

+  
New analysis

Reports

TI

Recycle Bin

VLC media player

silveryou...  
silveryou...

Mozilla Firefox

µTorrent

transfere...

Opera

FileZilla Client

westernm...  
westernm...

Google Chrome

graderequ...  
graderequ...

Acrobat Reader DC

perfector...  
perfector...

CCleaner

picamplai...

Skype

policecal...

ANY

RUN

Start

7:20 AM

No threats detected

Win7 32 bit  
Complete

Indicators: 

EXE

Get sample

IOC

MalConf

Restart

Text report

Graph

ATT&CK

AI Summary 

beta

Export

CPU

RAM

Processes

Filter by PID or name

☒ Only important

676

0c1ecb743841a12246f273f28312c949e7891a8b10bb59948446a481cc...

EXE

176

0

24

2720

cmd.exe /c wusa.exe C:\Users\admin\AppData\Local\Temp\...

258

37

80

3244

wusa.exe C:\Users\admin\AppData\Local\Temp\cryptba...

4

0

4

1492

wusa.exe C:\Users\admin\AppData\Local\Temp\cryptba...

4

0

4

1388

wusa.exe C:\Users\admin\AppData\Local\Temp\cryptba...

190

0

54

3708

cmd.exe /c uninstall.bat

381

38

78

2212

sysprep.exe C:\Users\admin\AppData\Local\Temp\gupd...

4

0

4

792

sysprep.exe C:\Users\admin\AppData\Local\Temp\gupdat...

4

0

4

1268

sysprep.exe C:\Users\admin\AppData\Local\Temp\gupd...

196

0

58

2924

gupdate.exe 

PE

281

5

112

3516

COM

scrcons.exe -Embedding

562

64

162

Pricing

Contacts

FAQ

Sign In

	HTTP Requests	7	Connections	7	DNS Requests	8	Threats	0	Filter by PID, name or url	PCAP
NETWORK	Timeshift	Headers	Rep	PID	Process name	CN	URL	Content		
	65481 ms	GET   303: See Other	?	3516	scrcons.exe		http://tvmusicclass.tumblr.com/rss			
	66487 ms	GET   500: Int Server ...	?	3516	scrcons.exe		http://carver.blog.com/feed/	19		
FILES	66500 ms	GET   302: Found	?	3516	scrcons.exe		http://musicctvclass.sosblogs.com/The...			
	66503 ms	GET   301: Moved Per...	?	3516	scrcons.exe		http://musictele.livejournal.com/data/r...	37		
	66505 ms	GET   301: Moved Per...	?	3516	scrcons.exe		http://moviemusictvm.wordpress.co...	17		
DEBUG	66520 ms	GET   301: Moved Per...	?	3516	scrcons.exe		http://yeetresbeau2012.livejournal.co...	38		
	67514 ms	GET   301: Moved Per...	?	3516	scrcons.exe		http://radiomusictv.wordpress.com/fe...	17		

Warning

[2924] gupdate.exe Removes files from Windows directory

Try community version for free!

Register now

Page 1 of 1