation strings were found

Try community version for free!

Register now

Page 1 of 1