Monitoring, Detection and Reporting of Security Incidents in CESNET NREN

Vaclav Bartos, Pavel Celeda, Tomas Kreuzwieser, Viktor Pus, Petr Velan, Martin Zadnik
Motivation

- Monitoring and detecting threats
- Incident handling and network troubleshooting
- Trends
Architecture

- Meters and exporters
- Collector
- Preprocessing
- Analysis
- Detection
- Reporting
Metering

- External links from/to CESNET2
- Speed full duplex 10 Gbps lines
- At some points Channel bonding
Meter architecture

- Standalone probe based on specialized network cards
- Packet parsing and DMA distribution
Meter architecture

- Applications:
  - flow monitoring,
  - tcpdump,
  - DPI

- Exporter – technology transfer with industry
  - INVEA-TECH Flow Exporter
  - Extensible using plugins
  - Export in IPFIX or NetFlow
Collector

- IPFIXcol
  - Modular collector
  - Extensible with internal plugins
Preprocessing

- Flow deduplication
- Flow aggregation
- Separation of transit and CESNET traffic
Analysis

• IP profile
  • Compute statistics per each IP address and interesting applications per 5 minute interval
  • volumes,
  • flags,
  • unique IPs

• Observe URLs

• Model IP prefix space
Detection

- Scanning
- Flooding
- Spoofing
- Password cracking
- Malware
Scanning & flooding

- Communication asymmetry
- Connection resets
- Behavioral patterns with absolute and floating thresholds (predictor + CUSUM)
- Verification in flow data
  - Horizontal, vertical, single port
Scanning & flooding

- Even a good pattern may fail
- Example
  - The reflection of DoS attack from CESNET network detected as massive scanning activity
Spoofing

- Spoofing as a symptom of DoS
- Detection based on
  - Bogon prefixes
  - Model of outgoing traffic is matched against incoming
  - Model source prefixes seen on entry points in the past
  - Model number of prefixes per destination prefix
Spoofing

- Bogon example
Spoofing

- New prefixes per each destination

![Graph showing number of new source prefixes over time](chart.png)
Password cracking

- SSH scan
- SSH password bruteforce
- RDP scan
- RDP password bruteforce
- Behavioral patterns
- Absolute thresholds
Botnets

- Behavioral pattern
- E.g. Command and Control Protocol for ZeroAccess/Sirefef malware

<table>
<thead>
<tr>
<th>Proto</th>
<th>Src IP Addr:Port</th>
<th>Dst IP Addr:Port</th>
<th>Out Pkt Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>0.0.119.9:49153</td>
<td>0.0.253.254:16470</td>
<td>147</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.119.9:49153</td>
<td>0.0.253.254:16470</td>
<td>344</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.119.9:49153</td>
<td>0.0.253.254:16470</td>
<td>147</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.119.9:49153</td>
<td>0.0.253.254:16470</td>
<td>134</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.119.9:49153</td>
<td>0.0.253.254:16470</td>
<td>145</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.119.9:49153</td>
<td>0.0.253.254:16470</td>
<td>170</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.119.9:49153</td>
<td>0.0.253.254:16470</td>
<td>115</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.119.9:49153</td>
<td>0.0.253.254:16470</td>
<td>175</td>
</tr>
</tbody>
</table>
Reporting

• Detected incidents are automatically reported to Warden
• Warden – automated and shared reporting of threats in CESNET2 network

• Incidents that are not private from the perspective of CESNET are about to be reported to NfQuery
• We also run NfQuery to correlate multi-domain incidents
Trends

- Flow characteristics
Trends

- IPv6 tunneling mechanisms
- Tunnels usually bypass firewalls
- Plugins to extend flow with tunnel info

<table>
<thead>
<tr>
<th></th>
<th>March 2019</th>
<th>March 2020</th>
<th>March 2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Native IPv6</td>
<td>71.230%</td>
<td>69.592%</td>
<td>71.290%</td>
</tr>
<tr>
<td>Teredo</td>
<td>26.598%</td>
<td>27.660%</td>
<td>24.143%</td>
</tr>
<tr>
<td>6to4</td>
<td>2.167%</td>
<td>2.747%</td>
<td>4.548%</td>
</tr>
<tr>
<td>Other</td>
<td>0.004%</td>
<td>0.002%</td>
<td>0.018%</td>
</tr>
<tr>
<td>ISATAP</td>
<td>0.000%</td>
<td>0.000%</td>
<td>0.000%</td>
</tr>
</tbody>
</table>
Conclusion

• Monitoring CESNET perimeter
• Global view on the network state
• Detection techniques may reveal suspicious activity which is reported
• Incidents are automatically reported to reporting systems
• But the action must be done manually
Future work

• 100G traffic monitoring using new concept
  • NetFlow
  • DPI
  • See poster: Software Defined Monitoring: A New Approach to Network Traffic Monitoring

• Combine multiple sources
• Include more and more detection mechanisms
• Correlate detected events
• Model long-term behavior and reputation