NETWORK INTRUSION DETECTION WITH SURICATA

Tatyana Shishkova

KASPERSKY lab

ABOUT ME

Tatyana Shishkova

Malware Analyst @ Kaspersky Lab

Android Threat Research & Network Intrusion Detection

KASPERSKY lab

NETWORK INTRUSION DETECTION SYSTEM

Open source:

snort.org

suricata-ids.org

NETWORK INTRUSION DETECTION SYSTEM

- Monitors inbound and outbound traffic
- Analyses passing traffic (scans with a set of rules)
- Identifies attack / abnormal behavior
- Sends an alert

WAYS OF USING NIDS

- Scanning traffic from unknown objects on sandbox for automatic detection
- Scanning live traffic in corporate network

WHAT WE WILL LEARN

- Rule writing & optimization for various protocols
- Regex
- Different types of malicious activity
- Fixing false alarms

CLASS MATERIALS

- VM: Xubuntu 18.04 LTS
- Suricata 4.1.3 installed
- Wireshark 2.6.6 installed
- U: overdrivecon PW: overdrivecon

MALWARE ANALYSIS?..

- Actually, me 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

TO BEGIN WITH

- Suricata config: /etc/suricata/suricata.yaml
- Define variables ($HOME_NET/$EXTERNAL_NET, ports, etc) or use default
- Define rule path and rule files

KNOWN MALICIOUS BEHAVIOR: DINIHOU WORM

Traffic dump

```
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
```

KNOWN MALICIOUS BEHAVIOR: DINIHOU WORM

Malicious indicators in traffic

```
POST http://viruoos.no-ip.biz:81/is-ready HTTP/1.1
```

- HTTP POST request
- “/is-ready” relative address

```
User-Agent: C27BE56B<|>BKRBR0129PC011<|>1995227<|>Microsoft Windows 7 Enterprise <
|>plus<|>nan-av<|>true - 29/06/2017
```

- User-Agent contains information about infected machine

```
Host: viruoos.no-ip.biz:81
```

- Host contains port number

KNOWN MALICIOUS BEHAVIOR: DINIHOU WORM

How to create Snort/Suricata rule?

Old fashioned – Snort

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS \
(msg:"Dinihou worm"; flow:established,to_server; \
content:"POST"; http_method; \
content:"/is-ready"; http_uri; \
content:"/is-ready HTTP"; \
classtype:trojan-activity; \
reference:url,threats.kaspersky.com/en/threat/Worm.VBS.Dinihou/; \
sid:1000001; rev:1;)
```

```
POST http://viruoos.no-ip.biz:81/is-ready HTTP/1.1
```

KNOWN MALICIOUS BEHAVIOR: DINIHOU WORM

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

- 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 – <>)

KNOWN MALICIOUS BEHAVIOR: DINIHOU WORM

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

- Message (meta-setting – info about the possible attack)
- Flow (optional):
  - established / not_established
  - direction:
    - to_client = from_server
    - from_client = to_server

KNOWN MALICIOUS BEHAVIOR: DINIHOU WORM

```
content:"POST"; http_method; \
content:"/is-ready"; http_uri; \
content:"/is-ready HTTP"; \
```

- Content – matching on bytes:
  - Printable characters
  - Hexadecimal notation:
    - `content:"|0D 0A|"`
    - `content:"http|3A|//"`
- Content modifiers

CONTENT KEYWORDS

- Content modifiers: related to the previous content
  - content:"POST"; http_method;
- Sticky buffers: related to all contents that go after
  - http_response_line; content:"403 Forbidden";

HTTP CONTENT KEYWORDS

- Content modifiers: request
  - http_uri
  - http_method
  - http_client_body
  - http_header
  - http_cookie
  - http_user_agent
  - http_host

*Snort-compatible

HTTP CONTENT KEYWORDS

- Content modifiers: response
  - http_header
  - http_cookie
  - http_stat_msg
  - http_stat_code
  - http_server_body

*Snort-compatible

HTTP CONTENT STICKY BUFFERS

- Sticky buffers: request
  - http_request_line
  - http_accept
  - http_referer
  - http_connection
  - http_content_type
  - http_content_len
  - http_protocol
  - http_header_names

*Snort-compatible?
None of them.

HTTP CONTENT STICKY BUFFERS

- Sticky buffers: response
  - http_response_line
  - file_data
  - http_protocol
  - http_header_names

*Snort-compatible

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

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)

MORE KEYWORDS…

- dsize:12; (dsize:>24; dsize:12<>24;) – the size of the packet payload
- pcre:"/^[a-z0-9]{5}\.php$/U"; – regular expression

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/suricata-4.1.3/rules/index.html

KNOWN MALICIOUS BEHAVIOR: DINIHOU WORM

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

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

KASPERSKY lab

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

KNOWN MALICIOUS BEHAVIOR: DINIHOU WORM

How to create Snort/Suricata rule?

Old fashioned – Snort

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS \
(msg:"Dinihou worm"; flow:established,to_server; \
content:"POST"; http_method; \
content:"/is-ready"; http_uri; \
content:"/is-ready HTTP"; \
classtype:trojan-activity; \
reference:url,threats.kaspersky.com/en/threat/Worm.VBS.Dinihou/; \
sid:1000001; rev:1;)
```

```
POST http://viruoos.no-ip.biz:81/is-ready HTTP/1.1
```

KNOWN MALICIOUS BEHAVIOR: DINIHOU WORM

How to create Snort/Suricata rule?

Suricata

```
alert http $HOME_NET any -> $EXTERNAL_NET any \
(msg:"Dinihou worm"; flow:established,to_server; \
content:"POST"; http_method; \
content:"/is-ready"; http_uri; \
http_request_line; content:"/is-ready HTTP"; \
classtype:trojan-activity; \
reference:url,threats.kaspersky.com/en/threat/Worm.VBS.Dinihou/; \
sid:1000002; rev:1;)
```

```
POST http://viruoos.no-ip.biz:81/is-ready HTTP/1.1
```

KNOWN MALICIOUS BEHAVIOR: DINIHOU WORM

How to create Snort/Suricata rule?

Suricata

```
alert http $HOME_NET any -> $EXTERNAL_NET any \
(msg:"Dinihou worm"; flow:established,to_server; \
content:"POST"; http_method; \
content:"/is-ready"; http_uri; endswith; \
classtype:trojan-activity; \
reference:url,threats.kaspersky.com/en/threat/Worm.VBS.Dinihou/; \
sid:1000003; rev:1;)
```

```
POST http://viruoos.no-ip.biz:81/is-ready HTTP/1.1
```

KASPERSKY lab

KNOWN MALICIOUS BEHAVIOR: DINIHOU WORM

How to create Snort/Suricata rule?

Old fashioned – Snort

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS \
(msg:"Dinihou worm"; flow:established,to_server; \
content:"POST"; http_method; \
content:"|3c 7c 3e|nan-av|3c 7c 3e|"; http_header; \
classtype:trojan-activity; \
reference:url,threats.kaspersky.com/en/threat/Worm.VBS.Dinihou/; \
sid:1000004; 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
```

KASPERSKY lab

KNOWN MALICIOUS BEHAVIOR: DINIHOU WORM

How to create Snort/Suricata rule?

Suricata

```
alert http $HOME_NET any -> $EXTERNAL_NET any \
(msg:"Dinihou worm"; flow:established,to_server; \
content:"POST"; http_method; \
content:"|3c 7c 3e|nan-av|3c 7c 3e|"; http_user_agent; \
classtype:trojan-activity; \
reference:url,threats.kaspersky.com/en/threat/Worm.VBS.Dinihou/; \
sid:1000005; 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
```

KASPERSKY lab

SURICATA RULES CREATING
GENERIC SILENT RULES FOR INTERCEPTED TRAFFIC

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

```
alert http $HOME_NET any -> $EXTERNAL_NET any \
(msg:"Probably Trojan-Spy.Win32.Noon"; \
flow:to_server,established; \
content:"GET"; http_method; \
content:"/?id="; http_uri; fast_pattern; \
pcre:"/^\/[a-zA-Z0-9/]+\/\?id\=/U"; \
http_header_names; content:"Host"; \
classtype:unknown; sid:1000006; rev:1;)
```

SURICATA RULES CREATING
AVOIDING FALSE ALARMS

Noon traffic:

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

False alarm:

```
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
```

```
content:"www."; http_host; startswith; \
http_header_names; content:!"Accept"; \
content:!"User-Agent"; \
```

SURICATA RULES CREATING
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
```

SURICATA RULES CREATING
EXACT REGULAR RULES FOR INTERCEPTED TRAFFIC

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

```
alert http $HOME_NET any -> $EXTERNAL_NET any \
(msg:"Trojan-Spy.Win32.Noon Checkin"; \
flow:to_server,established; \
content:"GET"; http_method; \
content:"/?id="; http_uri; fast_pattern; \
pcre:"/^(\/[a-zA-Z0-9]{2,5})+\/\?id\=[a-zA-Z0-9\/.&+=_-]+$/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:1000007; rev:1;)
```

RULES FOR DNS QUERIES

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;)
```

RULES FOR DNS QUERIES

example.com

Suricata syntax – 1

```
alert dns any any -> any 53 \
(msg:"example.com DNS query"; \
dns_query; \
content:"|07|example|03|com|00|"; \
classtype:unknown; \
sid:1000009; rev:1;)
```

RULES FOR DNS QUERIES

example.com

Suricata syntax – 2

```
alert dns any any -> any 53 \
(msg:"example.com DNS query"; \
dns_query; \
content:"example.com"; endswith; \
classtype:unknown; \
sid:1000010; rev:1;)
```

DNS TUNNELING

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

denis0X.pcap

marcher.pcap

RAW TCP TRAFFIC

- Usually RE the malware looking for specific bytes transferred
- Sometimes just compare several traffic dumps

spy.pcap

tRat.pcap

FIXING FALSE ALARMS

Gh0st RAT

```
alert tcp any any -> any !25 \
(msg:"Gh0st Trojan CnC"; \
dsize:<250; \
content:"Gh0st"; offset:8; depth:5;\
classtype:trojan-activity; sid:1000011; rev:1;)
```

FIXING FALSE ALARMS

Gh0st RAT

```
.......Gh0st.N3v......2!d......IH;:..-21T#$28Z...
...(....\\......c`r.*...J..
pf ..9....a.i.......xCs.3C..}hd`h.k`.kh.``dehI..#kN..~..K..08....F........?._
```

```
....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.
```

Not Gh0st

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

zegost01.pcap
zegost02.pcap

KASPERSKY lab

FIXING FALSE ALARMS

Gh0st RAT

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

Fix:

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

Thank you!

Tatyana.Shishkova@kaspersky.com

Twitter: @sh1shk0va

KASPERSKY lab