

+  
New analysis

Reports

TI

Recycle Bin

Skype

outbase...

Acrobat Reader DC

Microsoft Edge

sellany.jpg

CCleaner

classlabel.jpg

takenlearn.rtf

FileZilla Client

consideradd...

Firefox

damagedrill...

Google Chrome

giveidea.jpg

canquestio...

bdenviradm...

MOVE YOUR MOUSE TO VIEW SCREENSHOTS

←

→

ANY.RUN

It's not a game  
It's a Test Mode  
Windows 7  
Build 7601

Malicious activity

bd07fb1e9b4768e7202de6cc454c78c68...

MD5: 50B5582904FE34451F5CB2362E11CB24

Start: 18.04.2024, 14:34    Total time: 60 s

Win7 32 bit  
Complete

Indicators:

Get sample

IOC

MalConf

Restart

Text report

Graph

ATT&CK

Summary <sup>beta</sup>

Export

CPU

RAM

Processes

Filter by PID or name

Only important

3040

bd07fb1e9b4768e7202de6cc454c78c6891270af02085c51fce5539db...

366

533

57

3768

rundll32.exe "C:\Users\admin\AppData\Local\Microsoft\...

149

43

39

1072

cmd.exe /c REG ADD HKCU\SOFTWARE\Microsoft\Windows\...

109

37

13

2932

reg.exe ADD HKCU\SOFTWARE\Microsoft\Windows\Curr...

47

19

17

1316

cmd.exe /c "C:\Users\admin\AppData\qehe.bat"

159

36

15

Pricing

Contacts

FAQ

Sign In

NETWORK

FILES

DEBUG

HTTP Requests0

Connections4

DNS Requests0

Threats0

Filter by PID, name or url

PCAP

Timeshift

Headers

Rep

PID

Process name

CN

URL

Content

No data

Danger

[2932] reg.exe

Changes the autorun value in the registry

Try community version for free!

Register now

Page 1 of 1