

New analysis

Reports

TI

MOVE YOUR MOUSE TO VIEW SCREENSHOTS

Local Disk (C:)

OrganizeShare withNew folder

MSOCache

7/14/2009 3:37 AM

File folder

PerLogs

9/27/2019 3:14 AM

File folder

Program Files

3/19/2019 1:03 PM

File folder

ProgramData

10/5/2017 10:49 AM

File folder

Users

3/19/2019 1:05 PM

File folder

Windows

9/27/2019 3:13 AM

CAES File

1 KB

autoexec.bat.id[C4BA3647-2412].[recovery...

9/27/2019 3:13 AM

CAES File

1 KB

config.sys.id[C4BA3647-2412].[recoveryfas...

9/27/2019 3:13 AM

CAES File

1 KB

8 items

Start

3:14 AM

Shopping cart

Pricing

Envelope

Contacts

Help

FAQ

Sign In

HTTP Requests0Connections0DNS Requests0Threats0

Filter by PID, name or url

PCAP

NETWORK

FILES

DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
No data							

Info

[2732] explorer.exe

Manual execution by user

Malicious activity

svchost.exe

MD5: 1605DC744FE86B41F44C69A13AA092E9

Start: 27.09.2019, 04:13Total time: 60 s

ransomware

Indicators:

Tracker: Ransomware

Get sample

IOC

MalConf

Restart

Text report

Graph

ATT&CK

Summary

Export

CPU

RAM

Processes

Filter by PID or name

Only important

2948 svchost.exe PE

481539

3584 svchost.exe PE

51333882

2812 svchost.exe PE

159k223

3200 cmd.exe

154626

3852 netsh.exe advfirewall set currentprofile state off

62360252

2712 netsh.exe firewall set opmode mode=disable

54547228

2732 explorer.exe

1842680

Try community version for free!

Register now