METADATA IS LIKE GOLD, TIPS & TRICKS TO MINE IT!

Guy Bruneau
Senior Security Consultant
IPSS Inc.
@GuyBruneau

#RSAClare
ABOUT ME

- Senior Security Consultant @IPSS Inc.
- Incident Handler @Incident Storm Center
  - gbruneau@isc.sans.edu
- Experience: Planned, deployed, and used NetWitness 8.x to 10.6.x in medium and enterprise environments
AGENDA

- Why collect metadata?
- Tuning your data collection
- Build your network model
- Truncating payload
- Tuning Broker, Concentrator and Decoder
- Metadata search examples
WHY COLLECT METADATA?

- Metadata to assist with initial response
- Support for continuous monitoring and alert on potential threats
- Metadata aids retrospective analysis in an ongoing investigation

- This is the data that can be used to validate an alert
- Deep dive into an alert that triggers a potential incident
- The investigation is likely to take place over a large volume of data

GOAL IS MINING QUALITY DATA!
The primary goal is to detect and investigate incidents
- What, When, Where, How, and possibly Who/Why

Forensics is all about meta
- Creating, querying, and reporting

Answer basic questions → conversation between client/server (i.e. flows)
- Timestamp, Source/Destination Address/Port, site(s) involved, data volume exchange

Increase retention and performance by keeping only useful meta for analysis
- Improve response to queries
IMPROVING CAPTURE, DETECTION & RETENTION

NETWITNESS TUNING
MAKE NETWITNESS YOUR PARTNER
IDENTIFY YOUR NETWORK ON THE FLY

▪ Building your asset model is **well worth your time!**
▪ Identify IP ranges and names
▪ Categorize & prioritize business assets and networks
  - Build decoder network asset model in → `traffic_flow_options.lua` (Config, Files)
  - Identify which networks should *never exchange data*
    - Create decoder Application Rule(s) to alert on this unusual behavior
▪ Track anomalies
  - Generate automated reports or notifications

```
["192.168.2.5/32"] = "Proxy",
["192.168.24.0/24"] = "VPN",
["192.168.25.0/25"] = "Servers",
["192.168.25.128/25"] = "Hosts",
```

**Network Name** (14 values)

- other dst (7,580) - proxy src (4,938) - servers dst (4,258) - servers src (4,011) - hosts src (2,520) - other misc (2,040) - other src (717)
- proxy dst (253) - hosts dst (114) - broadcast src (37) - broadcast dst (18) - hosts misc (8) - servers misc (1) - proxy misc (1)
IMPROVE DECODER PERFORMANCE AND EXTEND GOOD TRAFFIC RETENTION

- BPF filter (Proto 47, 50, 51) on a decoder
  - **Note**: need to use Network Rules with PF_Ring enabled cards
- If you cannot decrypt SSL, keep the metadata and truncate the payload
- Truncate video content with an App Rule: `content begins "video"`
- Delete unused Parsers
- Turn off non necessary metadata keys

![GeoIP Table]
In-house metadata feeds → better detection
- Immediate flagging of your own Threat Intelligence
  - If decoder parses traffic from/to IP 10.3.25.6 then generate new meta (result: meta key = monitoring)

Custom feed for in-house monitoring & detection (including reporting)
- select ip.dst where monitoring exists && streams = 1 && direction = 'inbound'
- select asn.src where asn.dst = 1234

Application rules
- Tag unusual activity (Alert = alert.id)
  - nw00005 = attachment count 4-u
- Filter out traffic (Session Data = filter)
  - Drop Broadcast to 192.168.25.255 = ip.dst=192.168.25.255
- Decoder monitor meta to create new meta (Alert = threat.source)
  - Cisco AMP ThreatGrid = tg.analysis exists
A conversation has two parties: client → server
- Portscan without response is streams = 1
- select tcp.dstport where ip.dst = 192.168.2.5 && tcp.flags = 2 && streams = 1 && direction = 'inbound'

Not all metadata is indexed

Some meta is never or rarely queried
- Previous example: GoIP → Latitude, Longitude, City, Organization

To add indexing to previous captured metadata
- Need to change IndexValues to IndexKeys
- Restart Broker/Concentrator
- It immediately applies to all previously captured metadata...

Streams default setting → not indexed
ADDITIONAL INDEXING EXAMPLES

Not all meta is indexed

- `<key description="Session Streams" format="UInt8" level="IndexValues" name="streams" valueMax="2"/>
- `<key description="Filename" format="Text" level="IndexValues" name="filename" valueMax="500000"/>
- `<key description="Directory" format="Text" level="IndexValues" name="directory" valueMax="500000"/>
- `<key description="Request Payload" level="IndexValues" name="requestpayload" format="UInt32" valueMax="200000"/>
- `<key description="Response Payload" level="IndexValues" name="responsepayload" format="UInt32" valueMax="200000"/>

ASN feed example: https://community.rsa.com/thread/192914
MALWARE ANALYSIS

- Do you have multiple Malware Analysis brokers?
- Tune the decoder AppRule for better analysis

```
corporate.spectrum content = 'spectrum.consume' && netname = 'servers.src' content
```

- Update Malware Analysis query (config, general)

```
Query select * where content='corporate.spectrum'
```

- This can process hundreds of files per hour
INVESTIGATION, SAMPLE QUERIES AND HUNTING

DIVING INTO DATA
CUSTOM INVESTIGATION EVENTS DISPLAY

Mail → service = 25
- did
- ip.src
- ip.dst
- alias.host
- direction
- email.src
- email.dst
- subject
- Attachment
- email.url.host
- country.src
- errors
- threat.category
- risk.suspicious
- streams

Web → service = 80
- did
- ip.src
- ip.dst
- alias.host
- direction
- query
- referer
- action
- directory
- filename
- requestpayload
- responsepayload
- country.dst
- threat.category
- risk.suspicious
- session.split
- streams

DNS → service = 53
- did
- ip.src
- ip.dst
- alias.host
- alias.ip
- direction
- dns.querytype
- Error
- requestpayload
- responsepayload
- country.src
- country.dst
- threat.category
- risk.suspicious
- streams

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Event Type</th>
<th>Src IP</th>
<th>Dst IP</th>
<th>Hostname</th>
<th>Action</th>
<th>Directory</th>
<th>Filename</th>
<th>Content Type</th>
<th>Result Code</th>
<th>Req Payload</th>
<th>Resp Payload</th>
<th>Net Name</th>
<th>Streams</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-09-01T20:33:28</td>
<td>Network</td>
<td>192.168.2.25</td>
<td>23.45.108.56</td>
<td>cdn.content.prod.cms...</td>
<td>GET</td>
<td>/singletile/su...</td>
<td>today</td>
<td>text/xml</td>
<td>200</td>
<td>3064</td>
<td>3064</td>
<td>Proxy src</td>
<td>2</td>
</tr>
<tr>
<td>2017-09-01T20:33:28</td>
<td>Network</td>
<td>192.168.2.25</td>
<td>23.45.198.56</td>
<td>cdn.content.prod.cms...</td>
<td>GET</td>
<td>/singletile/su...</td>
<td>today</td>
<td>text/xml</td>
<td>200</td>
<td>394</td>
<td>1666</td>
<td>Proxy src</td>
<td>2</td>
</tr>
</tbody>
</table>
How NetWitness services meta info works?

Service for all web traffic is 80 but...
- service = 80 → means web on any ports (65535)

**Exception** → service = 0
- Bucket for all services that are not parsed natively
- Excellent place to search for anomalous traffic
- Remove inbound portscans first
  - service = 0 && streams != 1 && asn.dst = 1234
- Review protocols and unusual payloads
  - service = 0 && streams = 2 && ip.proto = 17 && payload = 100-u
- Analyze what is left
Traffic from/to IP 192.168.25.5

- Traffic from/to IP 192.168.25.5

Display all traffic to destination port 80 that isn’t identified as web traffic

- Displays all traffic to destination port 80 that isn’t identified as web traffic

Who accessed website adobe.flash-player-v12.com and was an EXE downloaded?

- Who accessed website adobe.flash-player-v12.com and was an EXE downloaded?
- alias.host = 'adobe.flash-player-v12.com' && directory = '/update' && filename = 'exe.exe'

Who is port scanning my network ASN 1234?

- Who is port scanning my network ASN 1234?
INDEX METADATA = POWER SEARCHES

- Stitching meta keys together = target search
  - service = '80' && filename = 'Today.xml'
  - ip.src != 10.1.8.0/24 && ip.proto = 6 && streams = 1 && tcp.flags = 2
- Exception! Backscatter Synflood
  - streams = 1 && payload = 0 && service = 0 && tcp.flags = 18
    - Viewed by Security Analytics

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2015-08-14 07:59:31 955197</td>
<td>50.115.126.69</td>
<td>99.246.21.179</td>
<td>TCP</td>
<td>60</td>
<td>80-34455 [SYN, ACK]</td>
</tr>
</tbody>
</table>

- Viewed by Wireshark
REPORTING

- **Rules**: report query structure
  - Highest efficiency: ASN & netname
- **Reports**: ad-hoc or scheduled
  - nwsdk_csv.py + netwitness_sdk.sh
- **Charts**: regular updates of a match rule
- **Alert**: triggers on a rule match
- **Lists**: define and update lists used in a rule
- **Decoders daily and past monthly report**
  - Tracks daily & monthly changes
  - Decoder/Concentrator retention

<table>
<thead>
<tr>
<th>Decoders</th>
<th>Total session size in bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>dec1</td>
<td>19.2 GB</td>
</tr>
<tr>
<td>logdec1</td>
<td>53.71 MB</td>
</tr>
</tbody>
</table>
FEEDBACK AND SHARING IS IMPORTANT!

- Provide feedback to your RSA contact
- Submit feature enhancement requests that would benefit everyone
- Participate in the community
  - Share parsers, feeds, techniques, ideas
  - NetWitness CMD Meta Parser
    https://community.rsa.com/message/897773
  - ASN feed parser
    https://community.rsa.com/thread/192914
  - NetWitness statistics script
    https://community.rsa.com/thread/192962

Oldest Meta - Concentrators

Concentrator 1 - 2017-Aug-01 18:34:16

Oldest Packets/Logs - Decoders

Decoder 1 - 2017-Jun-11 17:06:29
LogDecoder 1 - 2017-Mar-10 00:46:04

Decoders Uptime and Dropped Packet

Decoder 1 - 22 hours 44 minutes 3 seconds, 10 weeks 6 days 14 hours 59 minutes 31 seconds
Decoder 1 Packet Dropped - 0
LogDecoder 1 - 22 hours 33 minutes 44 seconds, 23 weeks 5 days 23 hours 6 minutes 11 seconds
LogDecoder 1 Packet Dropped - 0
SUMMARY & TAKE AWAY

- Tune, tune, tune - never stop tuning
- NetWitness network forensics is all about metadata!
- Keep only forensically sound meta for analysis
  - Review all parsers and meta keys collection (i.e. GeoIP meta)
- Categorize & prioritize business assets and networks
  - Take time to accurately define your network model in `traffic_flow_options.lua`
- Truncate SSL, videos, VPN, etc
  - Result → extend packet retention
Q&A?

- My contact information
  - gbruneau@ipss.ca or gbruneau@isc.sans.edu
  - @GuyBruneau
  - https://www.linkedin.com/in/guybruneau

- Posts & Projects
  - https://isc.sans.edu
  - http://handlers.sans.org/gbruneau
THANK YOU

METADATA IS LIKE GOLD
TIPS & TRICKS TO MINE IT!