

Writing IDS Signatures for Suricata and Snort

Jack Mott and Jason Williams



Who are we?

Jack Mott

- Security Research Analyst
 - Emerging Threats now part of Proofpoint
- Malware analysis
 - Ransomware and exploit kits are my favorite
- IDS Signature development
 - ETPRO/OPEN Rulesets
- ClamAV Signature Development
- OISF Core Training Team Member



Jae Williams

- Security Research Analyst
 - Emerging Threats now part of Proofpoint
- Malware analysis
 - Oddball targeted/exploit/vuln stuff
- IDS Signature development
 - ETPRO/OPEN Rulesets
- Phishing
- OISF Core Training Team Member



What is the point of this?

- Introduction to IDS rule language
- Be comfortable interpreting IDS rules
- Feel empowered to write IDS rules
- Be knowledgeable on detecting threats on the network

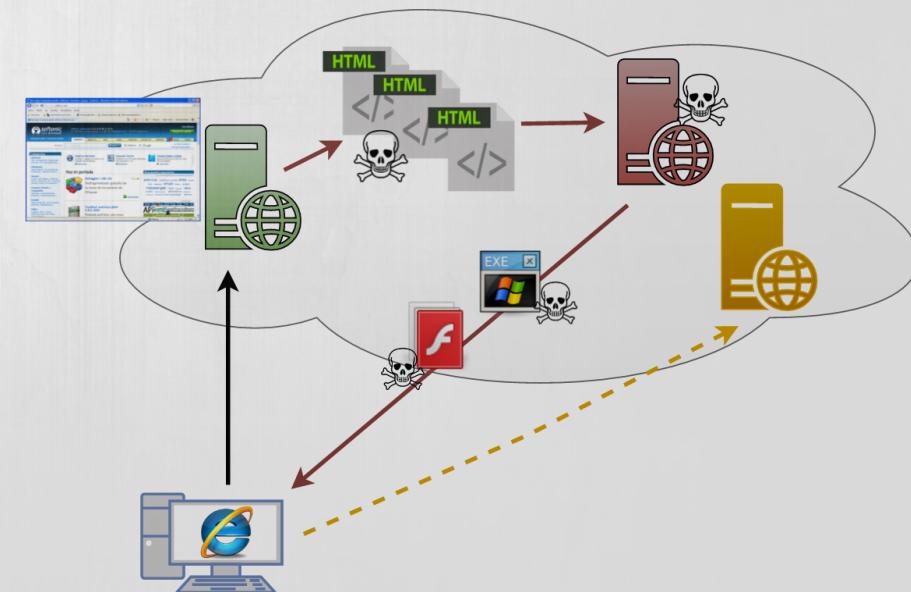


Network Analysis Basics



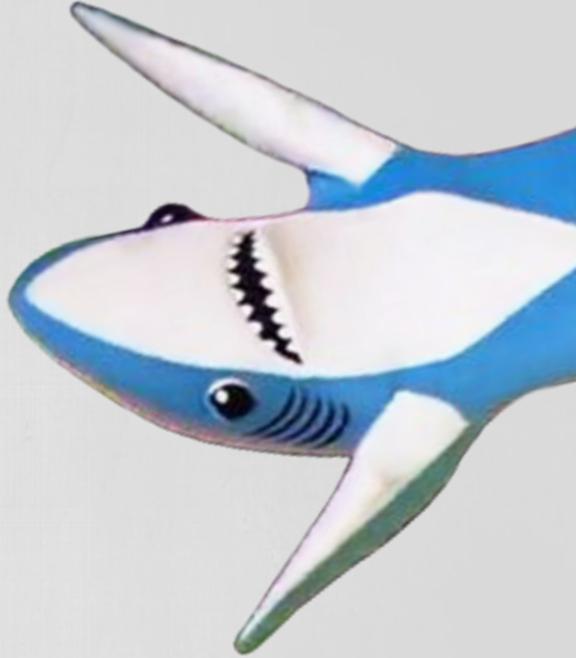
Network Traffic Analysis

- A basic understanding of TCP/IP
- Not enough time to dig into low-level stuff here
- We can talk about some tools
- Basic network traffic analysis techniques



Wireshark

- The best tool out there for graphical packet analysis
- Views & Column Layout
- Wireshark -> Preferences
 - Ability to add custom fields by clicking “+” and entering a filter (e.g http.response.code)
 - Arrange packet data layout for ease of analysis under “Layout” and chose a configuration



Wireshark - Appearance

The screenshot shows the Wireshark configuration interface with the 'Appearance' section selected. The 'Columns' tab is active, displaying a list of columns used in the packet list view. The columns are listed in rows with columns for 'Displayed', 'Title', 'Type', 'Field Name', and 'Field Occur'. Most columns have a checked checkbox in the 'Displayed' column.

Displayed	Title	Type	Field Name	Field Occur
<input checked="" type="checkbox"/>	No.	Number		
<input checked="" type="checkbox"/>	Time	Time (format as specified)		
<input checked="" type="checkbox"/>	Source	Source address		
<input checked="" type="checkbox"/>	SrcPort	Src port (resolved)		
<input checked="" type="checkbox"/>	Host	Custom	http.host	0
<input checked="" type="checkbox"/>	Destination	Destination address		
<input checked="" type="checkbox"/>	DstPort	Dest port (resolved)		
<input checked="" type="checkbox"/>	Protocol	Protocol		
<input checked="" type="checkbox"/>	Stat	Custom	http.response.code	0
<input checked="" type="checkbox"/>	Length	Packet length (bytes)		
<input checked="" type="checkbox"/>	Info	Information		

Wireshark - Appearance - Layout

Appearance

Layout

Columns

Appearance

Layout

Columns

Font and Colors

Capture

Filter Expressions

Name Resolution

Protocols

Statistics

Advanced

Displayed	Title	Type	Field Name	Field Occurr
<input checked="" type="checkbox"/>	No.	Number		

Pane 1:

Packet List

Packet Details

Packet Bytes

None

Show packet separator on Packet List

Pane 2:

Packet List

Packet Details

Packet Bytes

None

Pane 3:

Packet List

Packet Details

Packet Bytes

None

1 2 3

1 2 3

1 2
3

1
2 3

1
2
3

1 2
3

1 2
3

1 2 3

1 2 3

Wireshark - File Extraction (1)

Built in ability to parse PCAP for known HTTP, SMB/2, DICOM and TFTP objects (File -> Export Objects)

Filter: http.request							▼	Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info					
35	18.518048	172.16.130.140	104.168.188.170	HTTP	136	GET /~trehbaof/ass.exe HTTP/1.1					
276	25.292109	172.16.130.140	64.182.208.181	HTTP	117	GET / HTTP/1.1					
287	26.957915	172.16.130.140	173.194.77.104	HTTP	118	GET / HTTP/1.1					
346	27.681173	172.16.130.140	104.168.188.170	HTTP	927	POST /~trehbaof/insert_data_23481					
352	37.076603	172.16.130.140	173.194.77.104	HTTP	94	GET / HTTP/1.1					
410	37.331126	172.16.130.140	104.168.188.170	HTTP	357	POST /~trehbaof/update_data_23481					
418	48.626913	172.16.130.140	173.194.77.104	HTTP	94	GET / HTTP/1.1					

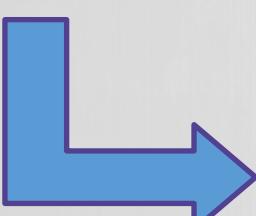
Wireshark - File Extraction (2)

Filter: http.request Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
35	18.518048	172.16.130.140	104.168.188.170	HTTP	136	GET /~trehbaof/ass.exe HTTP/1.1
276	25.292109	172.16.130.140	64.182.208.181	HTTP	117	GET / HTTP/1.1
287	26.957915	172.16.130.140	173.194.77.104	HTTP	118	GET / HTTP/1.1
346	27.681173	172.16.130.140	104.168.188.170	HTTP	927	POST /~trehbaof/insert_data_23481f98_f663_4689_8e0a_be2
352	37.076603	172.16.130.140	173.194.77.104	HTTP	94	GET / HTTP/1.1
410	37.33					
418	48.62					

Wireshark: HTTP object list

Packet num	Hostname	Content Type	Size	Filename
262	104.168.188.170	application/x-msdownload	241 kB	ass.exe
278	icanhazip.com	text/plain	14 bytes	\
338	www.google.com	text/html	49 kB	\
346	104.168.188.170	application/x-www-form-urlencoded	873 bytes	insert_data_23481f98_f663_4689_8e0a_be2



Wireshark - File Extraction (3)

Filter: http.request Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
35	18.518048	172.16.130.140	104.168.188.170	HTTP	136	GET /~trehbaof/ass.exe HTTP/1.1
276	25.292109	172.16.130.140	64.182.208.181	HTTP	117	GET / HTTP/1.1
287	26.957915	172.16.130.140	173.194.77.104	HTTP	118	GET / HTTP/1.1
346	27.681173	172.16.130.140	104.168.188.170	HTTP	927	POST /~trehbaof/insert_data_234811
352	37.076603	172.16.130.140	173.194.77.104	HTTP	94	GET / HTTP/1.1
410	37.333333					
418	48.622222					

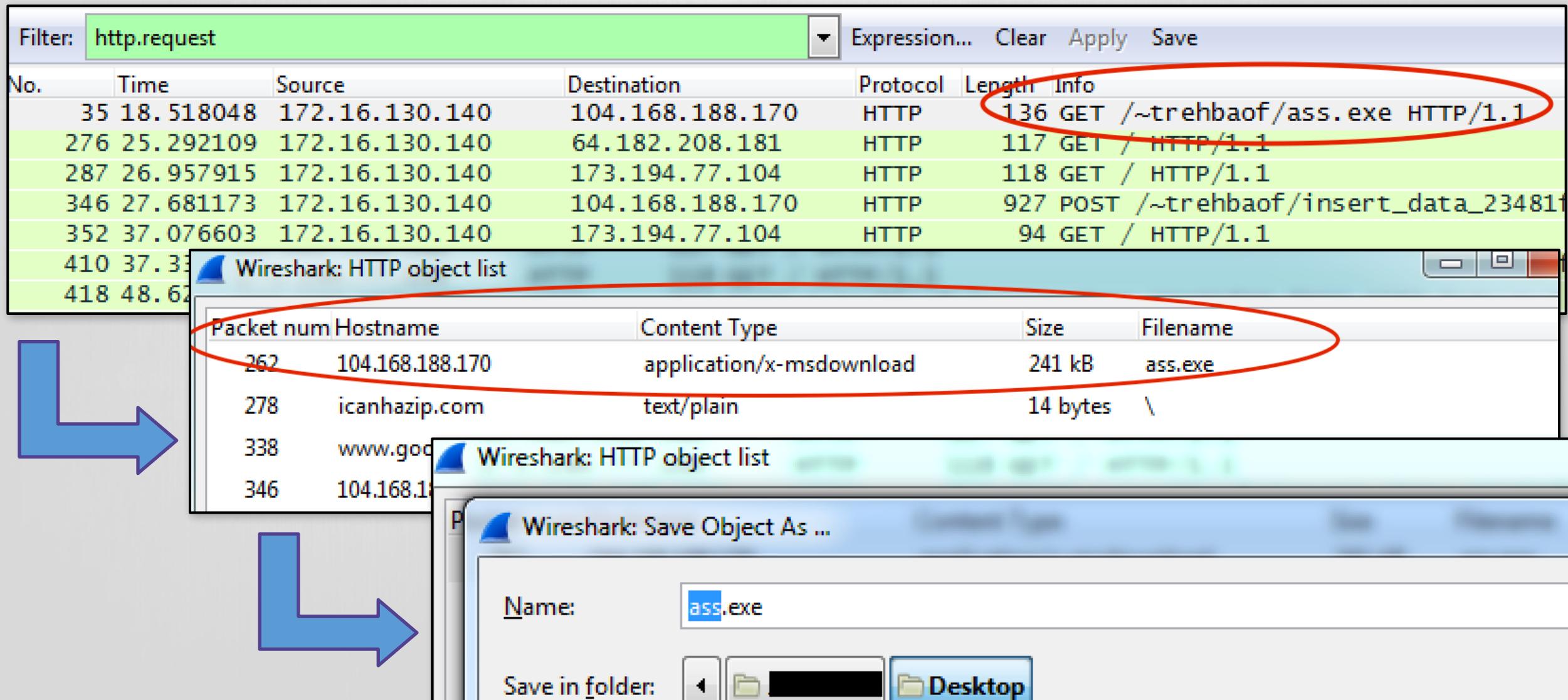
Wireshark: HTTP object list

Packet num	Hostname	Content Type	Size	Filename
262	104.168.188.170	application/x-msdownload	241 kB	ass.exe
278	icanhazip.com	text/plain	14 bytes	\
338	www.goo			
346	104.168.188.170			

Wireshark: Save Object As ...

Name: ass.exe

Save in folder: Desktop



Wireshark - Following Streams

- Ability to assemble TCP/HTTP streams to view session data
- Default view is ASCII, can change to Hex (useful) and other encodings
- Right click packet of interest -> Follow -> TCP (HTTP) Stream

Wireshark · Follow TCP Stream (tcp.stream eq 3) · shades

```
POST /~trehbaof/insert_data_23481f98_f663_4689_8e0a_be27b269582b.php?pass=q1w2e3r4r4e3w2q1 HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: 104.168.188.170
Content-Length: 873
Expect: 100-continue
Connection: Keep-Alive

pc_name=JIMJONES-PC&pc_username=Jim+Jones&ip_address=108.61.228.19&key_unlock=K57jA%24%24CzCsssJz%24B%5e%5eD%25%5ex
%5e9zjD13KKK1zzx87Aj8%246Vu2Vn2eQjBz9Q3wKio87IQR09d9%2boe37BWzSmsRfjGLRgONIN0nksgvnY%2fId0trKAA40ClpTfkJ8vYEgADFOWN9CofeV52K
%2bkgWERDMCjXbvOB40WwEIYzmY9IZK3qT8%2fP02v1VP1v34DQ8QI3f1FcAqNC6GA%2bXHPbF9g%3dCbY6XEJ%2byszw7ZIk0lsPDDmcjyWdy3XPXdpywVIfNc
%2fnWHeLQTTr0W9xY4Q%2bVMEhgATUKbj%2bABKGMyGI8miXcp8Sr8IqgSqqIPrgFGbaq2CUqNYBg5c%2boNCPe%2bErjc95LYwH12g2VJD5mETdmbjG2u44DYI
%3d&id_victim=d3RMoQKyc%2bIV0gVIUUmNJ8l06i1i2dCY6wYdIbR05kuPquy0yen7gaZG%2bc1lq7ranabSgePCPmKMcutfHgsEoQq0QolUks9B9%2fzR11
%2fawC7awaErz7qLdN9Wg0NB9coMBBSdLRumUnNZNBE7GlSTvkKaBvLqnahoLvoE%2fWBrL0kR4kqIH53PVTEviAUNoh4R9YkE0%2ftC98g2SdzxFMa%2f8
%2fiTDY1Ai9C07Bn3WT&time_locked=6%2f6%2f2016+9%3a54%3a55+AM&total_files_locked=0&reference=YoutubeHTTP/1.1 200 OK
```



Wireshark - Filters

- Filters are entered in the top bar and are limited to specific search parameters
- Can use qualifiers like `&&`, `!=`, `==`, `||`, `<=`, `>`

The screenshot shows the 'Display Filter Expression' dialog box in Wireshark. The title bar reads 'Wireshark · Display Filter Expression'. The dialog is divided into two main sections: 'Field Name' on the left and 'Relation' on the right.

Field Name:

- HTTP · Hypertext Transfer Protocol
 - http.accept · Accept
 - http.accept_encoding · Accept Encoding
 - http.accept_language · Accept-Language
 - http.authbasic · Credentials
 - http.authcitrix · Citrix AG Auth
 - http.authcitrix.domain · Citrix AG Domain
 - http.authcitrix.password · Citrix AG Password
 - http.authcitrix.session · Citrix AG Session ID

Relation:

- is present
- `==`
- `!=`
- `>`
- `<`
- `>=`
- `<=`

In the bottom text input field, the filter expression `http.request.method == POST && !http.user_agent` is entered. A small icon of a blue bookmark is positioned to the left of the input field. Below the input field, the word 'matches' is visible.

Network Analysis

- Use tools to your advantage - NSM!
- Proactive detection is hard, but can be fruitful
- Use your day-one knowledge of pattern recognition to your advantage!
- Look at small datasets and refine as you increase the size
- Baseline, baseline, baseline (do your best...)

Why IDS/IPS?

- Still an extremely valuable tool in your arsenal
- Applicable when discussing defense in depth
- Not perfect
- Provide context
- What can full PCAP provide?



IDS Rule Theory

- Generally, we want agile but effective rules
 - Don't be like generic AV names and hash-based detections
- Specific enough to capture desired traffic without False Negatives
- Loose enough to capture variants without False Positives
- Balance!
- Won't always work this way 😞

IDS Landscape

- Suricata (<https://suricata-ids.org/>)
 - Open-source, community driven
 - Multi-threaded for fast performance
 - Robust protocol identification (can parse HTTP on off-ports, etc)
 - More than just IDS - NSM! Lua! File Extraction!
- Snort (<https://snort.org/>)
 - Most influential IDS developed
 - Open-source
 - Developed/maintained by Sourcefire, now part of Cisco/Talos
- <http://suricata.readthedocs.io/en/latest/rules/differences-from-snort.html>



A word about (the common) rulesets

Emerging Threats

- ET OPEN
 - <https://rules.emergingthreats.net/open/>
- ETPRO
 - [Paid](#)

Talos (Cisco/VRT/Snort)

- Community
 - <https://snort.org/downloads/#rule-downloads>
- Snort Subscriber Ruleset
 - [Paid](#)



What is an IDS rule?

```
POST /generate.php HTTP/1.1
User-Agent: DetoxCrypto2
Content-Type: application/x-www-form-urlencoded
Host: detoxcrypto.net16.net
Content-Length: 26
Expect: 100-continue
Connection: Keep-Alive
```

```
publickey=sdJoFsAv3jSNMEYxHTTP/1.1 200 OK
Date: Sat, 13 Aug 2016 04:45:30 GMT
Server: Apache
X-Powered-By: PHP/5.2.17
Content-Length: 186
Connection: close
Content-Type: text/html
```

```
MQoxjmeGRPHGh2GVdFSPHnycHwL5i7Z4
<!-- Hosting24 Analytics Code -->
<script type="text/javascript" src="http://stats.hosting24.com/count.php"></script>
<!-- End Of Analytics Code -->
```

What is an IDS rule?

Suricata

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"DetoxCrypto Ransomware CnC Activity"; flow:established,to_server; content:"POST"; http_method; content:"/generate.php"; http_uri; content:"DetoxCrypto"; fast_pattern; http_user_agent; content:"publickey="; depth:10; http_client_body; content:!\"Referer|3a|"; http_header; pcre:"/\.\php$/U"; reference:md5,e273508a2f2ed45c20a2412f7d62eceb; classtype:trojan-activity; sid:1000000001; rev:1;)
```

Snort

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ETPRO TROJAN DetoxCrypto Ransomware CnC Activity"; flow:established,to_server; content:"POST"; http_method; content:"/generate.php"; http_uri; content:"User-Agent|3a 20|DetoxCrypto"; fast_pattern:3,20; http_header; content:"publickey="; depth:10; http_client_body; content:!\"Referer|3a|"; http_header; pcre:"/\.\php$/U"; reference:md5,e273508a2f2ed45c20a2412f7d62eceb; sid:1000000001; rev:1;)
```

Rule Foundations



IDS Rule Basic Format

action protocol from_ip port -> to_ip port

(msg:"something"; content:"something";

content:"something else"; sid:10000000; rev:1;)

IDS Rule Basic Format

```
action protocol from_ip port -> to_ip port
```

```
(msg:"something"; content:"something";
```

```
content:"something else"; sid:10000000; rev:1;)
```

IDS Rule Basic Format

```
action protocol from_ip port -> to_ip port
```

```
(msg:"something"; content:"something";
```

```
content:"something else"; sid:10000000; rev:1;)
```

IDS Rule Basic Format

```
action protocol from_ip port -> to_ip port
```

```
(msg:"something"; content:"something";
```

```
content:"something else"; sid:10000000; rev:1;)
```

Rule Action

- Tells the IDS engine what to do when traffic matches this rule
- alert
 - Generate alert, and log matching packets, but let the traffic through
- log
 - Log traffic- no alert
- pass
 - Ignore the packet, allow it through
- drop
 - If IPS mode, sensor should drop the offending packet
- reject
 - IDS will send TCP reset packet

Rule Action

- Tells the IDS engine what to do when traffic matches this rule
- alert
 - Generate alert, and log matching packets, but let the traffic through

```
action protocol from_ip port -> to_ip port (msg:"something";  
content:"something"; content:"something else"; sid:10000000; rev:1;)
```

- If IPS mode, sensor should drop the offending packet
- reject
 - IDS will send TCP reset packet

Rule Protocol

- Suricata and Snort have the ability to detect specific protocols declared by the rule writer
- tcp
- udp
- icmp
- ip
- http (Suricata only)
- tls (Suricata only)

Rule Protocol

- Suricata and Snort have the ability to detect specific protocols
~~declared by the rule writer~~

```
action protocol from_ip port -> to_ip port (msg:"something";  
content:"something"; content:"something else"; sid:10000000; rev:1;)
```

- ip
- http (Suricata only)
- tls (Suricata only)

Rule Hosts Variables

- This is how you declare who is sending traffic to who
- Configurable via suricata.yaml and snort.conf
 - Contains defaults, but double check them
- \$HOME_NET
 - Refers to internal networks, specified in the conf/yaml
- \$EXTERNAL_NET
 - Not \$HOME_NET, or what you choose in conf/yaml
- \$HTTP_SERVERS, \$SMTP_SERVERS, etc...
- Single IP

Rule Hosts Variables

- This is how you declare who is sending traffic to who

```
action protocol from_ip port -> to_ip port (msg:"something";  
content:"something"; content:"something else"; sid:10000000; rev:1;)
```

- \$EXTERNAL_NET
 - Not \$HOME_NET, or what you choose in conf/yaml
- \$HTTP_SERVERS, \$SMTP_SERVERS, etc...
- Single IP

Rule Direction

- Simply stated by an arrow: ->
- This tells the engine what direction traffic is flowing between hosts
- Traffic from internal host -> outbound
 - \$HOME_NET any -> \$EXTERNAL_NET any
- Traffic from external host -> inbound
 - \$EXTERNAL_NET -> \$HOME_NET any
- Can be bidirectional by using: <>
 - \$EXTERNAL_NET any <> \$HOME_NET any

Rule Direction

- Simply stated by an arrow: ->

```
action protocol from_ip port -> to_ip port (msg:"something";
content:"something"; content:"something else"; sid:10000000; rev:1;)
```

- Traffic from external host -> inbound
 - \$EXTERNAL_NET -> \$HOME_NET any
- Can be bidirectional by using: <>
 - \$EXTERNAL_NET any <> \$HOME_NET any

Rule Ports

- Used in tandem with the src/dst host variables
- Declares the port in which traffic for this rule will be evaluated
 - alert tcp \$HOME_NET any -> \$EXTERNAL_NET 9003
- Like the Hosts variables, ports may have variables as well
 - \$HTTP_PORTS, \$SMTP_PORTS, \$FTP_PORTS, etc...
 - Configurable in conf/yaml
- Ports may be negated by placing a ! In front of it
 - \$EXTERNAL_NET !80

Rule Ports (cont...)

- Ports may be expressed in various ways
 - Single port
 - 80
 - Multiple ports
 - [80,8080,443,9000]
 - Port ranges
 - [8000:9000]
 - Combination
 - \$HOME_NET [1024:] -> \$EXTERNAL_NET [80,800,6667:6669,!200]
 - What does this say?

Rule Ports (cont...)

- Ports may be expressed in various ways

~~Single port~~

```
action protocol from_ip port -> to_ip port (msg:"something";  
content:"something"; content:"something else"; sid:10000000; rev:1;)
```

- [8000:9000]
- Combination
 - \$HOME_NET [1024:] -> \$EXTERNAL_NET [80,800,6667:6669,!200]
 - What does this say?

Exercise – Rule Foundations

Source	SrcPort	Host	Destination	DstPort	Protocol	Stat	Length	Info
192.168.4.151	49689		137.74.223.62	80	TCP		0	49689→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1464 WS=4
137.74.223.62	80		192.168.4.151	49689	TCP		0	80→49689 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MS
192.168.4.151	49689		137.74.223.62	80	TCP		0	49689→80 [ACK] Seq=1 Ack=1 Win=65900 Len=0
192.168.4.151	49689	free.diendancacanh.net	137.74.223.62	80	HTTP		336	GET /radio/sometime-estate-sleepy-10006700 HTTP/1.
137.74.223.62	80		192.168.4.151	49689	TCP		0	80→49689 [ACK] Seq=1 Ack=337 Win=30336 Len=0
137.74.223.62	80		192.168.4.151	49689	TCP		1318	[TCP segment of a reassembled PDU]
137.74.223.62	80		192.168.4.151	49689	TCP		1209	[TCP segment of a reassembled PDU]
192.168.4.151	49689		137.74.223.62	80	TCP		0	49689→80 [ACK] Seq=337 Ack=1319 Win=65900 Len=0
137.74.223.62	80		192.168.4.151	49689	HTTP	200	5	HTTP/1.1 200 OK (text/html)

alert ____ \$ _____ -> \$ _____

Exercise – Rule Foundations

Source	SrcPort	Host	Destination	DstPort	Protocol	Stat	Length	Info
192.168.4.151	49689		137.74.223.62	80	TCP		0	49689→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1464 WS=4
137.74.223.62	80		192.168.4.151	49689	TCP		0	80→49689 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MS
192.168.4.151	49689		137.74.223.62	80	TCP		0	49689→80 [ACK] Seq=1 Ack=1 Win=65900 Len=0
192.168.4.151	49689	free.diendancacanh.net	137.74.223.62	80	HTTP		336	GET /radio/sometime-estate-sleepy-10006700 HTTP/1.
137.74.223.62	80		192.168.4.151	49689	TCP		0	80→49689 [ACK] Seq=1 Ack=337 Win=30336 Len=0
137.74.223.62	80		192.168.4.151	49689	TCP		1318	[TCP segment of a reassembled PDU]
137.74.223.62	80		192.168.4.151	49689	TCP		1209	[TCP segment of a reassembled PDU]
192.168.4.151	49689		137.74.223.62	80	TCP		0	49689→80 [ACK] Seq=337 Ack=1319 Win=65900 Len=0
137.74.223.62	80		192.168.4.151	49689	HTTP	200	5	HTTP/1.1 200 OK (text/html)

Suricata

```
alert http $HOME_NET any -> $EXTERNAL_NET any
```

Snort

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS
```

Exercise – Rule Foundations

Source	SrcPort	Host	Destination	DstPort	Protocol	Stat	Length	Info
10.0.2.15	1052		84.108.128.25	27132	TCP		0	1052→27132 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
84.108.128.25	27132		10.0.2.15	1052	TCP		0	27132→1052 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
10.0.2.15	1052		84.108.128.25	27132	TCP		0	1052→27132 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10.0.2.15	1052		84.108.128.25	27132	TCP		8	1052→27132 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=8
84.108.128.25	27132		10.0.2.15	1052	TCP		0	27132→1052 [ACK] Seq=1 Ack=9 Win=65535 Len=0
10.0.2.15	1052		84.108.128.25	27132	TCP		0	1052→27132 [RST, ACK] Seq=9 Ack=1 Win=0 Len=0

alert ____ \$_____ -> \$_____ _____

Exercise – Rule Foundations

Source	SrcPort	Host	Destination	DstPort	Protocol	Stat	Length	Info
10.0.2.15	1052		84.108.128.25	27132	TCP		0	1052→27132 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S/
84.108.128.25	27132		10.0.2.15	1052	TCP		0	27132→1052 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
10.0.2.15	1052		84.108.128.25	27132	TCP		0	1052→27132 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10.0.2.15	1052		84.108.128.25	27132	TCP		8	1052→27132 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=8
84.108.128.25	27132		10.0.2.15	1052	TCP		0	27132→1052 [ACK] Seq=1 Ack=9 Win=65535 Len=0
10.0.2.15	1052		84.108.128.25	27132	TCP		0	1052→27132 [RST, ACK] Seq=9 Ack=1 Win=0 Len=0

alert tcp \$HOME_NET any -> \$EXTERNAL_NET any

Exercise – Rule Foundations

Source	SrcPort	Host	Destination	DstPort	Protocol	Stat	Length	Info
10.0.25.10	1032		143.215.130.30	53	DNS			Standard query 0x9491 A ErnestRodgerRamsey.com
143.215.130.30	53		10.0.25.10	1032	DNS			Standard query response 0x9491 A ErnestRodgerRamsey.com A

alert ____ \$______ _____ -> \$_____ _____

Exercise – Rule Foundations

Source	SrcPort	Host	Destination	DstPort	Protocol	Stat	Length	Info
10.0.25.10	1032		143.215.130.30	53	DNS			Standard query 0x9491 A ErnestRodgerRamsey.com
143.215.130.30	53		10.0.25.10	1032	DNS			Standard query response 0x9491 A ErnestRodgerRamsey.com A

alert udp \$HOME_NET any -> any 53

Rule Message

- msg:"DetoxCrypto Ransomware CnC Activity";
 - Not the flavor
- Arbitrary text that appears when the rule fires and is logged/alert
- Consistency is key
- Consider adding:
 - Malware architecture: Win32/64, MSIL, ELF, OSX, etc
 - Malware family/name: njRAT, Locky, CryptXXX, Zeus
 - Malware action: Checkin, Activity, Key Exchange, Heartbeat, Exfil

Rule Message - Exercise

- msg:"Zeus Variant Checkin";



- msg:"IP Backup";



- msg:"Unknown Exploit Kit Plugin Check";



- msg:"CnCtivity";



Flow

- Declare the originator and responder in the conversation
- Most rules we will write, we want to have the engine looking at “established” tcp sessions
- `flow:<established>,<to_server|to_client>;`
 - can also use `from_server`, `from_client`
- `alert tcp $HOME_NET any -> $EXTERNAL_NET any`
 - `flow:established,to_server;`
- If protocol is UDP, can use direction
 - `flow:from_server;`



Dsize

- Allows rule writer to match using the size of the packet payload (not http)
- Based on TCP segment length, NOT total packet length
 - Wireshark filter: tcp.len
- `dszie:<number>;`
- Can be represented as single number, range, greater than, or less than
 - `dszie:312;`
 - `dszie:<300;`
 - `dszie:>300;`
 - `dszie:300<>400;`

Rule Content

- The most basic building block for pattern matching
- Matching unique content in packets for detection
- Careful on what you choose
- **Must use hex for certain characters**
 - ; “ :
- content:"some thing";
- content:"some|20|thing";
- content:"User-Agent|3a 20|";
- content:"s|00|o|00|m|00|e|00|t|00|h|00|i|00|n|00|g";

Rule Content (cont...)

```
POST /generate.php HTTP/1.1
User-Agent: DetoxCrypto2
Content-Type: application/x-www-form-urlencoded
Host: detoxcrypto.net16.net
Content-Length: 26
Expect: 100-continue
Connection: Keep-Alive

publickey=$dJoFsAv3jSNMEYxHTTP/1.1 200 OK
Date: Sat, 13 Aug 2016 04:45:30 GMT
Server: Apache
X-Powered-By: PHP/5.2.17
Content-Length: 186
Connection: close
Content-Type: text/html

MQoxjmeGRPHGh2GVdFSPHnycHwL5i7Z4
<!-- Hosting24 Analytics Code -->
<script type="text/javascript" src="http://stats.hosting24.com/count.php"></script>
<!-- End Of Analytics Code -->
```

Rule Content (cont...)

- content:"POST";
- content:"/generate.php";
- content:"User-Agent|3a 20|DetoxCrypto";
 - Same as “User-Agent: DetoxCrypto”
- content:"publickey=";

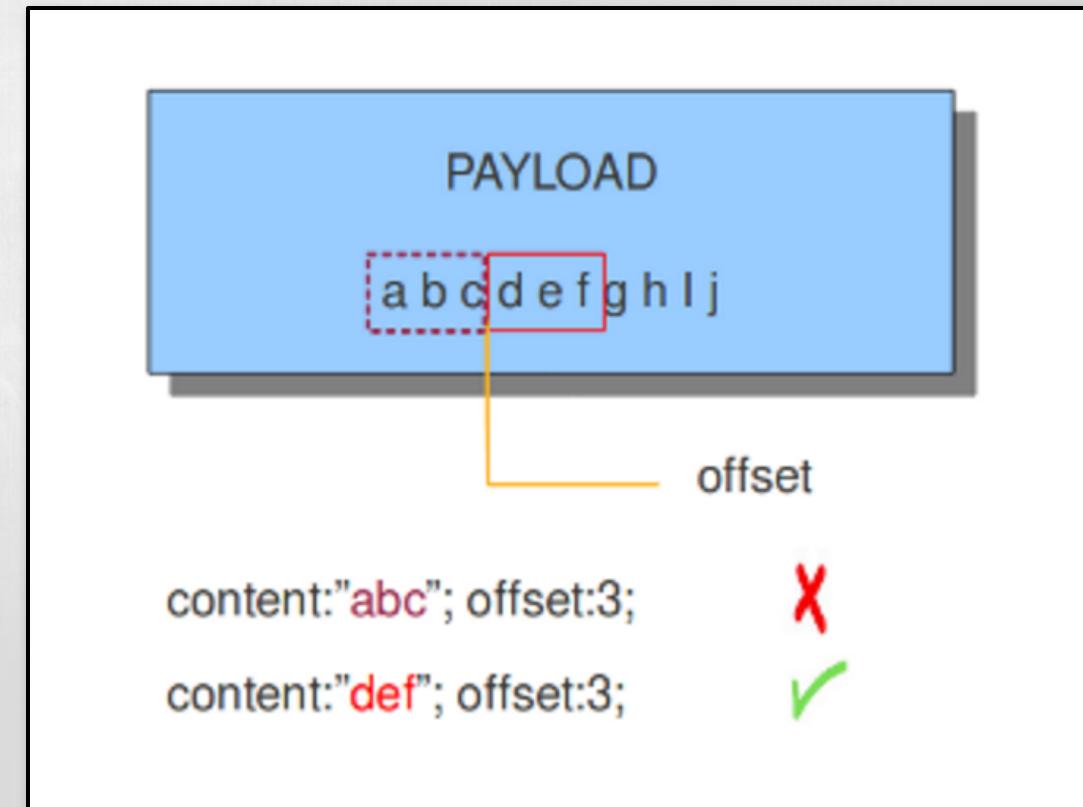
Rule Options

- Now that we have some content to match on, we can also add modifiers to assist in detection
- These can help the engine in finding exactly where content should be found
- Efficiency
- Accuracy



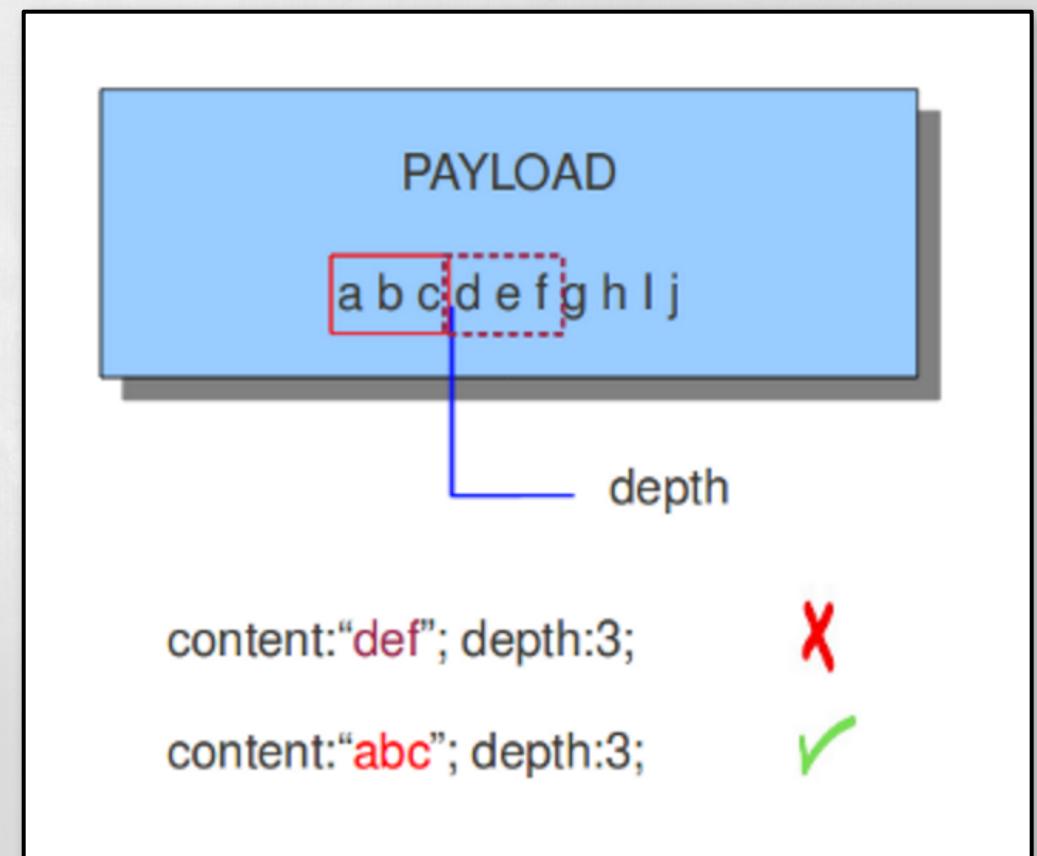
Offset

- Tells the engine to “go this far into the packet and start matching”
- `content:"blah"; offset:5;`
- Used in conjunction with “depth”



Depth

- Tells the engine how “deep” into the packet the content should be found
- content:”blah”; depth:4;
- Assumes offset:0; if not given



Offset + Depth

- Always together forever and ever 😊

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 3306 (msg:"ET CURRENT_EVENTS MySQL Malicious  
Scanning 1"; flow:to_server; content:"|00 03|"; offset:3; depth:2; content:"GRANT  
ALTER, ALTER ROUTINE"; distance:0; nocase; content:"T0 root@% WITH";
```

- Content of hex |00 03| will be found 3 bytes in, 2 bytes deep

Distance

- Tells engine to look for your content n bytes relative to the previous match
- content:"something"; content:"something else"; distance:5;
- distance:0; can be used to tell the engine a content comes after another
 - content:"x"; content:"y"; distance:0; means "y" must come **after** "x"

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 3306 (msg:"ET CURRENT_EVENTS MySQL Malicious  
Scanning 1"; flow:to_server; content:"|00 03|"; offset:3; depth:2; content:"GRANT  
ALTER, ALTER ROUTINE"; distance:0; nocase; [REDACTED] content:"T0 root@% WITH";
```



Within

- Tells the engine how many bytes within this content will be found
- Allows us to dictate the amount of packet data being analyzed

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 3306 (msg:"ET CURRENT_EVENTS MySQL Malicious  
Scanning 1"; flow:to_server; content:"|00 03|"; offset:3; depth:2; content:"GRANT  
ALTER, ALTER ROUTINE"; distance:0; nocase; within:30; content:"T0 root@% WITH";
```



- Content match is 26 characters
- 30 bytes within the previous match, this string must exist
- goes with “Distance”

Negation

- We can negate content just as easy as we match content
- Rule will not fire if negated content is present
- Simply place a ! before the content
- content:!”Referer|3a 20|”;
- Negate “normal“ content that doesn’t appear in traffic
 - Careful! Can cause False Negatives



Checking in

- content:"foo"; offset:4; depth:3; content:"bar"; distance:20; within:3;
- content:"something"; depth:9; content:"some|20|more"; distance:0
- alert udp \$HOME_NET any -> \$EXTERNAL_NET 53
- alert tcp \$HOME_NET any -> \$EXTERNAL_NET any (msg:"Something Evil"; flow:established,to_server; dsize:45;
- content:"User-Agent|3a 20|Internet"; content:!\"Accept|3a|";

Rule Meta

- SID
 - Signature ID
 - sid:10000000
- Reference
 - Attach reference to our rule to help provide context
 - reference:md5, e273508a2f2ed45c20a2412f7d62eceb;
 - reference:url, malwarefor.me/2015-12-27-sundown-ek-sending-neutrino;
 - reference:cve, 2016-3254;
- Revision
 - Tells us what version of the rule we are on
 - rev:9;



Basic Group Exercise



dszie:__; content:"_____"; content:"_____";
distance:0; content:"_____"; distance:0;

Data (260 bytes)	
Data: 414d44205068656e6f6d28746d2920393535302051756164... [Length: 260]	
0020	1f b9 04 08 07 c5 5e 19 73 d9 4c ac f8 04 50 18
0030	ff ff a7 3e 00 00 41 4d 44 20 50 68 65 6e 6f 6d
0040	28 74 6d 29 20 39 35 35 30 20 51 75 61 64 2d 43
0050	6f 72 65 20 50 72 6f 63 65 73 73 6f 72 00 00 00
0060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0	00 00 00 00 00 31 32 38 20 4d 42 00 00 00 00 00
00c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00d0	00 00 00 00 00 57 69 6e 64 6f 77 73 20 58 50
00e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00f0	00 00 00 00 00 56 31 2e 30 00 00 00 00 00 00 00
0100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0120	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0130	00 00 00 00 00 64 00 00 00

dszie:260; content:"MB|00 00|"; content:"Windows |
20|"; distance:0; content:"V1.0|00 00|"; distance:0;

Data (260 bytes)	
Data: 414d44205068656e6f6d28746d2920393535302051756164... [Length: 260]	
0020	1f b9 04 08 07 c5 5e 19 73 d9 4c ac f8 04 50 18
0030	ff ff a7 3e 00 00 41 4d 44 20 50 68 65 6e 6f 6d
0040	28 74 6d 29 20 39 35 35 30 20 51 75 61 64 2d 43
0050	6f 72 65 20 50 72 6f 63 65 73 73 6f 72 00 00 00
0060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0	00 00 00 00 00 00 31 32 38 20 4d 42 00 00 00 00
00c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00d0	00 00 00 00 00 00 57 69 6e 64 6f 77 73 20 58 50
00e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00f0	00 00 00 00 00 00 56 31 2e 30 00 00 00 00 00 00
0100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0120	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0130	00 00 00 00 00 00 64 00 00 00

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any
(msg:"njRAT/Syrian Malware Variant CnC Checkin ";
flow:_; content:"";
offset:_; depth:_; content:"";
distance:0; content:""; distance:0;
classtype:trojan-activity; sid:100; rev:1;)
```

0030	f4 23 93 43 00 00 21 30 2f 6a 7c 6e 5c 53 79 72	.#.C..!0 /j n\Syr
0040	69 61 6e 20 4d 61 6c 77 61 72 65 2f 6a 7c 6e 5c	ian Malw are/j n\
0050	74 65 6d 75 63 6f 2f 6a 7c 6e 5c 6d 65 2f 6a 7c	temuco/j n\me/j
0060	6e 5c 55 53 41 2f 6a 7c 6e 5c 57 69 6e 20 58 50	n\USA/j n\Win XP
0070	20 50 72 6f 66 65 73 73 69 6f 6e 61 6c 53 50 32	Profess ionalSP2
0080	20 78 38 36 2f 6a 7c 6e 5c 4e 6f 2f 6a 7c 6e 5c	x86/j n \No/j n\
0090	30 2e 31 2f 6a 7c 6e 5c 2f 6a 7c 6e 5c 61 62 6f	0.1/j n\ /j n\abo
00a0	75 74 3a 62 6c 61 6e 6b 20 2d 20 4d 69 63 72 6f	ut:blank - Micro
00b0	73 6f 66 74 20 49 6e 74 65 72 6e 65 74 20 45 78	soft Int ernet Ex
00c0	70 6c 6f 72 65 72 2f 6a 7c 6e 5c 5b 65 6e 64 6f	plorer/j n\[endo
00d0	66 5d	f]

```

alert tcp $HOME_NET any -> $EXTERNAL_NET any
(msg:"njRAT/Syrian Malware Variant CnC Checkin ";
flow:established,to_server; content:"|2f|j|7c|n|
5c|"; offset:2; depth:5; content:"Syrian Malware";
distance:0; content:[endof]; distance:0;
classtype:trojan-activity; sid:100; rev:1;)

```

0030	f4 23 93 43 00 00 21 30 2f 6a 7c 6e 5c 53 79 72	.#.C..!0 /j n\Syr
0040	69 61 6e 20 4d 61 6c 77 61 72 65 2f 6a 7c 6e 5c	ian Malw are/j n\
0050	74 65 6d 75 63 6f 2f 6a 7c 6e 5c 6d 65 2f 6a 7c	temuco/j n\me/j
0060	6e 5c 55 53 41 2f 6a 7c 6e 5c 57 69 6e 20 58 50	n\USA/j n\Win XP
0070	20 50 72 6f 66 65 73 73 69 6f 6e 61 6c 53 50 32	Profess ionalSP2
0080	20 78 38 36 2f 6a 7c 6e 5c 4e 6f 2f 6a 7c 6e 5c	x86/j n \No/j n\
0090	30 2e 31 2f 6a 7c 6e 5c 2f 6a 7c 6e 5c 61 62 6f	0.1/j n\ /j n\abo
00a0	75 74 3a 62 6c 61 6e 6b 20 2d 20 4d 69 63 72 6f	ut:blank - Micro
00b0	73 6f 66 74 20 49 6e 74 65 72 6e 65 74 20 45 78	soft Int ernet Ex
00c0	70 6c 6f 72 65 72 2f 6a 7c 6e 5c 5b 65 6e 64 6f	plorer/j n\[endo
00d0	66 5d	f]

Basic Rule Writing Lab

**Exercise 1: DDoSClient.pcap in the
workbook.pdf on the vm desktop**

If you are confident in your rule writing abilities, begin on page 7.

If you would like some assistance start on page 8.

We will write the rule live in 15 minutes.



Additional Rule Writing Features



fast_pattern



- Keyword placed after a content which **must** be matched before the rule is evaluated
- `content:"something|20|unique"; fast_pattern;`
- Should be used in every rule on most valuable content chosen by rule author
 - VERY efficient
- `fast_pattern;` by default is 20 bytes
 - If matching `content:"User-Agent|3a 20|Mozilla/5.0 (Evilness)"`;
`fast_pattern;`
 - `fast_pattern` will be “`User-Agent|3a 20|Mozilla/`”

fast_pattern (cont...)

- If a content is longer than 20 bytes... fast_pattern “chop”
- `fast_pattern:x,y;`
- Allows us to choose the 20 bytes of the content we want to use for our fast_pattern
- `content:"User-Agent|3a 20|Mozilla/5.0 (Evilness)"
fast_pattern:14,20;`
 - fast_pattern becomes “ozilla/5.0 (Evilness)”
- `content:"User-Agent|3a 20|DetoxCrypto"; fast_pattern:3,20;`
 - fast_pattern becomes “r-Agent|3a 20|DetoxCrypto”

HTTP Buffers

- Suricata and Snort have the ability to parse HTTP and place packet contents into buffers to easily match.
- Much faster than searching raw packet
- We can use these to our advantage in conjunction with the other keywords and modifiers!
 - content:"User-Agent|3a 20|DetoxCrypt"; http_header; fast_pattern:3,20;
- Suricata HTTP Buffers: <http://suricata.readthedocs.io/en/latest/rules/http-keywords.html>
- Snort HTTP Buffers: <http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node32.html>

HTTP Buffer (cont...)

POST /generate.php HTTP/1.1

User-Agent: DetoxCrypto2

Content-Type: application/x-www-form-urlencoded

Host: detoxcrypto.net16.net

Content-Length: 26

Expect: 100-continue

Connection: Keep-Alive

publickey=sdJoFsAv3jSNMEYxHTT

Date: Sat, 13 Aug 2016 04:45:

Server: Apache

X-Powered-By: PHP/5.2.17

Content-Length: 186

Connection: close

Content-Type: text/html

content:"POST"; http_method;

content:"/generate.php"; http_uri;

content:"User-Agent|3a 20|DetoxCrypto"; http_header;

content:"publickey="; http_client_body;

MQoxjmeGRPHGh2GVdFSPHnycHwL5i7Z4

<!-- Hosting24 Analytics Code -->

<script type="text/javascript" src="http://stats.hosting24.com/count.php"></script>

http_method

- The http_method; keyword can be used for a content involving the method in which the HTTP Request was made
 - content:"GET"; http_method;
 - content:"POST"; http_method;
 - content:"HEAD"; http_method;

```
POST /generate.php HTTP/1.1
User-Agent: DetoxCrypto2
Content-Type: application/x-www-form-urlencoded
Host: detoxcrypto.net16.net
Content-Length: 26
Expect: 100-continue
Connection: Keep-Alive
```

http_uri

- Used for capturing any content present in the URI string of a request
- content:"/generate.php"; http_uri;
- urilen keyword
 - urilen:<number>;
 - Used like dsize, but for the length of the URI

```
POST /generate.php HTTP/1.1
User-Agent: DetoxCrypto2
Content-Type: application/x-www-form-urlencoded
Host: detoxcrypto.net16.net
Content-Length: 26
Expect: 100-continue
Connection: Keep-Alive
```

http_header

- This is used for any field present in the Header section
- content:"User-Agent|3a|"; http_header;
- content:! "Referer|3a|"; http_header;
- Cookie is not able to be used with this buffer
 - It has its own buffer → http_cookie

```
POST /generate.php HTTP/1.1
User-Agent: DetoxCrypto2
Content-Type: application/x-www-form-urlencoded
Host: detoxcrypto.net16.net
Content-Length: 26
Expect: 100-continue
Connection: Keep-Alive
```

```
publickey=sdJoFsAv3jSNMEYxHTTP/1.1 200 OK
Date: Sat, 12 Aug 2016 04:45:30 GMT
```

http_client_body

- Used for an HTTP request's payload
- Commonly observed with POST requests
- content:"publickey="; http_client_body;



```
POST /generate.php HTTP/1.1
User-Agent: DetoxCrypto2
Content-Type: application/x-www-form-urlencoded
Host: detoxcrypto.net16.net
Content-Length: 26
Expect: 100-continue
Connection: Keep-Alive
```

```
publickey=sdJoFsAv3jSNMEYx HTTP/1.1 200 OK
```

```
Date: Sat, 13 Aug 2016 04:45:30 GMT
Server: Apache
X-Powered-By: PHP/5.2.17
Content-Type: text/html; charset=UTF-8
```

http_user_agent

- Suricata only! Fast! Use it!
- Will parse the field between User-Agent|3a 20| and |0d 0a|
- **Suricata**
 - content:"DetoxCrypto"; fast_pattern; **http_user_agent**;
- **Snort**
 - content:"User-Agent|3a 20|DetoxCrypto"; fast_pattern:3,20;
http_header;

```
POST /generate.php HTTP/1.1
User-Agent: DetoxCrypto2
Content-Type: application/x-www-form-urlencoded
Host: detoxcrypto.net16.net
Content-Length: 26
Expect: 100 continue
```

file_data

- Keyword used to declare content that is in the Response Body
- Used once in a rule; applies to content used after
- file_data;

```
POST /generate.php HTTP/1.1
User-Agent: DetoxCrypto2
Content-Type: application/x-www-form-urlencoded
Host: detoxcrypto.net16.net
Content-Length: 26
Expect: 100-continue
Connection: Keep-Alive

publickey=sd1oEsv3jSNMFYvHTTP/1.1 200 OK
Date: Sat, 13 Aug 2016 04:45:30 GMT
Server: Apache
X-Powered-By: PHP/5.2.17
Content-Length: 186
Connection: close
Content-Type: text/html
```

HTTP Response Headers

```
MQoxjmeGRPHGh2GVdFSPHnycHwL5i7Z4
<!-- Hosting24 Analytics Code -->
<script type="text/javascript" src="http://stats.hosting24.com/count.php"></script>
<!-- End Of Analytics Code -->
```

HTTP Response Body

Additional Rule Writing Features Group Exercise



content:"/g76gyui?"; _____; depth:_; content:"User-Agent|3a 20|Mozilla/4.0 (compatible|3b 20|MSIE 6.0|3b 20|Windows NT 5.0)|0d 0a|"; _____;
content:"Connection|3a 20|Keep-Alive|0d 0a|";
_____;

```
GET /g76gyui?cNENEDif=fIcXzg HTTP/1.1
Accept: */
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept-Encoding: gzip, deflate
Host: www.bytove.jadro.szm.com
Connection: Keep-Alive
```

content:"/g76gyui?"; **http_uri**; depth:**9**; content:"User-Agent|3a 20|Mozilla/4.0 (compatible|3b 20|MSIE 6.0|3b 20|Windows NT 5.0)|0d 0a|"; **http_header**; content:"Connection|3a 20|Keep-Alive|0d 0a|"; **http_header**;

```
GET /g76gyui?cNENEDif=fIcXzg HTTP/1.1
Accept: /*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept-Encoding: gzip, deflate
Host: www.bytove.jadro.szm.com
Connection: Keep-Alive
```

content:"Content-Length|3a 20|2"; _____;
content:"Content-Type|3a 20|text/html";
_____; _____; content:"<iframe src=|
22|"; depth:__; content:"width=|22|"; distance:__;
content:"height=|22|"; distance:__;
content:"_____"; fast_pattern;

HTTP/1.1 200 OK
Date: Fri, 02 Sep 2016 07:36:36 GMT
Server: Apache/2.2.22 (@RELEASE@)
X-Powered-By: PHP/5.3.3
Content-Length: 278
Connection: close
Content-Type: text/html; charset=UTF-8

<iframe src="http://v42pdxqt.top/?x3qJc7iaLxjHCYE=l3SKfPrfJxzFGMSUb-nJDa9GP0XCRQLPh4SGhKrXCJ-
ofSih170IFxzsqAycFUKCqrF4Qu4Fah2h1QWScEZrmYRPFgVIove8hQLfyhSWkpGBrBS0aAhA_pSRF-
U_2AygzLJFdcomwRWA6mcCmL5PQFFd" width="468" height="60" style="position:absolute;left:-10000px;"></
iframe>

```
content:"Content-Length|3a 20|2"; http_header;
content:"Content-Type|3a 20|text/html"; http_header;
file_data; content:"<iframe src=|22|"; depth:13;
content:"width=|22|"; distance:0; content:"height=|22|";
distance:0; content:"absolute|3b|left|3a|-1";
fast_pattern;
```

```
HTTP/1.1 200 OK
Date: Fri, 02 Sep 2016 07:36:36 GMT
Server: Apache/2.2.22 (@RELEASE@)
X-Powered-By: PHP/5.3.3
Content-Length: 278
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
<iframe src="http://v42pdxqt.top/?x3qJc7iaLxjHCYE=l3SKfPrfJxzFGMSUb-nJDa9GP0XCRQLPh4SGhKrXCJ-
ofSih170IFxzsqAycFUKCqrF4Qu4Fah2h1QWScEZrmYRPFgVIove8hQLfyhSwkpGBrBS0aAhA_pSRF-
U_2AygzLJFdcomwRWA6mcCmL5PQFFd" width="468" height="60" style="position:absolute;left:-10000px;"></
iframe>
```

HTTP Rule Writing Lab

**Exercise 2: Ursnif.pcap in the
workbook.pdf on the vm desktop**

If you are confident in your rule writing abilities, begin on page 10.

If you would like some assistance start on page 11.

We will write the rule live in 15 minutes.



PCRE

welcome to hell



B3SIDES
LAS VEGAS

PCRE

- Pearl Compatible Regular Expression
- Similar to other regex vernacular (JavaScript, etc)
- Called using “pcre” followed by the regular expression
- PCRE must be wrapped in leading and trailing forward slashes
- `pcre:"/something flags";`



PCRE (cont...)

- `pcre:"/\/[A-Za-z0-9]{6}\.php$/U";`
- Looks for 6 chars in the range followed by .php and nothing after
- Must wrap the PCRE with forward slashes (“/”)
- Flags go after the last forward slash
- Anchors go after and before wrapped slashes
- Need to escape certain characters with a backslash if used literally
 - \/
 - \\$
 - ?

PCRE - Special Chars

- `^`
 - Leading anchor (start matching here)
 - `pcre:"/^foo/P";`
- `$`
 - Trailing anchor (nothing after)
 - `pcre:"foo$/P";`
- `[]`
 - Character set- wrap characters in brackets
 - `pcre:"/[A-Za-z0-9]/U";`
- `()`
 - Capturing group
 - `pcre:"([A-Z0-9]{8})+/";`
- `{}`
 - Certain number, or range of something you match
 - `pcre:"/[A-Za-z0-9]{5,10}/U";`
 - Matches between 5 and 10 of alphanumeric

- `\s`
 - Matches a space
 - Good for Javascript and HTML
- `\r`
 - Matches Carriage return
 - Same is `|0d|`
- `\n`
 - Matches new-line
 - Same as `|0a|`
- `.`
 - Matches anything
- `?`
 - Matches 1 or 0
- `*`
 - Matches 0 or more
- `+`
 - 1 or more
 - `pcre:"/[A-Za-z0-9]+/U";`
- `?:`
 - Non-capture group
 - ALWAYS use this...
 - `pcre:"/(?:this|that)/";`

PCRE - Flags

- Used to represent the various buffers available in the engine
- To be used just like content + buffer
- U - http_uri;
- H - http_header;
- P - http_client_body;
- i - Makes PCRE case-insensitive
- R - Makes PCRE relative (distance:0;) to last match
- m - Multi-line matching



PCRE Group Exercise



Exercise - PCRE

- What could a PCRE look like for this traffic...? We know the command (URI) is between 2 and 5 characters long

```
GET /PWD HTTP/1.1
Host: cdn.fastaccesshosting.xyz
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.0.15
Date: Tue, 08 Mar 2016 19:55:28 GMT
Content-Type: application/octet-stream
Content-Length: 283702
Last-Modified: Sun, 31 May 2015 17:47:42 GMT
Connection: keep-alive
Accept-Ranges: bytes
```

Exercise - PCRE

- What could a PCRE look like for this traffic...?
- `pcre:"/^V[A-Z]{2,5}$/"`;

```
GET /PWD HTTP/1.1
Host: cdn.fastaccesshosting.xyz
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.0.15
Date: Tue, 08 Mar 2016 19:55:28 GMT
Content-Type: application/octet-stream
Content-Length: 283702
Last-Modified: Sun, 31 May 2015 17:47:42 GMT
Connection: keep-alive
Accept-Ranges: bytes
```

Exercise - PCRE

- Write a PCRE for this HTTP URI string, assuming the variables will change per infection

```
GET /ping.php?hostname=AMBROSE&username=peggysue&domain=AMBROSE HTTP/1.1
Accept: /*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/
7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media
Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.2)
Host: 52.65.108.15
Connection: Keep-Alive
```

Exercise - PCRE

- Write a PCRE for this HTTP URI string, assuming the variables will change per infection
- `pcre:"/^\\ping\\.php\\?hostname=[^\\r\\n]+&username=[^\\r\\n]+&domain=[^\\r\\n]+$/Ui";`

```
GET /ping.php?hostname=AMBROSE&username=peggysue&domain=AMBROSE HTTP/1.1
Accept: /*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/
7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media
Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.2)
Host: 52.65.108.15
Connection: Keep-Alive
```

Exercise - PCRE

- Write a PCRE for the http_header order

```
GET /g76gyui?cNENEDif=fIcXzg HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept-Encoding: gzip, deflate
Host: www.bytove.jadro.szm.com
Connection: Keep-Alive
```

Exercise - PCRE

- Write a PCRE for the http_header order
- pcre:"/^Accept\x3a\x20[^r\n]+r\nAccept-Language\x3a\x20en-us\r\nUser-Agent\x3a\x20[^r\n]+\r\nAccept-Encoding[^r\n]+\r\nHost\x3a\x20[^r\n]+\r\nConnection[^r\n]+\r\n\r\n\$/Hmi";

```
GET /g76gyui?cNENEDif=fIcXzg HTTP/1.1
Accept: */
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept-Encoding: gzip, deflate
Host: www.bytove.jadro.sz.m.com
Connection: Keep-Alive
```

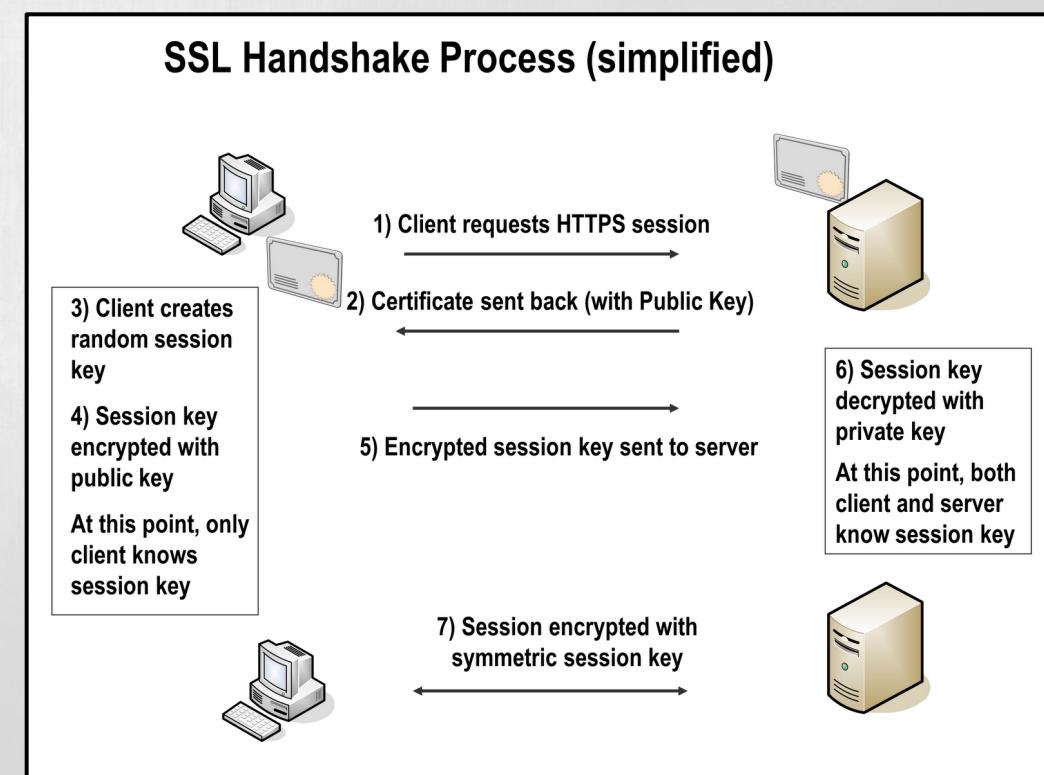
SSL / TLS



BSides LAS VEGAS

SSL / TLS

- A blind spot for most IDS/IPS
- Cannot see into the traffic, just that its happening
 - Unless MITM, which is cool too!
- Let's Encrypt!
- Wait!
- We can do something with SSL/TLS



SSL / TLS Basics

No.	Time	Source	SrcPort	Host	Destination	DstPort	Protocol	Stat	Length	Info
67	2016-09-06 13:38:19.229795	192.168.78.20	49181		91.219.31.12	443	TLSv1		117	Client Hello
69	2016-09-06 13:38:19.833871	91.219.31.12	443		192.168.78.20	49181	TLSv1		741	Server Hello, Certificate,
70	2016-09-06 13:38:19.901833	192.168.78.20	49181		91.219.31.12	443	TLSv1		198	Client Key Exchange, Change
71	2016-09-06 13:38:20.336401	91.219.31.12	443		192.168.78.20	49181	TLSv1		59	Change Cipher Spec, Encrypt

▼ TLSv1 Record Layer: Handshake Protocol: Certificate

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 641

▼ Handshake Protocol: Certificate

Handshake Type: Certificate (11)

Length: 637

Certificates Length: 634

▼ Certificates (634 bytes)

Certificate Length: 631

▼ Certificate: 30820273308201dca00302010202045da0decc300d06092a... (id-at-commonName=vuinuzhz.com)

▼ signedCertificate

version: v3 (2)

serialNumber: 1570823884

► signature (sha256WithRSAEncryption)

► issuer: rdnSequence (0)

► validity

▼ subject: rdnSequence (0)

▼ rdnSequence: 1 item (id-at-commonName=vuinuzhz.com)

▼ RDNSequence item: 1 item (id-at-commonName=vuinuzhz.com)

▼ RelativeDistinguishedName item (id-at-commonName=vuinuzhz.com)

SSL / TLS - What to sig on

- Serial Number
 - content:"|09 00 97 ae 20 7e 61 5f 58 15|";
- Common Name (CN)
 - content:"|55 04 03|";
- Organization (O)
 - content:"|55 04 0a|";
- Organizational Unit (OU)
 - content:"|55 04 0b|";
- Country (C)
 - content:"|55 04 06|";
- State (S)
 - content:"|55 04 08|";
- Locality (L)
 - content:"|55 04 07|";

00000090	04	03	0c	0c	76	75	69	6e	75	7a	68	7a	2e	63	6f	6dvuin	uzhz.com	
000000A0	30	1e	17	0d	31	36	30	38	32	33	31	35	34	39	35	35	0...1608	23154955	
000000B0	5a	17	0d	31	39	30	38	32	33	31	35	34	39	35	35	5a	Z..19082	3154955Z	
000000C0	30	17	31	15	30	13	06	03	55	04	03	0c	0c	76	75	69	0.1.0...	U....vui	
000000D0	6e	75	7a	68	7a	2e	63	6f	6d	30	81	9f	30	0d	06	09	nuzhz.co	m0...0...	
000000E0	2a	86	48	86	f7	0d	01	01	01	05	00	03	81	8d	00	30	*.H.....0	
000000F0	81	89	02	81	81	00	9d	73	56	26	25	61	42	00	2c	36s	V&%aB.,6	
00000100	cb	fd	b5	a3	0e	61	b0	d9	c0	ea	24	4b	81	c6	49	a4a...	...\$K..I.	
00000110	92	3a	28	82	3d	3b	9d	b5	e5	bf	ca	e2	5b	31	02	91	.:(.=;..[1..	
00000120	69	3e	b9	61	c6	5a	79	d4	ce	6a	89	e0	7d	8e	fd	97	i>.a.Zy.	.j...}...	
00000130	d1	9e	74	cb	cf	96	61	25	8f	ce	1b	d3	81	9c	39	a0	..t...a%9.	
00000140	17	b7	37	20	ef	2b	a8	09	6d	e6	43	c8	c8	65	4d	2f	.7	+.+..	m.C..eM/

Writing Signatures for SSL / TLS

```
alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"ET TROJAN ABUSE.CH SSL Fingerprint  
Blacklist Malicious SSL Certificate Detected (H1N1 CnC)"; flow:established,from_server;  
content:"|09 00 cc e5 16 49 2c 1e 96 57|"; content:"|55 04 0a|"; distance:0; content:  
"\x13|Default Company Ltd"; distance:1; within:20; reference:url,sslbl.abuse.ch; classtype:  
trojan-activity; sid:2022959; rev:2;)
```

- Protocol: tls (Suricata) or tcp (Snort)
- Ports: any/any (Suricata) or 443/any (Snort)
- Content: Serial number
- Content: Organization
 - \x13 is the length of the field in Decimal
 - 13 hex = 19 decimal

Writing Signatures for SSL / TLS

```
alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"ETPRO TROJAN Malicious SSL Certificate Observed (Vawtrak)"; flow:established,from_server; content:"|55 04 03|"; content:"|\x0c|vuinuzhz.com"; distance:1; within:13; classtype:trojan-activity; sid:100000034; rev:1;)
```

- Protocol: tls (Suricata) or tcp (Snort)
- Ports: any/any (Suricata) or 443/any (Snort)
- Content: Common Name (CN)
 - \x0c is the length of the domain name
 - \x0c hex = 12 in decimal

SSL / TLS Group Exercise



```
alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Malicious SSL  
Cert Inbound"; flow:_____; content:"_____";  
fast_pattern; content:"_____"; content:"_____"; distance:0;  
content:"_____"; distance:____; within:____;
```

53	2016-05-31	09:07:02.722134	109.236.92.237	443	10.0.2.15	1050	TLSv1	318
54	2016-05-31	09:07:02.722740	10.0.2.15	1050	109.236.92.237	443	TLSv1	318
▼ Handshake Protocol: Certificate								
Handshake Type:	Certificate (11)	fb	5f	00	0a	00	16	03
Length:	981	d2	00	03	cf	30	82	03
Certificates Length:	978	cb	30	82	02	b3	a0	03
▼ Certificates (978 bytes)	Certificate Length: 975	02	02	09	00	96	90	d4
Certificate Length:	975	7b	0a	4c	dd	5a	30	0d
▼ Certificate: 308203cb308202b3a0030201020	09	06	03	55	04	06	13	02
▼ signedCertificate	02	55	53	31	0e	30	0c	06
version: v3 (2)	03	55	04	08	0c	05	61	61
serialNumber: -7597338946455151270	20	61	61	31	0d	30	0b	06
► signature (sha256WithRSAEncryption)	55	55	04	07	0c	04	74	65
▼ issuer: rdnSequence (0)	73	73	74	31	74	31	0d	30
▼ rdnSequence: 7 items (pkcs-9-at-emailAddress=test@test.com, id-at-commonName=test.test, id-at-orga	74	31	0b	06	03	55	04	03
► RDNSequence item: 1 item (id-at-countryName=US)	09	0b	0c	04	74	65	73	74
► RDNSequence item: 1 item (id-at-stateOrProvinceName=aa aa)	2e	74	65	73	74	31	1c	30
► RDNSequence item: 1 item (id-at-localityName=test)	74	65	73	74	2e	74	31	1a
► RDNSequence item: 1 item (id-at-organizationName=test)	31	12	30	10	06	03	55	04
► RDNSequence item: 1 item (id-at-organizationalUnitName=test)	09	0c	09	74	65	73	74	31
► RDNSequence item: 1 item (id-at-commonName=test.test)	74	65	73	74	2e	74	31	1c
► RDNSequence item: 1 item (pkcs-9-at-emailAddress=test@test.com)	74	65	73	74	31	1c	30	1a

```
alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:"Malicious  
SSL Cert Inbound"; flow:established,from_server; content:"|00  
96 90 d4 7b 0a 4c dd 5a|"; fast_pattern; content:"|55 04  
0a|"; distance:0; content:"|04|test"; distance:1; within:5;
```

53	2016-05-31	09:07:02.722134	109.236.92.237	443	10.0.2.15	1050	TLSv1	318
54	2016-05-31	09:07:02.722740	10.0.2.15	1050	109.236.92.237	443	TLSv1	318
▼ Handshake Protocol: Certificate								
Handshake Type:	Certificate (11)	fb	5f	00	0a	00	16	03
Length:	981	d2	00	03	cf	30	82	03
Certificates Length:	978	cb	30	82	02	b3	a0	03
▼ Certificates (978 bytes)	Certificate Length: 975	02	02	09	00	96	90	d4
Certificate Length:	975	7b	0a	4c	dd	5a	30	0d
▼ Certificate: 308203cb308202b3a0030201020	09	06	03	55	04	06	13	02
▼ signedCertificate	02	55	53	31	0e	30	0c	06
version: v3 (2)	03	55	04	08	0c	05	61	61
serialNumber: -7597338946455151270	20	61	61	31	0d	30	0b	06
► signature (sha256WithRSAEncryption)	55	55	04	07	0c	04	74	65
▼ issuer: rdnSequence (0)	73	73	74	31	74	31	0d	30
▼ rdnSequence: 7 items (pkcs-9-at-emailAddress=test@test.com, id-at-commonName=test.test, id-at-orga	74	31	0b	06	03	55	04	03
► RDNSequence item: 1 item (id-at-countryName=US)	09	0b	0c	04	74	65	73	74
► RDNSequence item: 1 item (id-at-stateOrProvinceName=aa aa)	2e	74	65	73	74	31	1c	30
► RDNSequence item: 1 item (id-at-localityName=test)	74	65	73	74	2e	74	31	1a
► RDNSequence item: 1 item (id-at-organizationName=test)	31	12	30	10	06	03	55	04
► RDNSequence item: 1 item (id-at-organizationalUnitName=test)	09	0c	09	74	65	73	74	31
► RDNSequence item: 1 item (id-at-commonName=test.test)	74	65	73	74	2e	74	31	1c
► RDNSequence item: 1 item (pkcs-9-at-emailAddress=test@test.com)	74	65	73	74	31	1c	30	1a

alert tls \$EXTERNAL_NET any -> \$HOME_NET any
(msg:"Malicious SSL Cert Inbound"; flow:_____;
content:"____"; content:"_____"; distance:____;
within:____;

▼ Handshake Protocol: Certificate

Handshake Type: Certificate (11)

Length: 663

Certificates Length: 660

▼ Certificates (660 bytes)

Certificate Length: 657

▼ Certificate: 3082028d308201f6020900bc9b2399128eb25f300

▼ signedCertificate	9b 0b 00 02 97 00 02 94 00 02 91 30 82 02 8d 30 82 01 f6 02 09 00 bc 9b 23 99 12 8e b2 5f 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30 81 8a 31 0b 30 09 06 03 55 04 06 13 02 5a 41 31 0b 30 09 06 03 55 04 08 0c 02 46 58 31 0c 30 0a 06 03 55 04 07 0c 03 42 6e 7a 31 0d 30 0b 06 03 55 04 0a 0c 04 48 6f 73 6c 31 0b 30 09 06 03 55 04 0b 0c 02 41 56 31 1e 30 1c 06 03 55 04 03 0c 15 6e 79 63 74 72 61 64 65 72 73 61 63 61 64 65 6d 79 2e 63 6f 6d 31 24 30 22 06 09 2a 86 48 86 f7 0d 01 09 01 16 15 6e 79 63 74 72 61 64 65 72 73 61 0...0 #....0. .*.H...0.. 1.0...U. ...ZA1.0 ...U.... FX1.0... U....Bnz 1.0...U. ...Hosl1 .0...U.. .AV1.0. ...U....n yctrader sacademy .com1\$0" ...*.H...nyc tradersa
serialNumber: -4856248632840637857		
► signature (sha256WithRSAEncryption)		
► issuer: rdnSequence (0)		
► validity		
▼ subject: rdnSequence (0)		
▼ rdnSequence: 7 items (pkcs-9-at-emailAddress=nyctradersacademy.com, id-at-commonName=nyctradersacademy.com, id-at-org		
► RDNSequence item: 1 item (id-at-countryName=ZA)		
► RDNSequence item: 1 item (id-at-stateOrProvinceName=FX)		
► RDNSequence item: 1 item (id-at-localityName=Bnz)		
► RDNSequence item: 1 item (id-at-organizationName=Hosl)		
► RDNSequence item: 1 item (id-at-organizationalUnitName=AV)		
► RDNSequence item: 1 item (id-at-commonName=nyctradersacademy.com)		
► RDNSequence item: 1 item (pkcs-9-at-emailAddress=nyctradersacademy.com)		
► subjectPublicKeyInfo		

► subjectPublicKeyInfo

alert tls \$EXTERNAL_NET any -> \$HOME_NET any (msg:"Malicious SSL Cert Inbound"; flow:**established,from_server**; content:"|
55 04 03 |"; content:"| **15 | nyctradersacademy.com**"; distance:
1; within:**22**;

▼ Handshake Protocol: Certificate

Handshake Type: Certificate (11)

Length: 663

Certificates Length: 660

▼ Certificates (660 bytes)

Certificate Length: 657

▼ Certificate: 3082028d308201f6020900bc9b2399128eb25f300

▼ signedCertificate

 serialNumber: -4856248632840637857

 ► signature (sha256WithRSAEncryption)

 ► issuer: rdnSequence (0)

 ► validity

 ▼ subject: rdnSequence (0)

 ▼ rdnSequence: 7 items (pkcs-9-at-emailAddress=nyctradersacademy.com, id-at-commonName=nyctradersacademy.com, id-at-org

 ► RDNSequence item: 1 item (id-at-countryName=ZA)

 ► RDNSequence item: 1 item (id-at-stateOrProvinceName=FX)

 ► RDNSequence item: 1 item (id-at-localityName=Bnz)

 ► RDNSequence item: 1 item (id-at-organizationName=Hosl)

 ► RDNSequence item: 1 item (id-at-organizationalUnitName=AV)

 ► RDNSequence item: 1 item (id-at-commonName=nyctradersacademy.com)

 ► RDNSequence item: 1 item (pkcs-9-at-emailAddress=nyctradersacademy.com)

 ► subjectPublicKeyInfo

9b 0b 00 02 97 00 02 94 00 02 91 30 82 02 8d 30 0...0
82 01 f6 02 09 00 bc 9b 23 99 12 8e b2 5f 30 0d #....0.
06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30 81 8a	.*.H...0..
31 0b 30 09 06 03 55 04 06 13 02 5a 41 31 0b 30	1.0...U. ...ZA1.0
09 06 03 55 04 08 0c 02 46 58 31 0c 30 0a 06 03	...U.... FX1.0...
55 04 07 0c 03 42 6e 7a 31 0d 30 0b 06 03 55 04	U....Bnz 1.0...U.
0a 0c 04 48 6f 73 6c 31 0b 30 09 06 03 55 04 0b	...Hosl1 .0...U..
0c 02 41 56 31 1e 30 1c 06 03 55 04 03 0c 15 6e	.AV1.0. ...U....n
79 63 74 72 61 64 65 72 73 61 63 61 64 65 6d 79	yctrader sacademy
2e 63 6f 6d 31 24 30 22 06 09 2a 86 48 86 f7 0d	.com1\$0" ...*.H...
01 09 01 16 15 6e 79 63 74 72 61 64 65 72 73 61nyc tradersa

SSL Rule Writing Lab

**Exercise 3: Zeus.pcap in the
workbook.pdf on the vm desktop**

If you are confident in your rule writing abilities, begin on page 13.

If you would like some assistance start on page 14.

We will write the rule live in 10 minutes.



Writing Signatures for SSL/TLS

- ssl_sigs.py
 - https://github.com/malwareforme/ssl_sigs
- Example:
 - \$ python ssl_sigs.py -d something.bad.com -m "TROJAN Observed Malicious SSL Cert (Ursnif Injects)" -s 100000000
 - alert tls \$EXTERNAL_NET 443 -> \$HOME_NET any (msg:"TROJAN Observed Malicious SSL Cert (Ursnif Injects)"; flow:established:from_server; content "| 55 04 03 |"; content:"|11|something.bad.com"; distance:1; within:18; classtype:trojan-activity; sid:100000000; rev:1;)

APPLICATION LABS

Phishing: Ex. 4 - Adobe.pcap

Ransomware: Ex. 5 - Cerber.pcap

Malicious Document: Ex. 6 - Maldoc.pcap

Exploit Kit: Ex. 7 - Neutrino.pcap

Targeted Attack: Ex. 8 - Patchwork.pcap



Wrapping Up

- Network analysis!
- The more you look into your network, the more likely you will be to know what “normal” and “abnormal” look like.
- Use multiple rule options together for maximum detection/efficiency
- Continue working...
 - ET OPEN Ruleset - Free to download and play with (learn from)
 - Snort Community Ruleset - Free to download and play with (learn from)
 - Security Onion - Free Ubuntu distro with Network Analysis tools
 - malware-traffic-analysis.net- PCAPs and malware samples galore
 - broadanalysis.net- PCAPs and malware samples galore

Resources

- Suricata Manual
 - <http://suricata.readthedocs.io/en/latest/index.html>
- Snort Manual
 - <http://manual-snort-org.s3-website-us-east-1.amazonaws.com/>
- Emerging Threats Open Mailing List
 - <https://lists.emergingthreats.net/mailman/listinfo/emerging-sigs>
- OISF Mailing List
 - <https://lists.openinfosecfoundation.org/mailman/listinfo/oisf-users>
- Snort Community Mailing List
 - <https://lists.snort.org/mailman/listinfo/snort-sigs>

Continued Education

- OISF - <https://suricata-ids.org/training/>
 - Suricata User Training (2 Day)
 - Suricon - Nov 15-17 2017, Prague, CZ - <https://suricon.net/>
 - Suricata Sigdev (2 Day)
 - Derbycon 2017 (Sold Out)
 - Suricon
 - Suricata Developer Training
 - Sept 11 2017, Cork, Ireland
 - Private trainings available
- SANS 503 - <https://www.sans.org/course/intrusion-detection-in-depth>

Contact

Jack Mott

@malwareforme

Security Research Analyst

jmott@emergingthreats.net

Jae Williams

@switchingtoguns

Security Research Analyst

jae@emergingthreats.net

