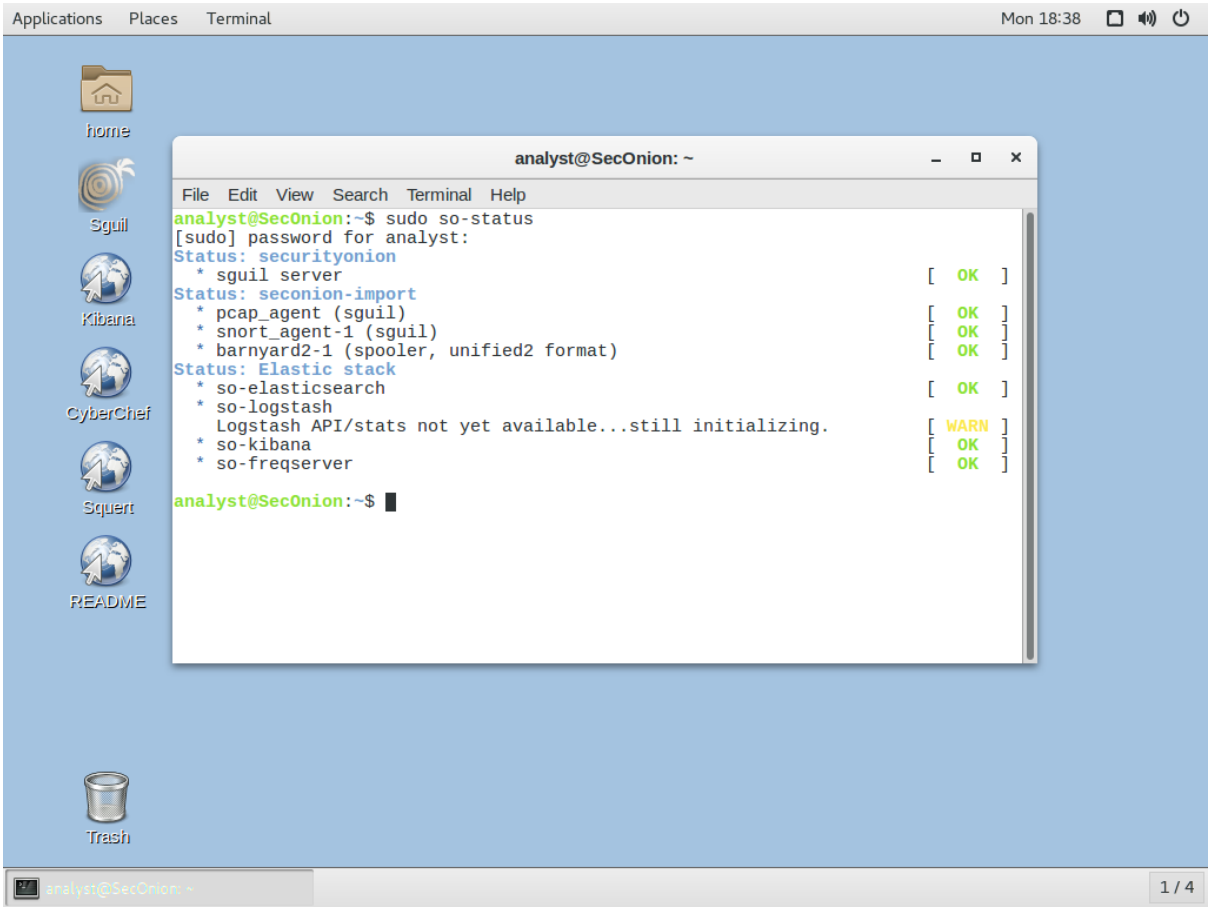
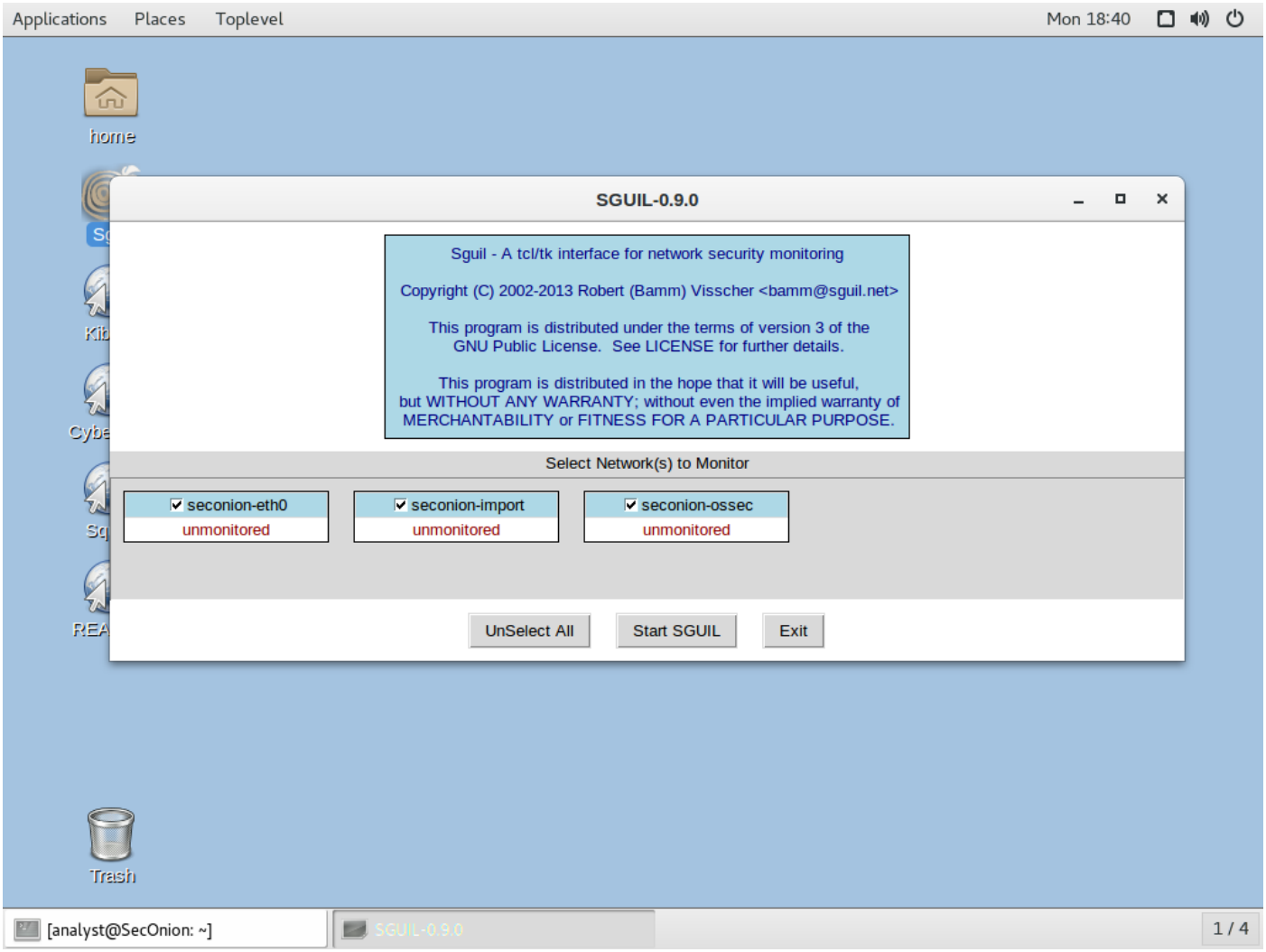
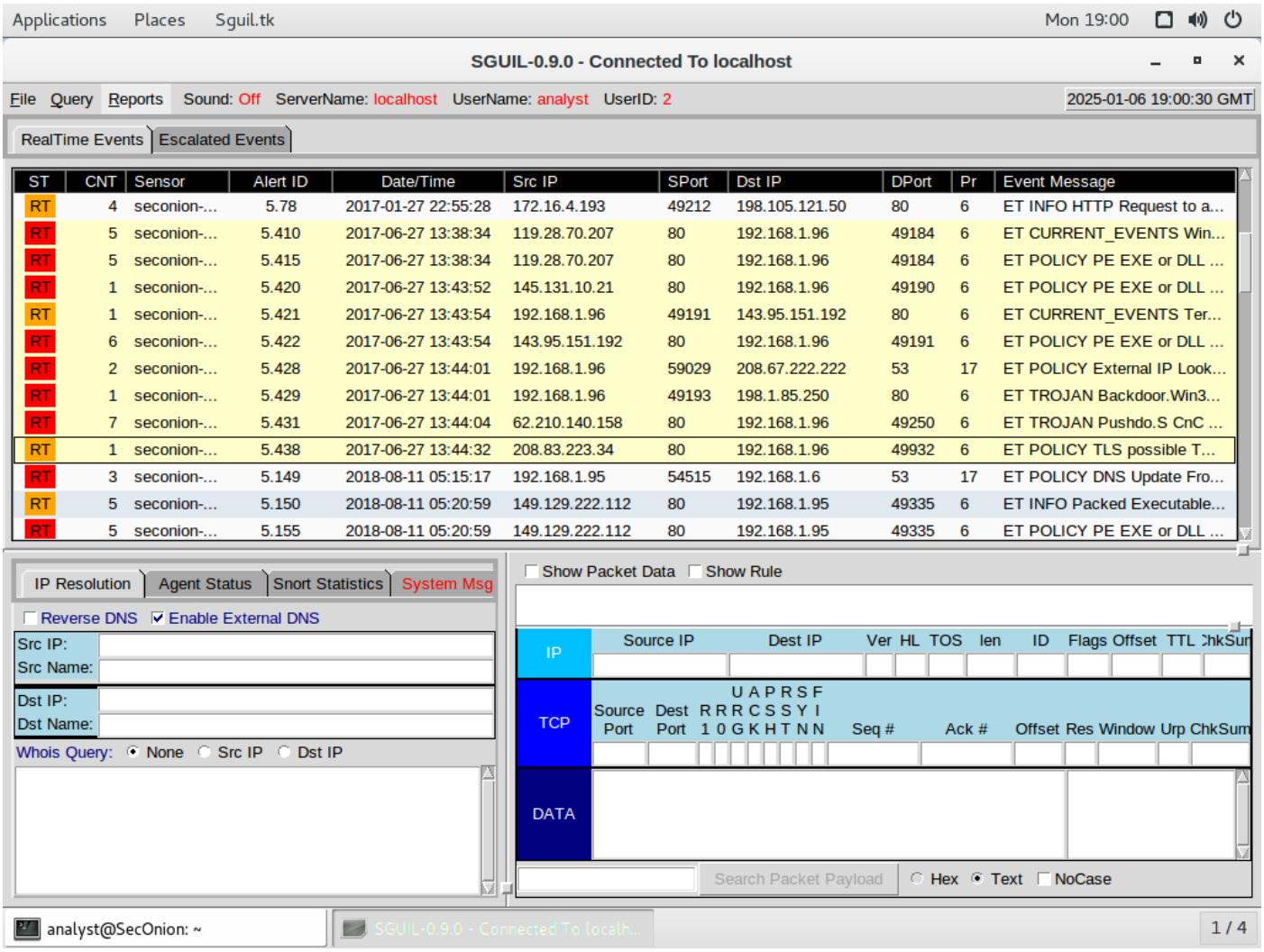
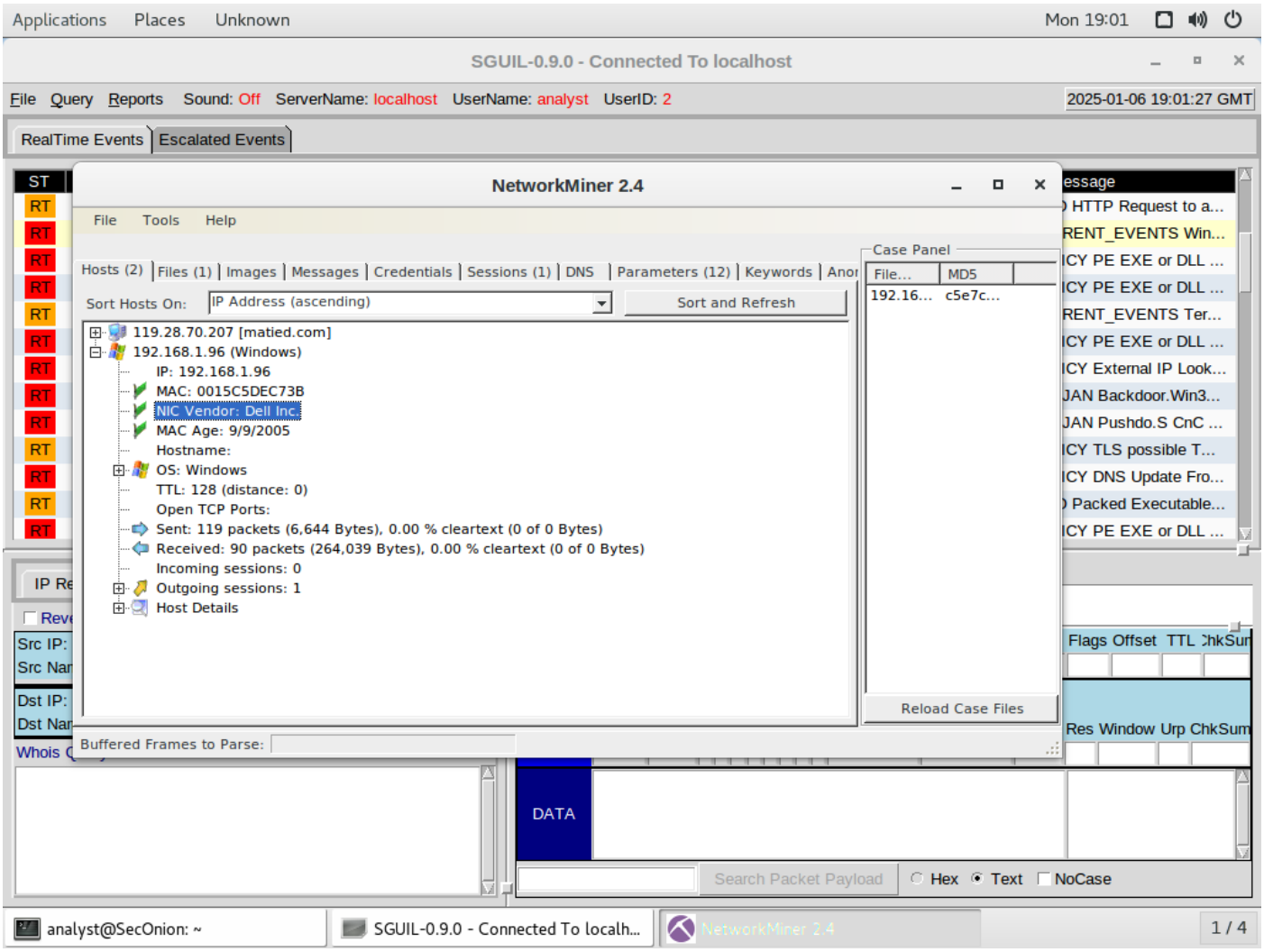
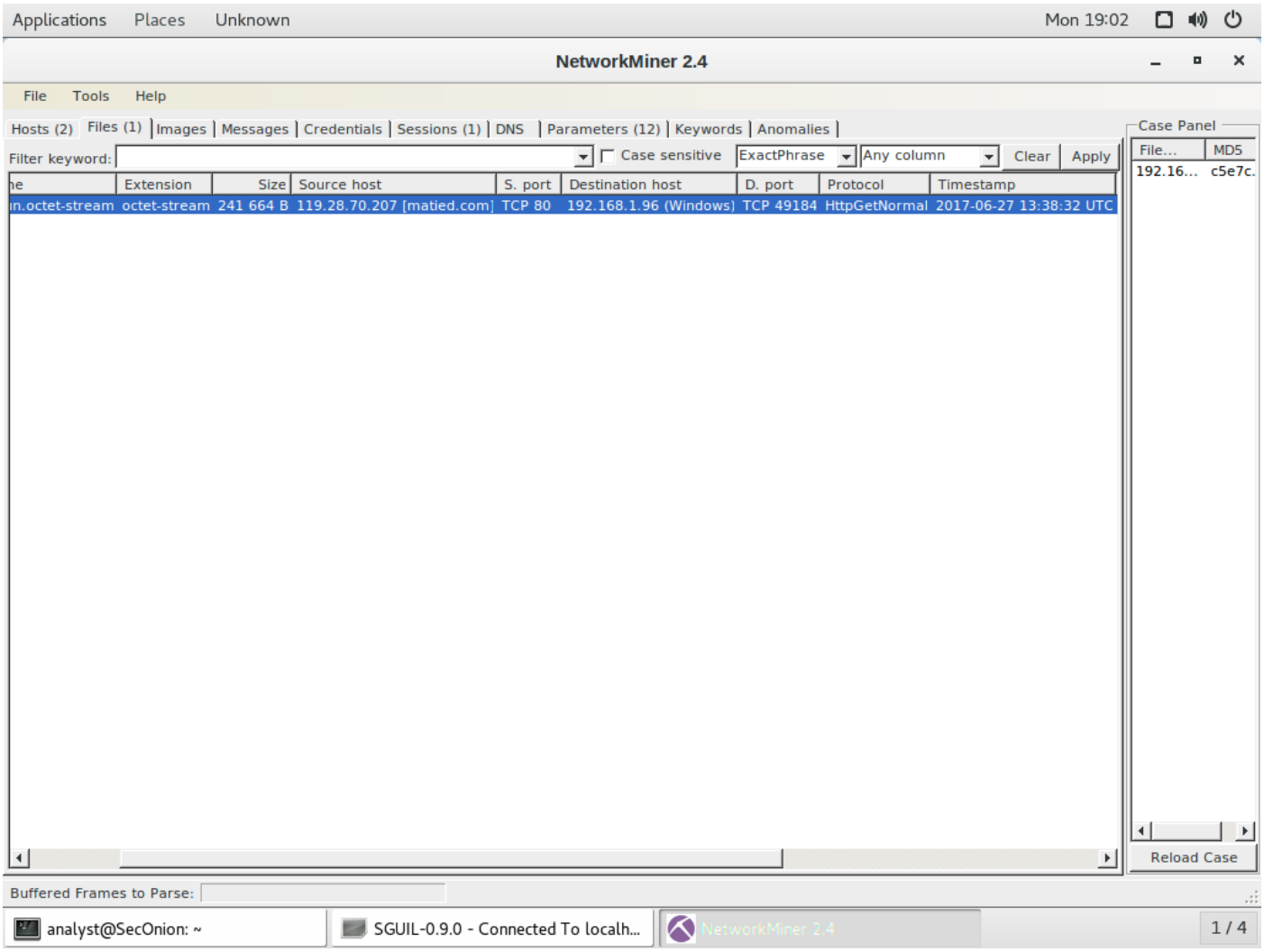

Applications Places Terminal Mon 18:38
home
Sguil
Kibana
CyberChef
Squert
README
Trash
analyst@SecOnion: ~
File Edit View Search Terminal Help
analyst@SecOnion:~$ sudo so-status
[sudo] password for analyst:
Status: securityonion
* sguil server [OK]
Status: seconion-import
* pcap_agent (sguil) [OK]
* 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]
analyst@SecOnion:~$
analyst@SecOnion: ~
1 / 4

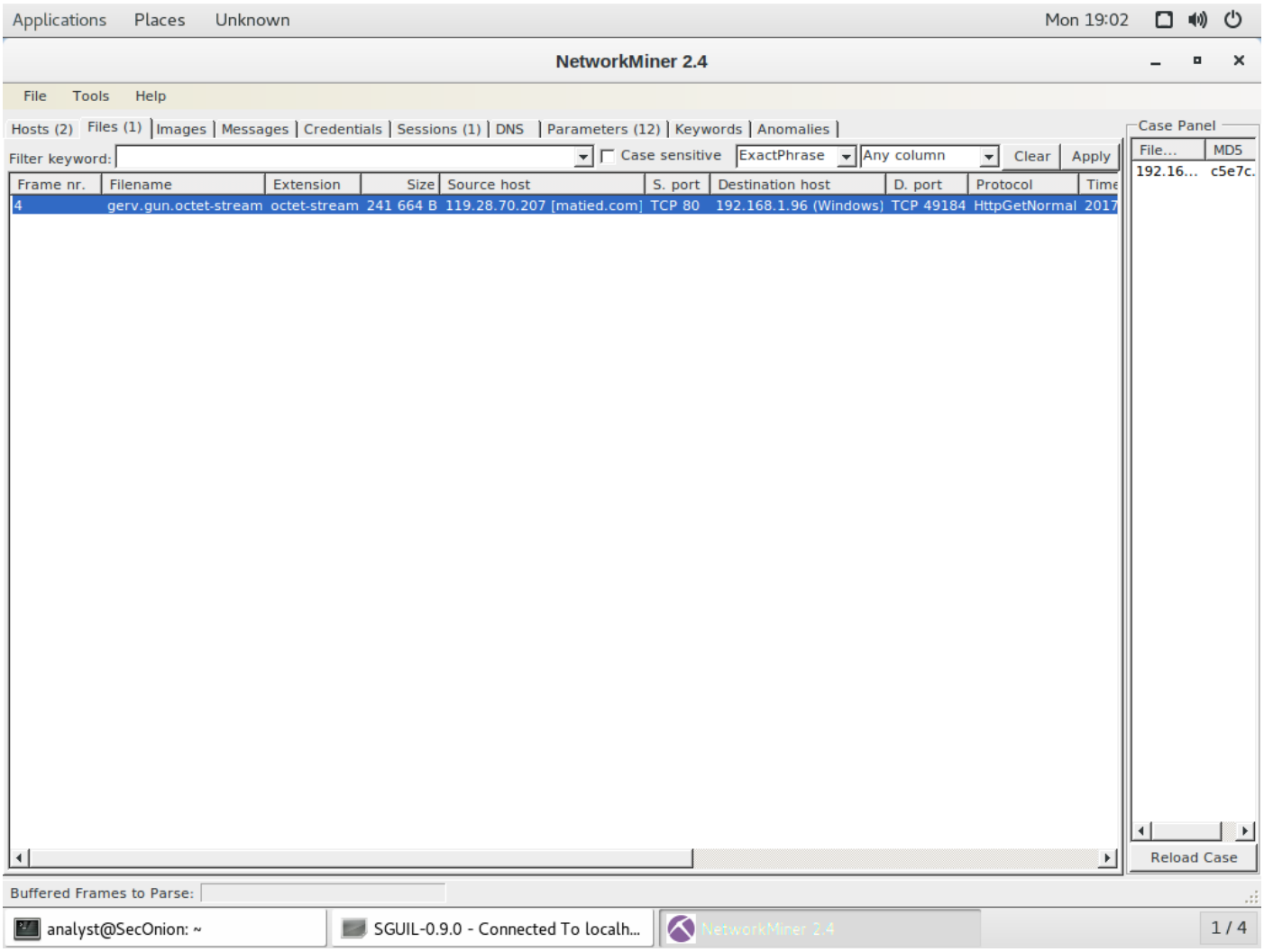

Applications Places Toplevel Mon 18:40
home
Sguil
Kibana
CyberChef
Squert
README
Trash
SGUIL-0.9.0
sguil
Sguild Host: localhost
Sguild Port: 7734
Username: analyst
Password: ********
Ok
Exit
[analyst@SecOnion: ~]
SGUIL-0.9.0
1 / 4

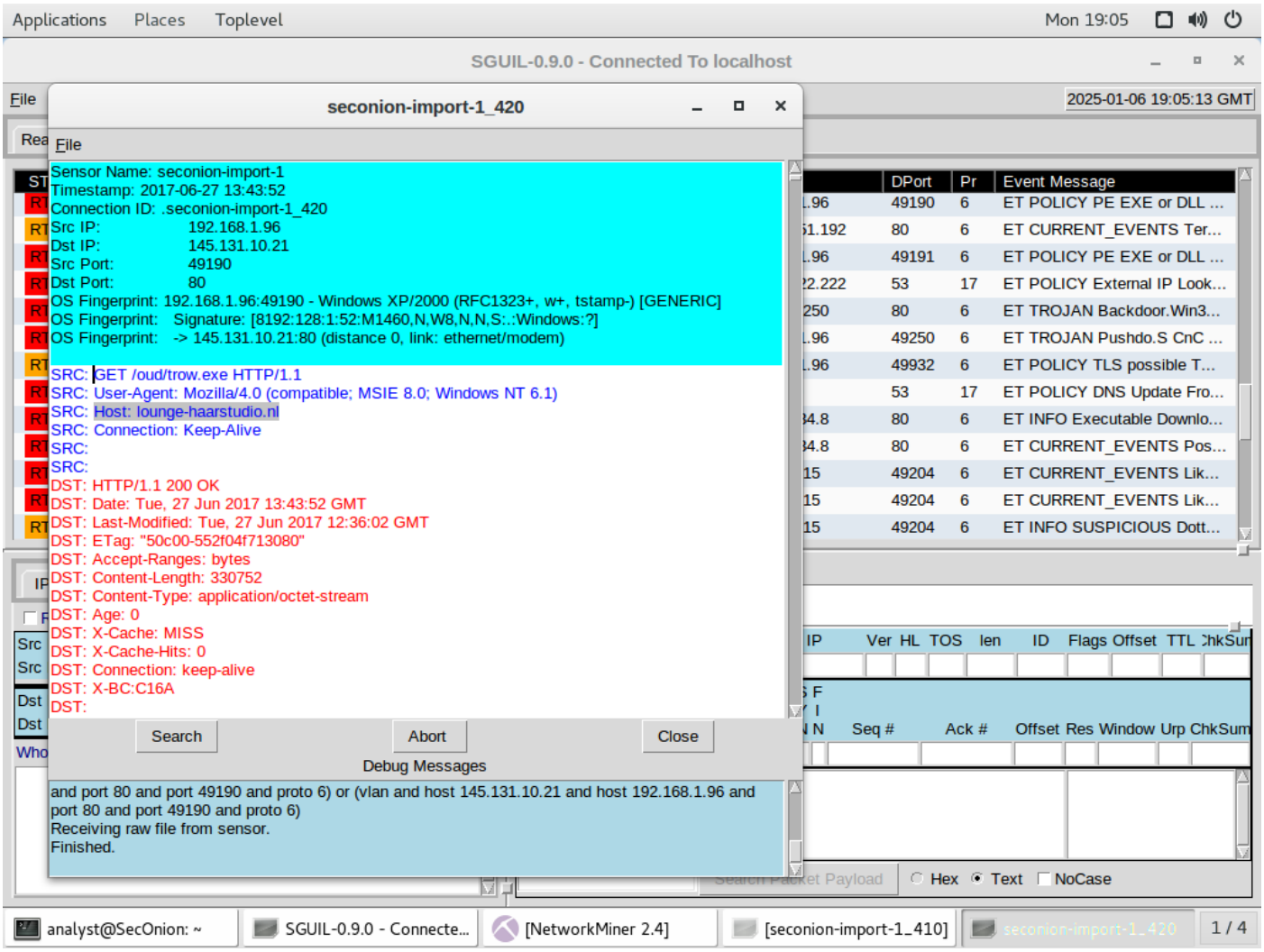

Applications
Places
Toplevel
Mon 18:40
home
SGUIL-0.9.0
Sguil - A tcl/tk interface for network security monitoring
Copyright (C) 2002-2013 Robert (Bamm) Visscher <bamm@sguil.net>
This program is distributed under the terms of version 3 of the GNU Public License. See LICENSE for further details.
This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
Select Network(s) to Monitor
seconion-eth0
unmonitored
seconion-import
unmonitored
seconion-ossec
unmonitored
UnSelect All
Start SGUIL
Exit
Trash
[analyst@SecOnion: ~]
SGUIL-0.9.0
1 / 4

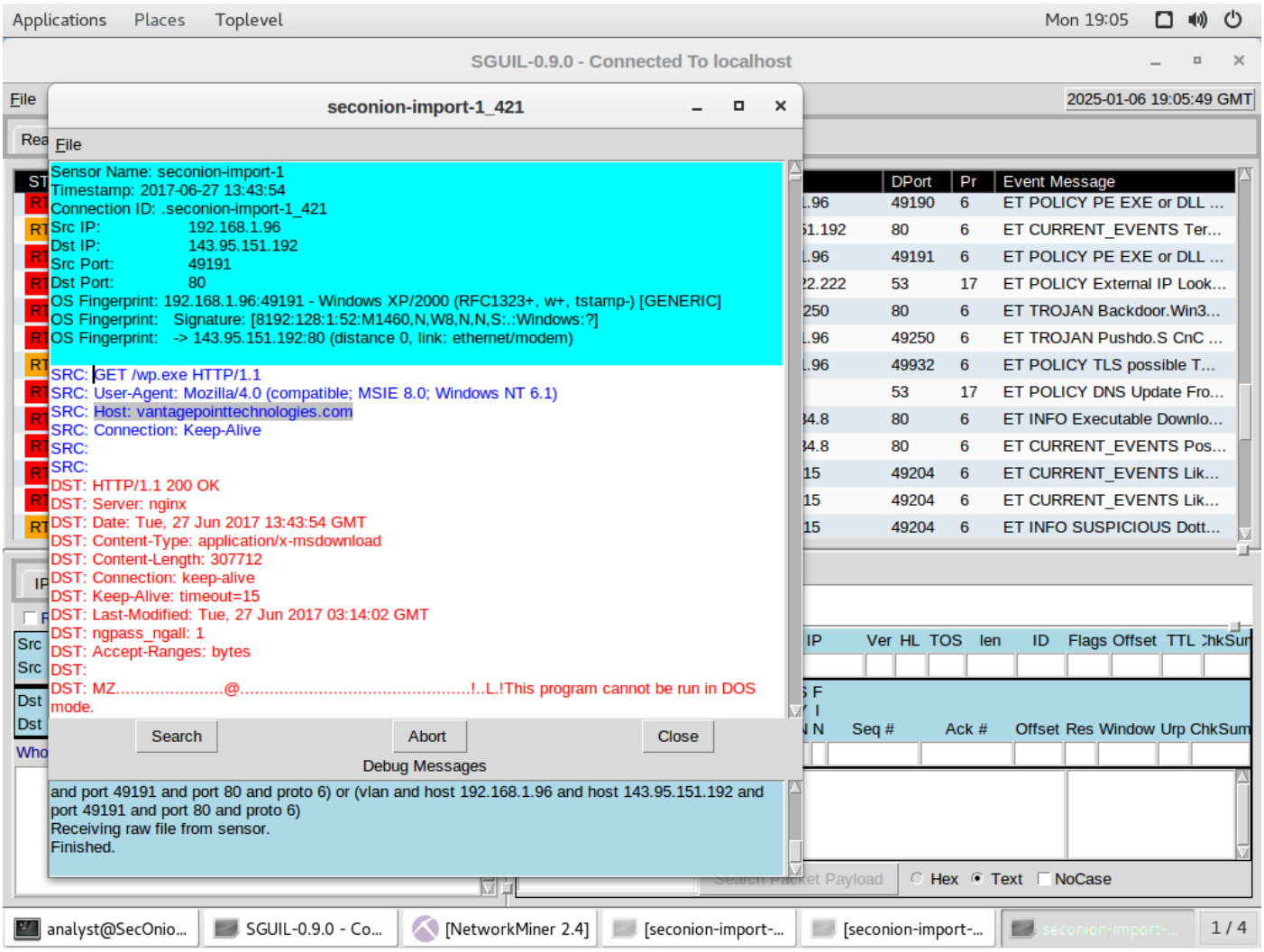

Applications
Places
Sguil.tk
Mon 19:00
SGUIL-0.9.0 - Connected To localhost
File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2
2025-01-06 19:00:30 GMT
RealTime Events
Escalated Events
ST CNT Sensor Alert ID Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 4 seconion-... 5.78 2017-01-27 22:55:28 172.16.4.193 49212 198.105.121.50 80 6 ET INFO HTTP Request to a...
RT 5 seconion-... 5.410 2017-06-27 13:38:34 119.28.70.207 80 192.168.1.96 49184 6 ET CURRENT_EVENTS Win...
RT 5 seconion-... 5.415 2017-06-27 13:38:34 119.28.70.207 80 192.168.1.96 49184 6 ET POLICY PE EXE or DLL ...
RT 1 seconion-... 5.420 2017-06-27 13:43:52 145.131.10.21 80 192.168.1.96 49190 6 ET POLICY PE EXE or DLL ...
RT 1 seconion-... 5.421 2017-06-27 13:43:54 192.168.1.96 49191 143.95.151.192 80 6 ET CURRENT_EVENTS Ter...
RT 6 seconion-... 5.422 2017-06-27 13:43:54 143.95.151.192 80 192.168.1.96 49191 6 ET POLICY PE EXE or DLL ...
RT 2 seconion-... 5.428 2017-06-27 13:44:01 192.168.1.96 59029 208.67.222.222 53 17 ET POLICY External IP Look...
RT 1 seconion-... 5.429 2017-06-27 13:44:01 192.168.1.96 49193 198.1.85.250 80 6 ET TROJAN Backdoor.Win3...
RT 7 seconion-... 5.431 2017-06-27 13:44:04 62.210.140.158 80 192.168.1.96 49250 6 ET TROJAN Pushdo.S CnC ...
RT 1 seconion-... 5.438 2017-06-27 13:44:32 208.83.223.34 80 192.168.1.96 49932 6 ET POLICY TLS possible T...
RT 3 seconion-... 5.149 2018-08-11 05:15:17 192.168.1.95 54515 192.168.1.6 53 17 ET POLICY DNS Update Fro...
RT 5 seconion-... 5.150 2018-08-11 05:20:59 149.129.222.112 80 192.168.1.95 49335 6 ET INFO Packed Executable...
RT 5 seconion-... 5.155 2018-08-11 05:20:59 149.129.222.112 80 192.168.1.95 49335 6 ET POLICY PE EXE or DLL ...
IP Resolution
Agent Status
Snort Statistics
System Msg
Reverse DNS
Enable External DNS
Src IP:
Src Name:
Dst IP:
Dst Name:
Whois Query: None Src IP Dst IP
Show Packet Data
Show Rule
IP
Source IP
Dest IP
Ver HL TOS len ID Flags Offset TTL ChkSum
TCP
Source Port
Dest Port
R R R U A P R S F
1 0 G K H T N N
Seq #
Ack #
Offset Res Window Urp ChkSum
DATA
Search Packet Payload
Hex
Text
NoCase
analyst@SecOnion: ~
SGUIL-0.9.0 - Connected To localh...
1 / 4

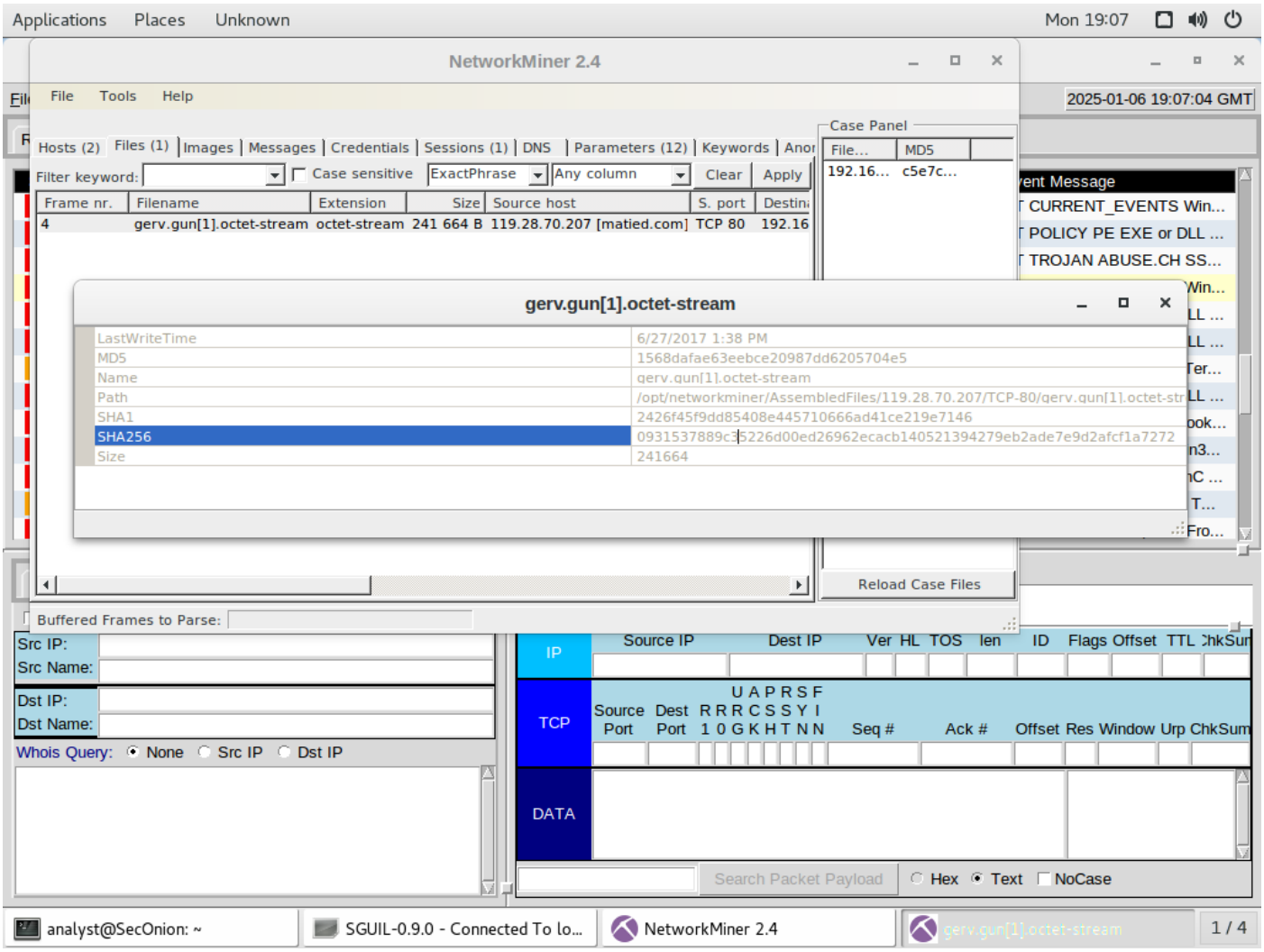

Applications
Places
Unknown
Mon 19:01
SGUIL-0.9.0 - Connected To localhost
File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2
2025-01-06 19:01:27 GMT
RealTime Events
Escalated Events
NetworkMiner 2.4
File
Tools
Help
Hosts (2)
Files (1)
Images
Messages
Credentials
Sessions (1)
DNS
Parameters (12)
Keywords
Sort Hosts On:
IP Address (ascending)
Sort and Refresh
119.28.70.207 [matied.com]
192.168.1.96 (Windows)
IP: 192.168.1.96
MAC: 0015C5DEC73B
NIC Vendor: Dell Inc
MAC Age: 9/9/2005
Hostname:
OS: Windows
TTL: 128 (distance: 0)
Open TCP Ports:
Sent: 119 packets (6,644 Bytes), 0.00 % cleartext (0 of 0 Bytes)
Received: 90 packets (264,039 Bytes), 0.00 % cleartext (0 of 0 Bytes)
Incoming sessions: 0
Outgoing sessions: 1
Host Details
Case Panel
File...
MD5
192.16...
c5e7c...
Reload Case Files
Buffered Frames to Parse:
DATA
Search Packet Payload
Hex
Text
NoCase
analyst@SecOnion: ~
SGUIL-0.9.0 - Connected To localh...
NetworkMiner 2.4
1 / 4

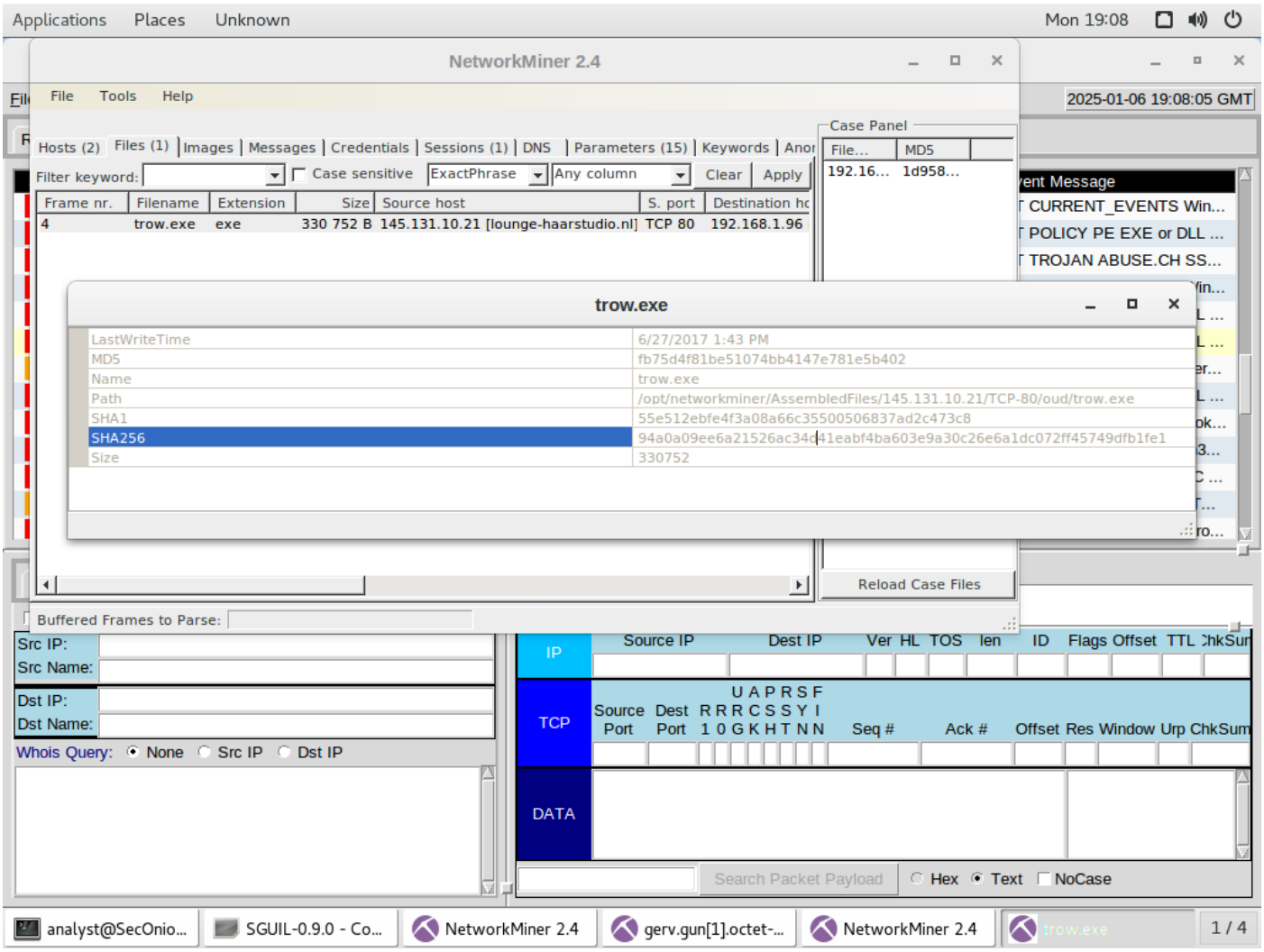

Applications
Places
Unknown
Mon 19:02
NetworkMiner 2.4
File
Tools
Help
Hosts (2)
Files (1)
Images
Messages
Credentials
Sessions (1)
DNS
Parameters (12)
Keywords
Anomalies
Filter keyword:
Case sensitive
ExactPhrase
Any column
Clear
Apply
he
Extension
Size
Source host
S. port
Destination host
D. port
Protocol
Timestamp
in.octet-stream
octet-stream
241 664 B
119.28.70.207 [matied.com]
TCP 80
192.168.1.96 (Windows)
TCP 49184
HttpGetNormal
2017-06-27 13:38:32 UTC
Case Panel
File...
MD5
192.16...
c5e7c.
Reload Case
Buffered Frames to Parse:
analyst@SecOnion: ~
SGUIL-0.9.0 - Connected To localh...
NetworkMiner 2.4
1 / 4

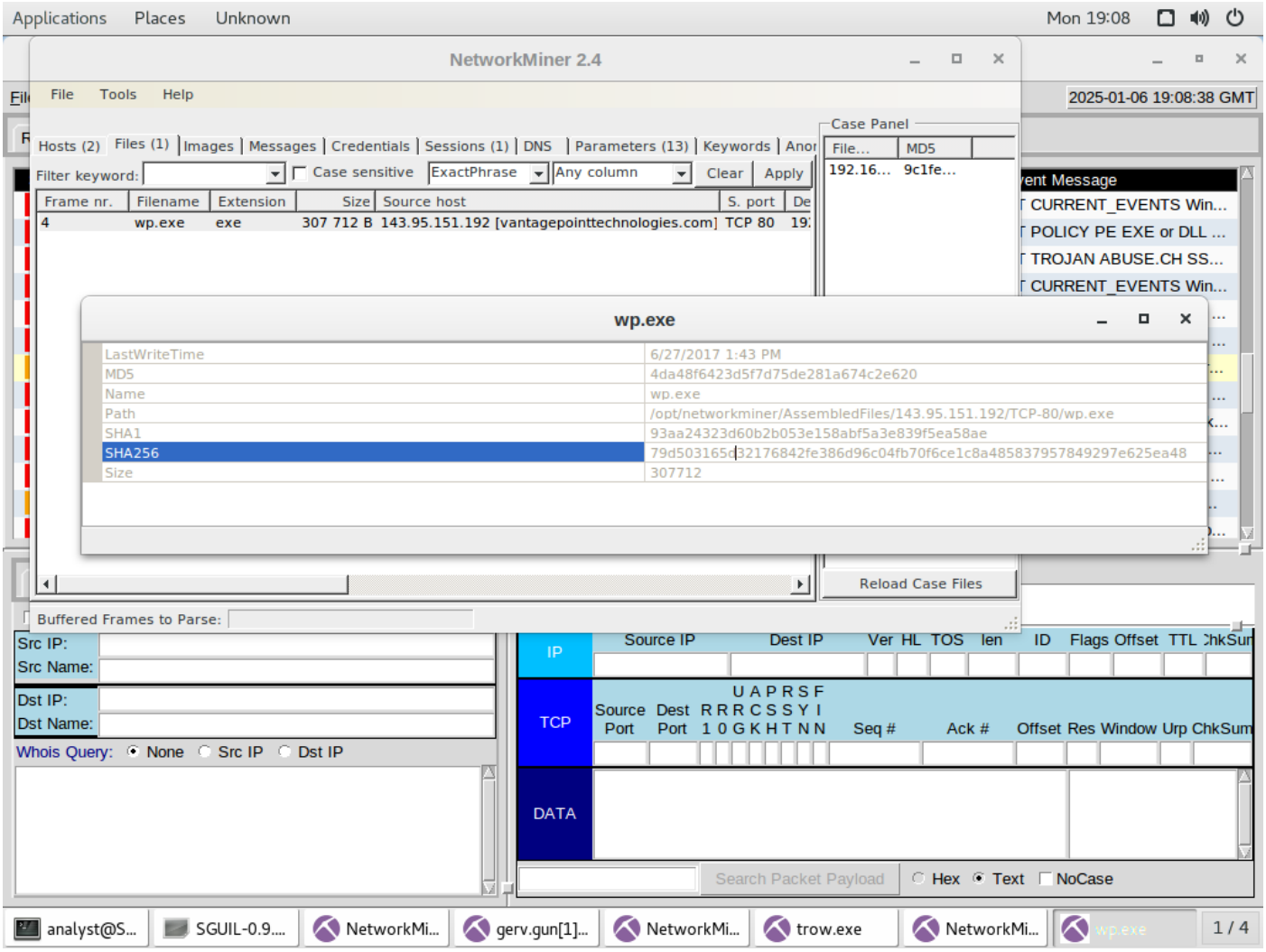

Applications
Places
Unknown
Mon 19:02
NetworkMiner 2.4
File
Tools
Help
Hosts (2)
Files (1)
Images
Messages
Credentials
Sessions (1)
DNS
Parameters (12)
Keywords
Anomalies
Filter keyword:
Case sensitive
ExactPhrase
Any column
Clear
Apply
Frame nr.
Filename
Extension
Size
Source host
S. port
Destination host
D. port
Protocol
Time
4
gerv.gun.octet-stream
octet-stream
241 664 B
119.28.70.207 [matied.com]
TCP 80
192.168.1.96 (Windows)
TCP 49184
HttpGetNormal
2017
Case Panel
File...
MD5
192.16...
c5e7c.
Reload Case
Buffered Frames to Parse:
analyst@SecOnion: ~
SGUIL-0.9.0 - Connected To localh...
NetworkMiner 2.4
1 / 4

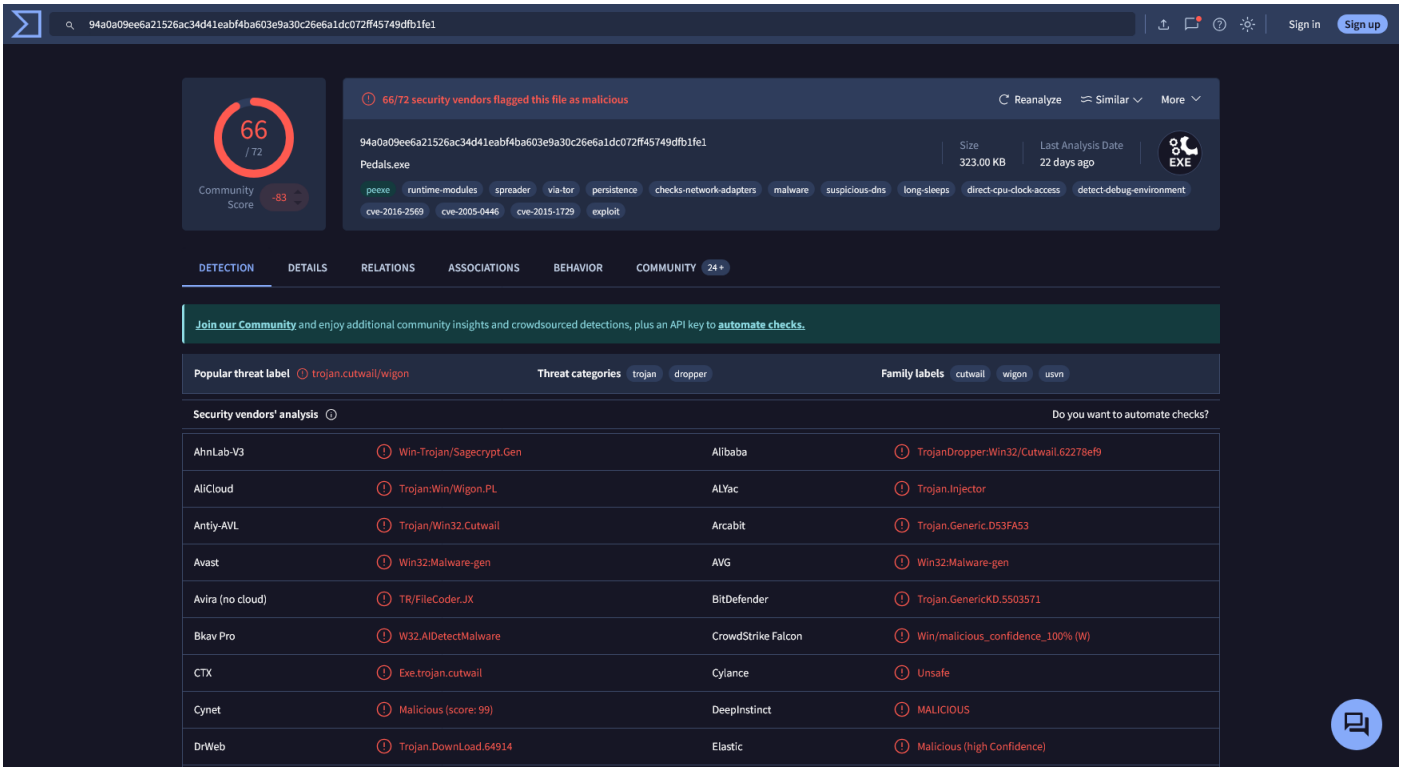

Applications
Places
Toplevel
Mon 19:05
SGUIL-0.9.0 - Connected To localhost
File
2025-01-06 19:05:13 GMT
seconion-import-1_420
File
Sensor Name: seconion-import-1
Timestamp: 2017-06-27 13:43:52
Connection ID: .seconion-import-1_420
Src IP: 192.168.1.96
Dst IP: 145.131.10.21
Src Port: 49190
Dst Port: 80
OS Fingerprint: 192.168.1.96:49190 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint: Signature: [8192:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint: -> 145.131.10.21:80 (distance 0, link: ethernet/modem)
SRC: GET /oud/trow.exe HTTP/1.1
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
SRC: Host: lounge-haarstudio.nl
SRC: Connection: Keep-Alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Tue, 27 Jun 2017 13:43:52 GMT
DST: Last-Modified: Tue, 27 Jun 2017 12:36:02 GMT
DST: ETag: "50c00-552f04f713080"
DST: Accept-Ranges: bytes
DST: Content-Length: 330752
DST: Content-Type: application/octet-stream
DST: Age: 0
DST: X-Cache: MISS
DST: X-Cache-Hits: 0
DST: Connection: keep-alive
DST: X-BC:C16A
DST:
Search
Abort
Close
Debug Messages
and port 80 and port 49190 and proto 6) or (vlan and host 145.131.10.21 and host 192.168.1.96 and port 80 and port 49190 and proto 6)
Receiving raw file from sensor.
Finished.
DPort
Pr
Event Message
ET POLICY PE EXE or DLL ...
ET CURRENT_EVENTS Ter...
ET POLICY PE EXE or DLL ...
ET POLICY External IP Look...
ET TROJAN Backdoor.Win3...
ET TROJAN Pushdo.S CnC ...
ET POLICY TLS possible T...
ET POLICY DNS Update Fro...
ET INFO Executable Downlo...
ET CURRENT_EVENTS Pos...
ET CURRENT_EVENTS Lik...
ET CURRENT_EVENTS Lik...
ET INFO SUSPICIOUS Dott...
IP
Ver
HL
TOS
len
ID
Flags
Offset
TTL
Seq #
Ack #
Offset
Res
Window
Urp
ChkSum
Hex
Text
NoCase
analyst@SecOnion: ~
SGUIL-0.9.0 - Connecte...
[NetworkMiner 2.4]
[seconion-import-1_410]
seconion-import-1_420
1 / 4

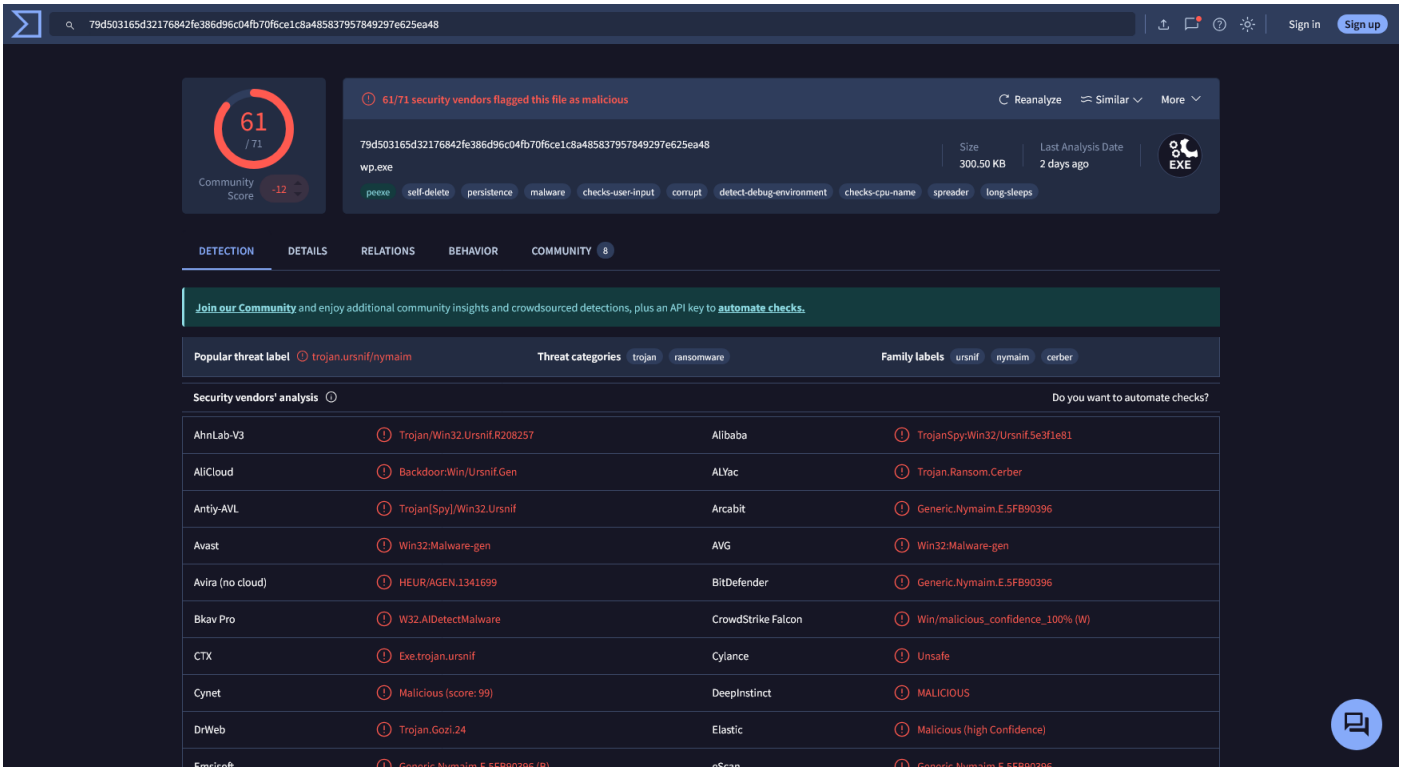

Applications
Places
Toplevel
Mon 19:05
SGUIL-0.9.0 - Connected To localhost
File
2025-01-06 19:05:49 GMT
seconion-import-1_421
File
Sensor Name: seconion-import-1
Timestamp: 2017-06-27 13:43:54
Connection ID: .seconion-import-1_421
Src IP: 192.168.1.96
Dst IP: 143.95.151.192
Src Port: 49191
Dst Port: 80
OS Fingerprint: 192.168.1.96:49191 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint: Signature: [8192:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint: -> 143.95.151.192:80 (distance 0, link: ethernet/modem)
SRC: GET /wp.exe HTTP/1.1
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
SRC: Host: vantagepointtechnologies.com
SRC: Connection: Keep-Alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Server: nginx
DST: Date: Tue, 27 Jun 2017 13:43:54 GMT
DST: Content-Type: application/x-msdownload
DST: Content-Length: 307712
DST: Connection: keep-alive
DST: Keep-Alive: timeout=15
DST: Last-Modified: Tue, 27 Jun 2017 03:14:02 GMT
DST: ngpass_ngall: 1
DST: Accept-Ranges: bytes
DST:
DST: MZ.....@.....!..L.!This program cannot be run in DOS mode.
Search
Abort
Close
Debug Messages
and port 49191 and port 80 and proto 6) or (vlan and host 192.168.1.96 and host 143.95.151.192 and port 49191 and port 80 and proto 6)
Receiving raw file from sensor.
Finished.
DPort
Pr
Event Message
ET POLICY PE EXE or DLL ...
ET CURRENT_EVENTS Ter...
ET POLICY PE EXE or DLL ...
ET POLICY External IP Look...
ET TROJAN Backdoor.Win3...
ET TROJAN Pushdo.S CnC ...
ET POLICY TLS possible T...
ET POLICY DNS Update Fro...
ET INFO Executable Downlo...
ET CURRENT_EVENTS Pos...
ET CURRENT_EVENTS Lik...
ET CURRENT_EVENTS Lik...
ET INFO SUSPICIOUS Dott...
Hex
Text
NoCase
analyst@SecOnio...
SGUIL-0.9.0 - Co...
[NetworkMiner 2.4]
[seconion-import-...
[seconion-import-...
seconion-import-...
1 / 4

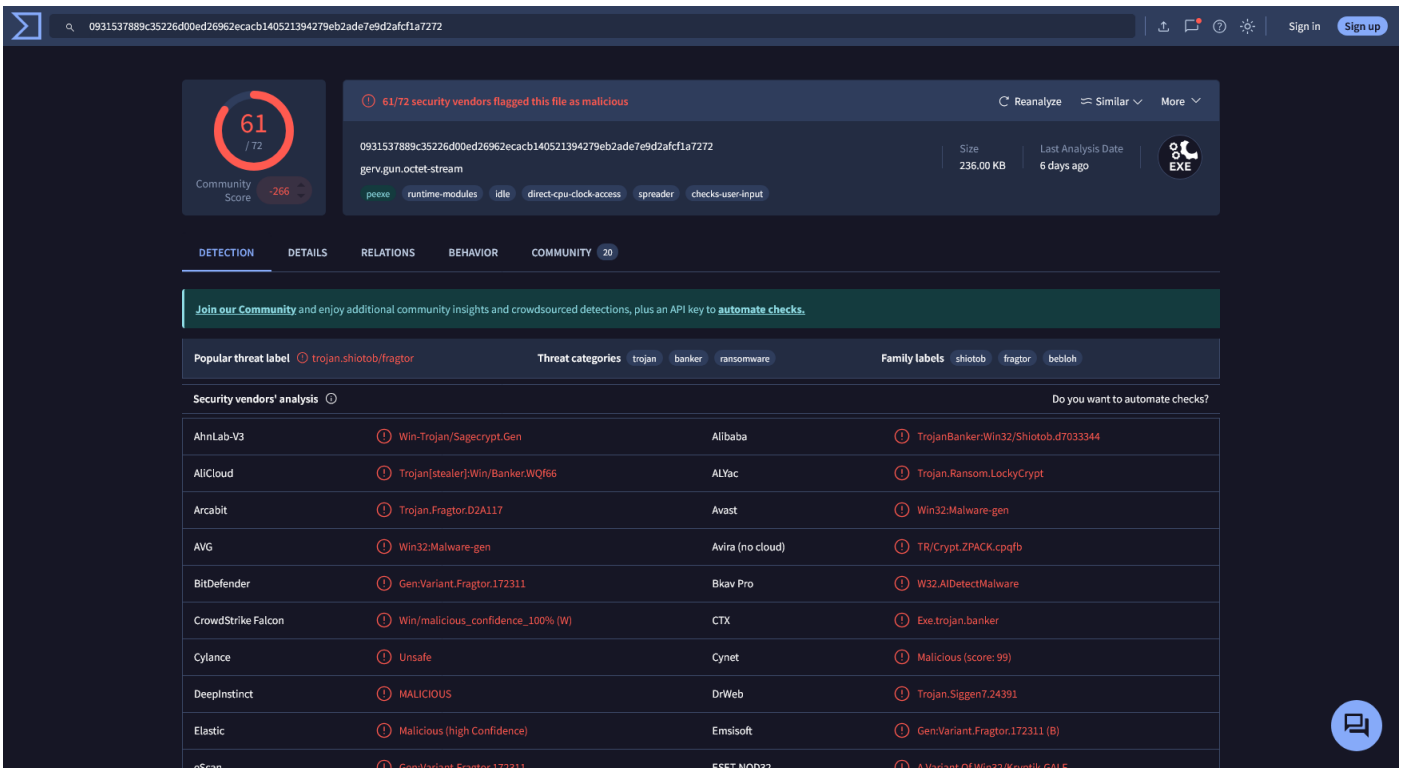

Applications
Places
Unknown
Mon 19:07
NetworkMiner 2.4
File
Tools
Help
2025-01-06 19:07:04 GMT
Hosts (2)
Files (1)
Images
Messages
Credentials
Sessions (1)
DNS
Parameters (12)
Keywords
Filter keyword:
Case sensitive
ExactPhrase
Any column
Clear
Apply
Frame nr.
Filename
Extension
Size
Source host
S. port
Destina
4
gerv.gun[1].octet-stream
octet-stream
241 664 B
119.28.70.207 [matied.com]
TCP 80
192.16
Case Panel
File...
MD5
192.16...
c5e7c...
gerv.gun[1].octet-stream
LastWriteTime
6/27/2017 1:38 PM
MD5
1568dafae63eebce20987dd6205704e5
Name
gerv.gun[1].octet-stream
Path
/opt/networkminer/AssembledFiles/119.28.70.207/TCP-80/gerv.gun[1].octet-str
SHA1
2426f45f9dd85408e445710666ad41ce219e7146
SHA256
0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272
Size
241664
Reload Case Files
Buffered Frames to Parse:
Src IP:
Src Name:
Dst IP:
Dst Name:
Whois Query:
None
Src IP
Dst IP
IP
Source IP
Dest IP
Ver
HL
TOS
len
ID
Flags
Offset
TTL
TCP
Source Port
Dest Port
Seq #
Ack #
Offset
Res
Window
Urp
ChkSum
DATA
Search Packet Payload
Hex
Text
NoCase
analyst@SecOnion: ~
SGUIL-0.9.0 - Connected To lo...
NetworkMiner 2.4
gerv.gun[1].octet-stream
1 / 4

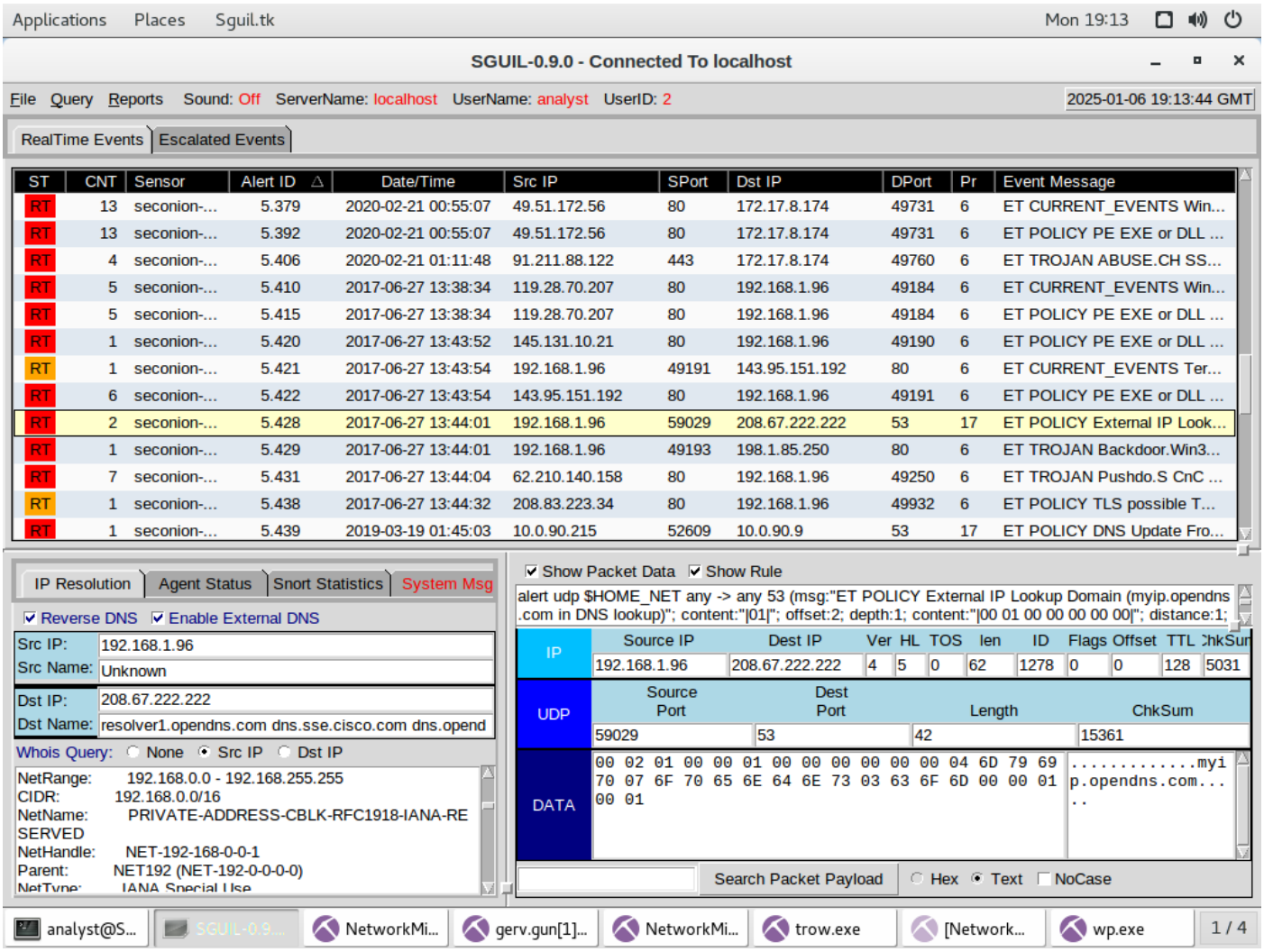

Applications
Places
Unknown
Mon 19:08
NetworkMiner 2.4
File
Tools
Help
2025-01-06 19:08:05 GMT
Hosts (2)
Files (1)
Images
Messages
Credentials
Sessions (1)
DNS
Parameters (15)
Keywords
Filter keyword:
Case sensitive
ExactPhrase
Any column
Clear
Apply
Frame nr.
Filename
Extension
Size
Source host
S. port
Destination ho
4
trow.exe
exe
330 752 B
145.131.10.21 [lounge-haarstudio.nl]
TCP 80
192.168.1.96
Case Panel
File...
MD5
192.16...
1d958...
trow.exe
LastWriteTime
6/27/2017 1:43 PM
MD5
fb75d4f81be51074bb4147e781e5b402
Name
trow.exe
Path
/opt/networkminer/AssembledFiles/145.131.10.21/TCP-80/oud/trow.exe
SHA1
55e512ebfe4f3a08a66c35500506837ad2c473c8
SHA256
94a0a09ee6a21526ac34c41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1
Size
330752
Reload Case Files
Buffered Frames to Parse:
Src IP:
Src Name:
Dst IP:
Dst Name:
Whois Query:
None
Src IP
Dst IP
IP
Source IP
Dest IP
Ver
HL
TOS
len
ID
Flags
Offset
TTL
TCP
Source Port
Dest Port
Seq #
Ack #
Offset
Res
Window
Urp
ChkSum
DATA
Search Packet Payload
Hex
Text
NoCase
analyst@SecOnio...
SGUIL-0.9.0 - Co...
NetworkMiner 2.4
gerv.gun[1].octet-...
NetworkMiner 2.4
trow.exe
1 / 4


Applications Places Unknown Mon 19:08
NetworkMiner 2.4
File Tools Help
2025-01-06 19:08:38 GMT
Hosts (2) Files (1) Images Messages Credentials Sessions (1) DNS Parameters (13) Keywords Anor
Filter keyword: Case sensitive ExactPhrase Any column Clear Apply
Frame nr. Filename Extension Size Source host S. port De
4 wp.exe exe 307 712 B 143.95.151.192 [vantagepointtechnologies.com] TCP 80 19
Case Panel
File... MD5
192.16... 9c1fe...
wp.exe
LastWriteTime 6/27/2017 1:43 PM
MD5 4da48f6423d5f7d75de281a674c2e620
Name wp.exe
Path /opt/networkminer/AssembledFiles/143.95.151.192/TCP-80/wp.exe
SHA1 93aa24323d60b2b053e158abf5a3e839f5ea58ae
SHA256 79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48
Size 307712
Reload Case Files
Buffered Frames to Parse:
Src IP:
Src Name:
Dst IP:
Dst Name:
Whois Query: None Src IP Dst IP
IP Source IP Dest IP Ver HL TOS len ID Flags Offset TTL ChkSum
TCP Source Port Dest Port U A P R S F R R R C S S Y I 1 0 G K H T N N Seq # Ack # Offset Res Window Urp ChkSum
DATA
Search Packet Payload Hex Text NoCase
analyst@S... SGUIL-0.9.... NetworkMi... gerv.gun[1]... NetworkMi... trow.exe NetworkMi... wp.exe 1 / 4


94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1
Sign in Sign up
66 / 72
Community Score -83
66/72 security vendors flagged this file as malicious
Reanalyze Similar More
94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1
Pedals.exe
Size 323.00 KB
Last Analysis Date 22 days ago
EXE
peexe runtime-modules spreader via-tor persistence checks-network-adapters malware suspicious-dns long-sleeps direct-cpu-clock-access detect-debug-environment
cve-2016-2569 cve-2005-0446 cve-2015-1729 exploit
DETECTION DETAILS RELATIONS ASSOCIATIONS BEHAVIOR COMMUNITY 24+
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.cutwail/wigon
Threat categories trojan dropper
Family labels cutwail wigon usvn
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3 Win-Trojan/Sagecrypt.Gen
Alibaba TrojanDropper:Win32/Cutwail.62278ef9
AliCloud Trojan:Win/Wigon.PL
ALYac Trojan.Injector
Antiy-AVL Trojan/Win32.Cutwail
Arcabit Trojan.Generic.D53FA53
Avast Win32:Malware-gen
AVG Win32:Malware-gen
Avira (no cloud) TR/FileCoder.JX
BitDefender Trojan.GenericKD.5503571
Bkav Pro W32.AIDetectMalware
CrowdStrike Falcon Win/malicious_confidence_100% (W)
CTX Exe.trojan.cutwail
Cylance Unsafe
Cynet Malicious (score: 99)
DeepInstinct MALICIOUS
DrWeb Trojan.DownLoad.64914
Elastic Malicious (high Confidence)


79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48
Sign in
Sign up
61
/ 71
Community Score
-12
61/71 security vendors flagged this file as malicious
Reanalyze
Similar
More
79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48
wp.exe
peexe
self-delete
persistence
malware
checks-user-input
corrupt
detect-debug-environment
checks-cpu-name
spreader
long-sleeps
Size
300.50 KB
Last Analysis Date
2 days ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 8
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.ursnif/nymaim
Threat categories trojan ransomware
Family labels ursnif nymaim cerber
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3 Trojan/Win32.Ursnif.R208257
Alibaba TrojanSpy:Win32/Ursnif.5e3f1e81
AliCloud Backdoor:Win/Ursnif.Gen
ALYac Trojan.Ransom.Cerber
Antiy-AVL Trojan[Spy]/Win32.Ursnif
Arcabit Generic.Nymaim.E.5FB90396
Avast Win32:Malware-gen
AVG Win32:Malware-gen
Avira (no cloud) HEUR/AGEN.1341699
BitDefender Generic.Nymaim.E.5FB90396
Bkav Pro W32.AIDetectMalware
CrowdStrike Falcon Win/malicious_confidence_100% (W)
CTX Exe.trojan.ursnif
Cylance Unsafe
Cynet Malicious (score: 99)
DeepInstinct MALICIOUS
DrWeb Trojan.Gozi.24
Elastic Malicious (high Confidence)


0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272
Sign in
Sign up
61
/ 72
Community Score
-266
61/72 security vendors flagged this file as malicious
Reanalyze
Similar
More
0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272
gerv.gun.octet-stream
peexe
runtime-modules
idle
direct-cpu-clock-access
spreader
checks-user-input
Size
236.00 KB
Last Analysis Date
6 days ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 20
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.shiotob/fragtor
Threat categories trojan banker ransomware
Family labels shiotob fragtor bebloh
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3 Win-Trojan/Sagecrypt.Gen
Alibaba TrojanBanker:Win32/Shiotob.d7033344
AliCloud Trojan[stealer]:Win/Banker.WQf66
ALYac Trojan.Ransom.LockyCrypt
Arcabit Trojan.Fragtor.D2A117
Avast Win32:Malware-gen
AVG Win32:Malware-gen
Avira (no cloud) TR/Crypt.ZPACK.cpqfb
BitDefender Gen:Variant.Fragtor.172311
Bkav Pro W32.AIDetectMalware
CrowdStrike Falcon Win/malicious_confidence_100% (W)
CTX Exe.trojan.banker
Cylance Unsafe
Cynet Malicious (score: 99)
DeepInstinct MALICIOUS
DrWeb Trojan.Siggen7.24391
Elastic Malicious (high Confidence)
Emsisoft Gen:Variant.Fragtor.172311 (B)


Applications Places Sguil.tk Mon 19:13
SGUIL-0.9.0 - Connected To localhost
File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2 2025-01-06 19:13:44 GMT
RealTime Events Escalated Events
ST CNT Sensor Alert ID Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 13 seconion-... 5.379 2020-02-21 00:55:07 49.51.172.56 80 172.17.8.174 49731 6 ET CURRENT_EVENTS Win...
RT 13 seconion-... 5.392 2020-02-21 00:55:07 49.51.172.56 80 172.17.8.174 49731 6 ET POLICY PE EXE or DLL ...
RT 4 seconion-... 5.406 2020-02-21 01:11:48 91.211.88.122 443 172.17.8.174 49760 6 ET TROJAN ABUSE.CH SS...
RT 5 seconion-... 5.410 2017-06-27 13:38:34 119.28.70.207 80 192.168.1.96 49184 6 ET CURRENT_EVENTS Win...
RT 5 seconion-... 5.415 2017-06-27 13:38:34 119.28.70.207 80 192.168.1.96 49184 6 ET POLICY PE EXE or DLL ...
RT 1 seconion-... 5.420 2017-06-27 13:43:52 145.131.10.21 80 192.168.1.96 49190 6 ET POLICY PE EXE or DLL ...
RT 1 seconion-... 5.421 2017-06-27 13:43:54 192.168.1.96 49191 143.95.151.192 80 6 ET CURRENT_EVENTS Ter...
RT 6 seconion-... 5.422 2017-06-27 13:43:54 143.95.151.192 80 192.168.1.96 49191 6 ET POLICY PE EXE or DLL ...
RT 2 seconion-... 5.428 2017-06-27 13:44:01 192.168.1.96 59029 208.67.222.222 53 17 ET POLICY External IP Look...
RT 1 seconion-... 5.429 2017-06-27 13:44:01 192.168.1.96 49193 198.1.85.250 80 6 ET TROJAN Backdoor.Win3...
RT 7 seconion-... 5.431 2017-06-27 13:44:04 62.210.140.158 80 192.168.1.96 49250 6 ET TROJAN Pushdo.S CnC ...
RT 1 seconion-... 5.438 2017-06-27 13:44:32 208.83.223.34 80 192.168.1.96 49932 6 ET POLICY TLS possible T...
RT 1 seconion-... 5.439 2019-03-19 01:45:03 10.0.90.215 52609 10.0.90.9 53 17 ET POLICY DNS Update Fro...
IP Resolution Agent Status Snort Statistics System Msg
Reverse DNS Enable External DNS
Src IP: 192.168.1.96
Src Name: Unknown
Dst IP: 208.67.222.222
Dst Name: resolver1.opendns.com dns.sse.cisco.com dns.opend
Whois Query: None Src IP Dst IP
NetRange: 192.168.0.0 - 192.168.255.255
CIDR: 192.168.0.0/16
NetName: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle: NET-192-168-0-0-1
Parent: NET192 (NET-192-0-0-0-0)
NetType: IANA Special Use
Show Packet Data Show Rule
alert udp $HOME_NET any -> any 53 (msg:"ET POLICY External IP Lookup Domain (myip.opendns.com in DNS lookup)"; content:"|01|"; offset:2; depth:1; content:"|00 01 00 00 00 00 00|"; distance:1;
IP Source IP Dest IP Ver HL TOS len ID Flags Offset TTL ChkSum
192.168.1.96 208.67.222.222 4 5 0 62 1278 0 0 128 5031
UDP Source Port Dest Port Length ChkSum
59029 53 42 15361
DATA
00 02 01 00 00 01 00 00 00 00 00 00 04 6D 79 69
70 07 6F 70 65 6E 64 6E 73 03 63 6F 6D 00 00 01
00 01
.....myi
p.opendns.com...
..
Search Packet Payload Hex Text NoCase
analyst@S... SGUIL-0.9... NetworkMi... gerv.gun[1]... NetworkMi... trow.exe [Network... wp.exe 1 / 4

Part 1: Gather the Basic Information

Step 2: Gather basic information.

a. Identify the time frame of the Pushdo Trojan attack, including the date and approximate time.

2017-06-27 from 13:38:34 to 13:44:32

b. List the alerts noted during this time frame associated with the trojan.

ET CURRENT_EVENTS WinHttpRequest Downloading EXE
ET POLICY PE EXE or DLL Windows file download HTTP
ET POLICY PE EXE or DLL Windows file download HTTP
ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile
ET POLICY PE EXE or DLL Windows file download HTTP
ET POLICY External IP Lookup Domain (myip.opendns .com in DNS lookup)
ET TROJAN Backdoor.Win32.Pushdo.s Checkin
ET TROJAN Pushdo.S CnC response
ET POLICY TLS possible TOR SSL traffic

c. List the internal IP addresses and external IP addresses involved.

Internal IP address:

- 192.168.1.96

External IP addresses:

- 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: Learn about the Exploit

Step 1: Infected host

a. Based on the alerts, what is the IP and MAC addresses of the infected computer? Based on the MAC address, what is the vendor of the NIC chipset?

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

b. Based on the alerts, when (date and time in UTC) and how was the PC infected?

2017-06-27 13:38:32 UTC
Through the **Pushdo Trojan, gerv.gun** malware got executed.

How did the malware infect the PC?

The user on the PC with the IP address 192.168.1.96 accessed a malicious domain, leading to the installation of malware through the Pushdo trojan. Pushdo is classified as a "downloader" trojan, designed specifically to download and install additional malicious software. Once executed, Pushdo communicates with one of several control server IP addresses embedded in its code. These servers operate on TCP port 80 and mimic Apache web servers. If an HTTP request contains the correct parameters, the server delivers one or more executable files via HTTP. The specific malware downloaded by Pushdo is determined by the value appended to the "s-underscore" segment of the URL.

Pushdo also collects and tracks various details about the victim system, including the IP address, whether the user is an administrator, the primary hard drive's serial number (retrieved using the SMART_RCV_DRIVE_DATA IO control code), whether the filesystem is NTFS, how many times a variant of Pushdo has been executed on the system, and the Windows OS version, as obtained via the GetVersionEx API call.

Step 2: Examine the exploit.

a. Based on the alerts associated with HTTP GET request, what files were downloaded? List the malicious domains observed and the files downloaded.

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

Use any available tools in Security Onion VM, determine and record the SHA256 hash for the downloaded files that probably infected the computer?

gerv.gun = 0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272
trow.exe = 94a0a09ee6a21526ac34d41eabf4ba603e9a30c26e6a1dc072ff45749dfb1fe1
wp.exe = 79d503165d32176842fe386d96c04fb70f6ce1c8a485837957849297e625ea48

b. Navigate to www.virustotal.com, input the SHA256 hash to determine if these were detected as malicious files. Record your findings, such as file type and size, other names, and target machine. You can also include any information that is provided by the community posted in VirusTotal.

gerv.gun:

- 58 engines detected this file
- File type: Win32 EXE
- File size: 236.00 KB (241664 bytes)
- Names:
    - gerv.gun
    - test
    - tmp523799.697
    - tmp246975.343
    - tmp213582.420
    - extract-1498570714.111294-HTTP-FG0jno3bJLiIzR4hrh.exe
    - 0931537889c35226d00ed26962ecacb140521394279eb2ade7e9d2afcf1a7272.bin
    - vector.tui
- Target Machine: Intel 386 or later processors and compatible processors

trow.exe:

- 63 engines detected this file
- File type: Win32 EXE
- File size: 323.00 KB (330752 bytes)
- Names:
    - Pedals
    - Pedals.exe
    - trow.exe
    - test3
    - 2017-06-28_18-18-14.exe
    - bma2beo4.exe
- Target Machine: Intel 386 or later processors and compatible processors

wp.exe:

- 55 engines detected this file

- File type: Win32 EXE
- File size: 300.50 KB (307712 bytes)
- Names:
    - wp.exe
    - test2
    - test_3
    - 4da48f6423d5f7d75de281a674c2e620.virobj
    - wp.exe.x-msdownload
- Target Machine: Intel 386 or later processors and compatible processors

c. Examine other alerts associated with the infected host during this timeframe and record your findings

ET POLICY External IP Lookup Domain (myip.opendns .com in DNS lookup) – infection started when the user of the **192.168.1.96** host performed a DNS lookup through a malicious domain – destination IP: **208.67.222.222**

Step 3: Report Your Findings

A Windows PC with the IP address 192.168.1.96 accessed a malicious domain for a DNS query and became infected with the Pushdo trojan. Pushdo operates by mimicking an Apache web server, listening on port 80. After infection, it proceeds to download and install additional malware. On the compromised PC, three malicious files were downloaded and installed: *gerv.gun*, *trow.exe*, and *wp.exe*. These files were analyzed on VirusTotal.com using their SHA256 hashes, where they were confirmed as malware by the majority of sources.