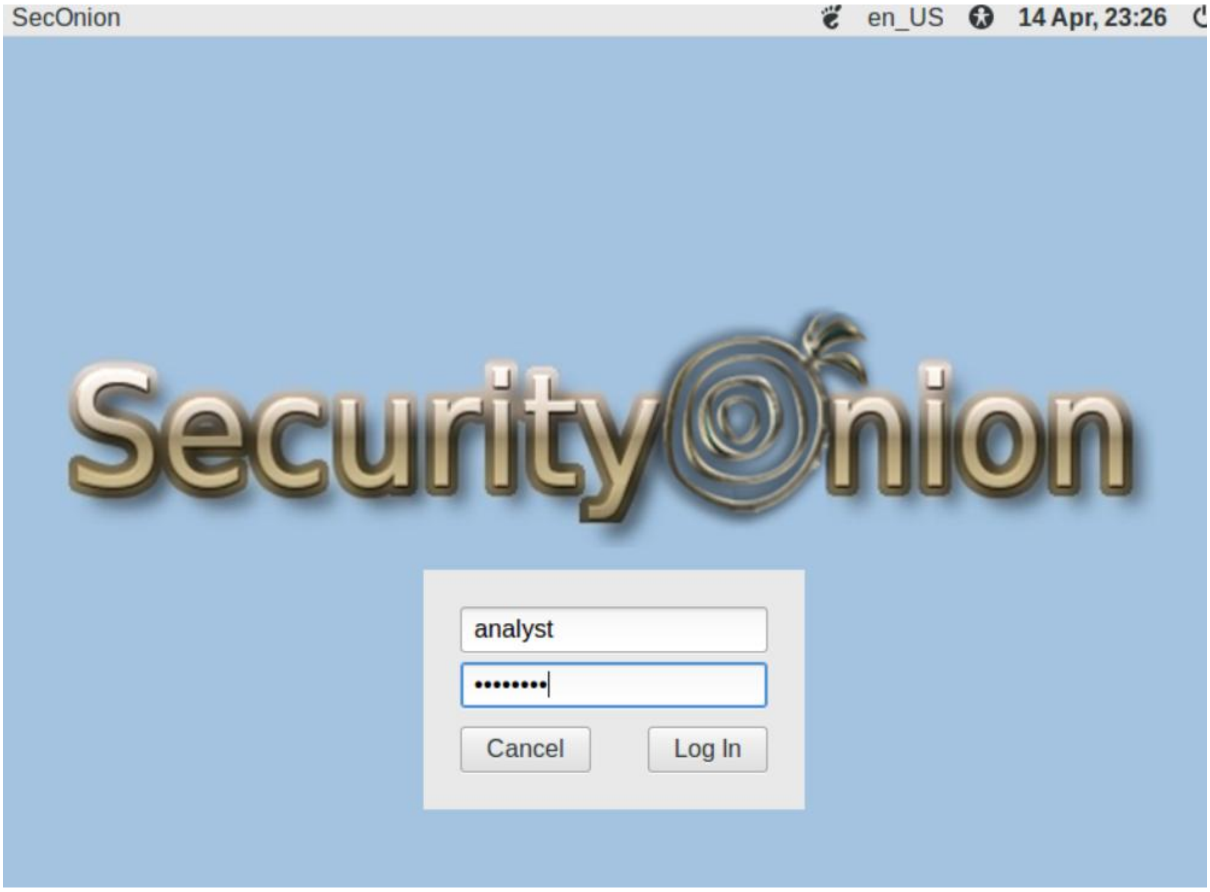
CyberOPs Associates skill koe dokumentointi

Part 1

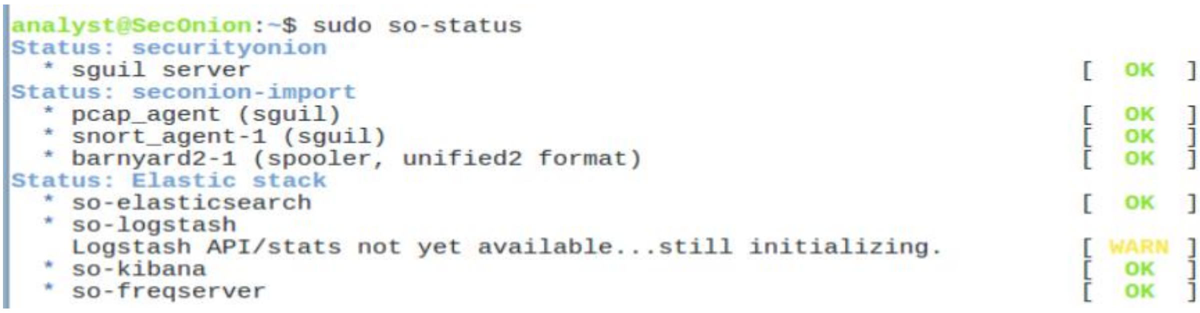
a)



analyst

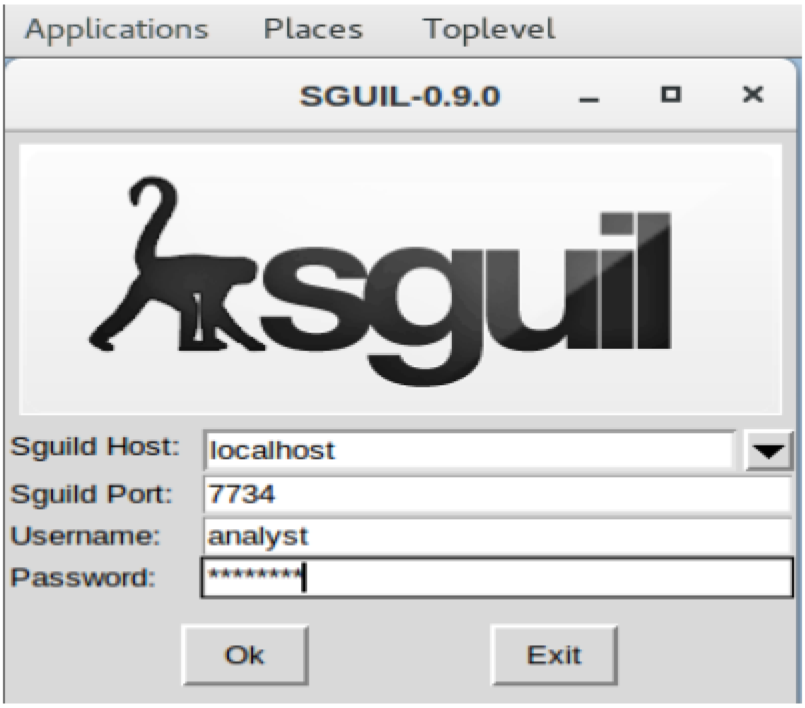
••••••••

b)



```
analyst@SecOnion:~$ sudo so-status
Status: securityonion
  * sguil server                                                     [  OK  ]
Status: seconion-import
  * pcap_agent (sguil)                                               [  OK  ]
  * snort_agent-1 (sguil)                                            [  OK  ]
  * barnyard2-1 (spooler, unified2 format)                           [  OK  ]
Status: Elastic stack
  * so-elasticsearch                                                 [  OK  ]
  * so-logstash
    Logstash API/stats not yet available...still initializing.       [ WARN ]
  * so-kibana                                                        [  OK  ]
  * so-freqserver                                                    [  OK  ]
```

c)



Sguild Host: localhost

Sguild Port: 7734

Username: analyst

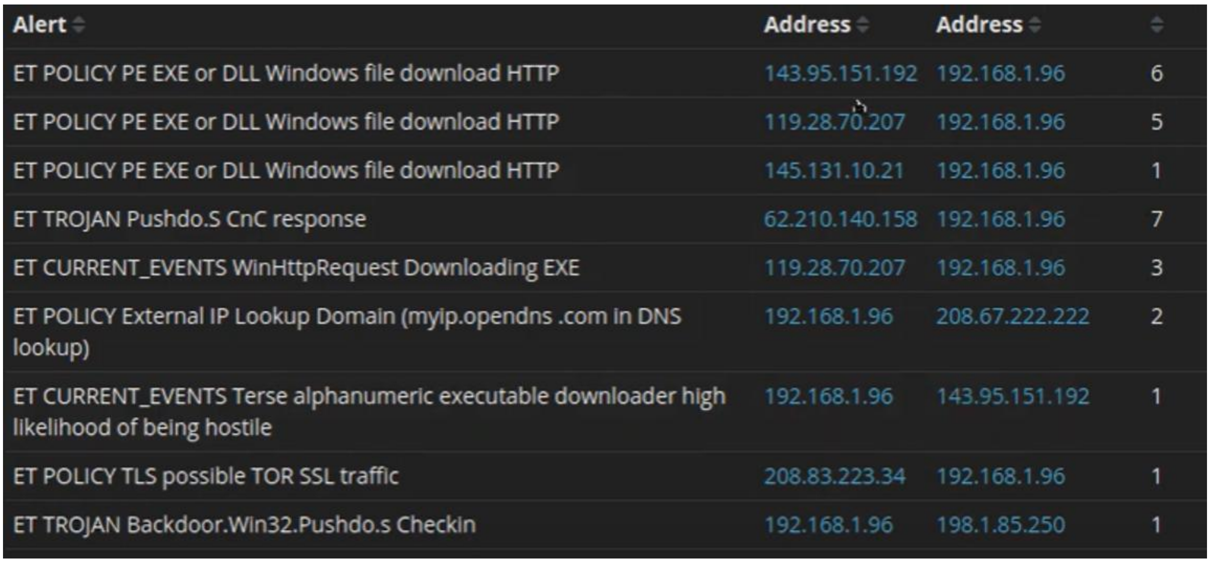
Password: ********

Step2

a)

27.6.2017 from 13:38:34 to 13:44:32

b)



Alert	Address	Address	
ET POLICY PE EXE or DLL Windows file download HTTP	143.95.151.192	192.168.1.96	6
ET POLICY PE EXE or DLL Windows file download HTTP	119.28.70.207	192.168.1.96	5
ET POLICY PE EXE or DLL Windows file download HTTP	145.131.10.21	192.168.1.96	1
ET TROJAN Pushdo.S CnC response	62.210.140.158	192.168.1.96	7
ET CURRENT_EVENTS WinHttpRequest Downloading EXE	119.28.70.207	192.168.1.96	3
ET POLICY External IP Lookup Domain (myip.opendns .com in DNS lookup)	192.168.1.96	208.67.222.222	2
ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile	192.168.1.96	143.95.151.192	1
ET POLICY TLS possible TOR SSL traffic	208.83.223.34	192.168.1.96	1
ET TROJAN Backdoor.Win32.Pushdo.s Checkin	192.168.1.96	198.1.85.250	1

c)

Internal IP address:
- 192.168.1.96

External IP address:

- 143.95.151.192
- 119.28.70.207
- 145.131.10.21
- 62.210.140.158
- 119.28.70.207
- 208.67.222.222
- 208.83.223.34
- 198.1.85.250

Part 2

step 1:

a)
IP: 192.168.1.96
MAC: 00-15-C5-DE-C7-3B
NIC Vendor: Dell Inc.

b) 27.6.2017 13:38:32 UTC. The gerv.gun was executed with Pushdo Trojan

Miten haittaohjelma vaikutti tietokoneen toimintaan?

Pushdo on troijalainen, jonka tarkoitus on ladata ja asentaa lisää haittaohjelmia.

Kun Pushdo ajetaan, se raportoi takaisin yhteen useista sen koodiin upotetuista komentopalvelimen IP-osoitteista. Palvelin kuuntelee TCP-porttia 80 ja teeskentelee olevansa Apache palvelin.

Tartunnan tapahduttua tämäntyyppinen haittaohjelma antaa hyökkääjälle mahdollisuuden ottaa yhteyttä koneellesi, salakuunnella ja katsella mitä teet. Varastaa henkilökohtaisia tietojasi tai pankkitietojasi, tuhota tiedostoja tai käyttää konettasi.

Step 2:

a)

gerv.gun -> matied.com/gerv.gun
trow.exe -> lounge-haarstudio.nl/oud/trow.exe
wp.exe -> vantagepointtechnologies.com/wp.exe

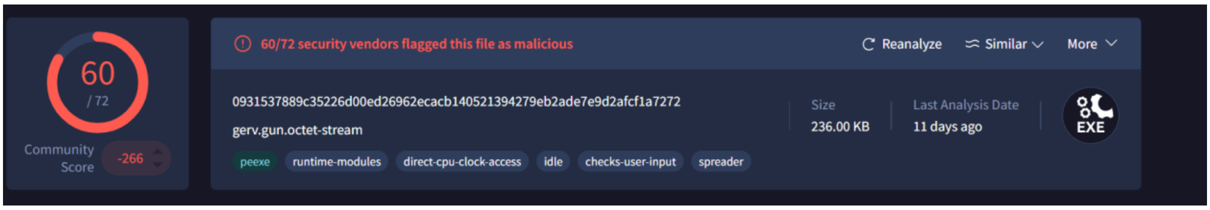
gerv.gun->
0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272

trow.exe->
94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1

wp.exe->
79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48

b)

gerv.gun



60
/ 72
Community Score -266

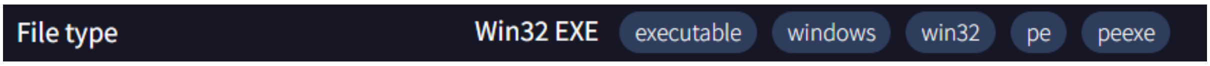
60/72 security vendors flagged this file as malicious

0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272
gerv.gun.octet-stream

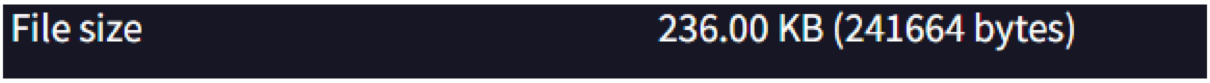
peexe runtime-modules direct-cpu-clock-access idle checks-user-input spreader

Size 236.00 KB

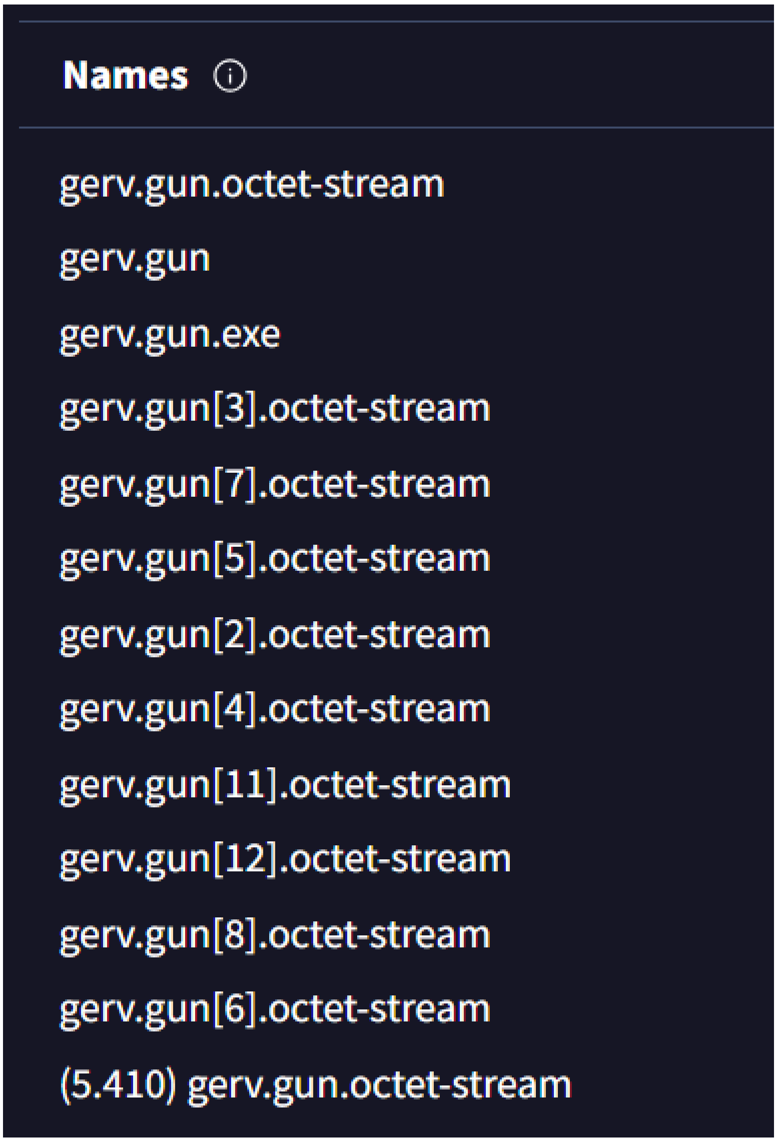
Last Analysis Date 11 days ago



File type Win32 EXE executable windows win32 pe peexe

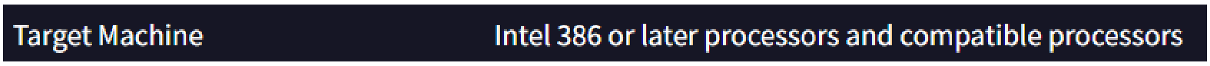


File size 236.00 KB (241664 bytes)



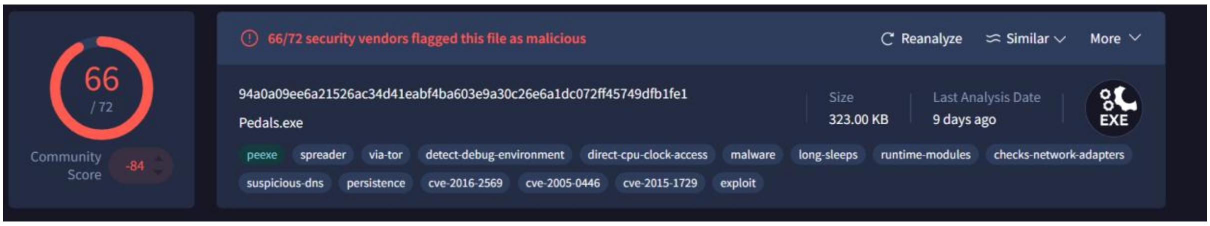
Names

gerv.gun.octet-stream
gerv.gun
gerv.gun.exe
gerv.gun[3].octet-stream
gerv.gun[7].octet-stream
gerv.gun[5].octet-stream
gerv.gun[2].octet-stream
gerv.gun[4].octet-stream
gerv.gun[11].octet-stream
gerv.gun[12].octet-stream
gerv.gun[8].octet-stream
gerv.gun[6].octet-stream
(5.410) gerv.gun.octet-stream



Target Machine	Intel 386 or later processors and compatible processors

trow.exe



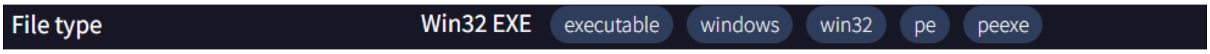
66/72 security vendors flagged this file as malicious

94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1
Pedals.exe

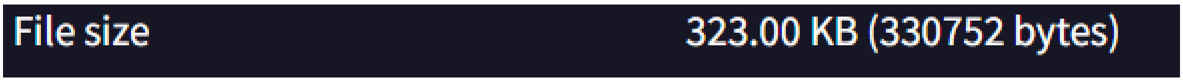
Size 323.00 KB

Last Analysis Date 9 days ago

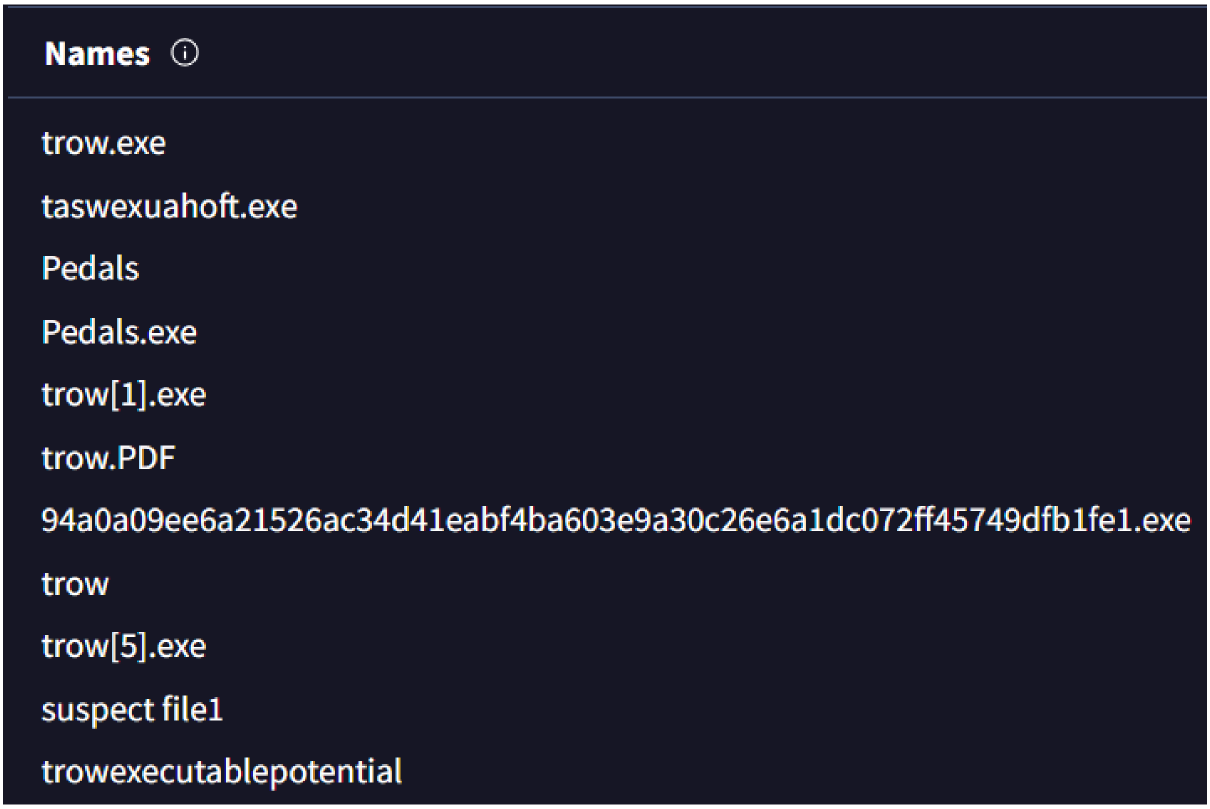
peexe spreader via-tor detect-debug-environment direct-cpu-clock-access malware long-sleeps runtime-modules checks-network-adapters suspicious-dns persistence cve-2016-2569 cve-2005-0446 cve-2015-1729 exploit



File type	Win32 EXE executable windows win32 pe peexe



File size	323.00 KB (330752 bytes)



Names

trow.exe

taswexuahoft.exe

Pedals

Pedals.exe

trow[1].exe

trow.PDF

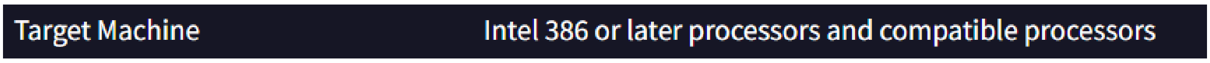
94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1.exe

trow

trow[5].exe

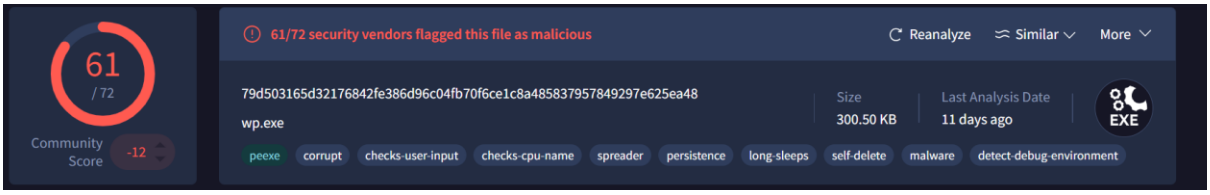
suspect file1

trowexecutablepotential



Target Machine	Intel 386 or later processors and compatible processors

wp.exe



61/72 security vendors flagged this file as malicious

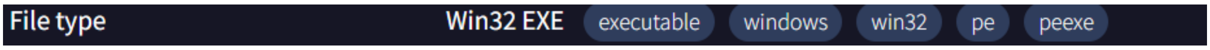
79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48

wp.exe

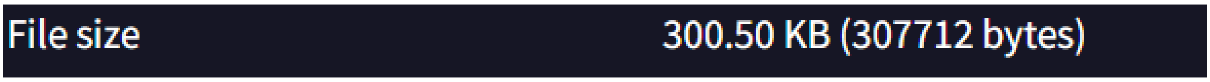
Size: 300.50 KB

Last Analysis Date: 11 days ago

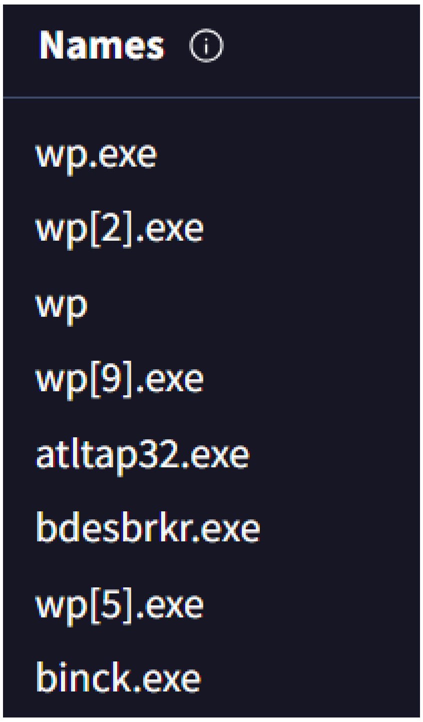
peexe corrupt checks-user-input checks-cpu-name spreader persistence long-sleeps self-delete malware detect-debug-environment



File type	Win32 EXE executable windows win32 pe peexe



File size	300.50 KB (307712 bytes)



Names ⓘ

wp.exe

wp[2].exe

wp

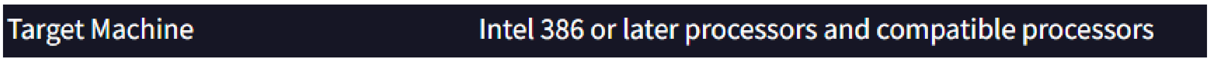
wp[9].exe

atltap32.exe

bdesbrkr.exe

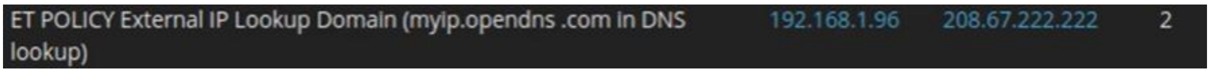
wp[5].exe

binck.exe



Target Machine	Intel 386 or later processors and compatible processors

c)



ET POLICY External IP Lookup Domain (myip.opendns .com in DNS lookup)	192.168.1.96	208.67.222.222	2

Tartunta alkoi, kun käyttäjä IP-osoite 192.168.1.96 suoritti DNS kyselyn haittaohjelman sisältäneen domainin IP-osoitteen 208.67.222.222 kautta.

Step 3:

Tartunta tapahtui, kun Windows tietokone host ip 192.168.1.96 suoritti DNS-kyselyä IP-osoitteesta 208.67.222.222, josta tietokone sai Pushdo-troijalais tartunnan. Pushdo-troijalainen kuuntelee porttia 80. Tartunnan jälkeen Pushdo-troijalainen lataa gerv.gun, trow.exe ja wp.exe haittaohjelmatiedostot tietokoneeseen. Tiedostojen haittaohjelma mahdollisuuden tarkistin virustotal.com-sivustoa käyttäen niiden SHA256 hash hyödyntäen. Virustotal.com kertoi tiedostojen olevan haittaohjelmia.