

+
New analysis

Reports

TI

Recycle Bin

Acrobat Reader DC

gotwhole.rtf

Firefox

FileZilla Client

hadpost.png

Google Chrome

abstractch.rtf

modeldb.rtf...

Opera

addadmaie...

plant.rtf...

Skype

chidara.png

sewerh.png

CCleaner

georgafan...

twelve.rtf

VLC media player

ground.jpg

riverin.jpg

ANY.RUN

MOVE YOUR MOUSE TO VIEW SCREENSHOTS

Start

5:37 PM

Malicious activity

111.exe

Win7 32 bit Complete

Indicators:

Get sample

IOC

MalConf

Restart

Text report

Graph

ATT&CK

AI Summary

beta

Export

CPU

RAM

Processes

Filter by PID or name

Only important

1656 111.exe PE

3036 server.exe PE

3524 netsh.exe firewall add allowedprogram "C:\Users\admin\...

1252 netsh.exe firewall delete allowedprogram "C:\Users\adm...

2576 netsh.exe firewall add allowedprogram "C:\Users\admin\...

4072 svchost.exe PE

4020 server.exe PE

2556 netsh.exe firewall add allowedprogram "C:\User...

3480 netsh.exe firewall delete allowedprogram "C:\Us...

2932 netsh.exe firewall add allowedprogram "C:\User...

2668 svchost.exe PE

3084 server.exe PE

3048 netsh.exe firewall add allowedprogram ...

3604 netsh.exe firewall delete allowedprogra...

3584 netsh.exe firewall add allowedprogram ...

836 svchost.exe PE

1252 server.exe PE

2124 netsh.exe firewall add allowedpr...

812 netsh.exe firewall delete allowed...

HTTP Requests 0

Connections 0

DNS Requests 0

Threats 0

Filter by PID, name or url

PCAP

NETWORK

FILES

DEBUG

Timeshift

Headers

Rep

PID

Process name

CN

URL

Content

No data

Shopping cart

Pricing

Envelope

Contacts

Question mark

FAQ

Cursor

Sign In

Info

[4076] netsh.exe Reads the computer name

Try community version for free!

Register now