Implementing a country-wide sensor infrastructure for proactive detection of malicious activity

Rildo Souza
Regarding the RNP

- Brazilian National Research and Education Network (RNP).
- Created in 1989.
- Implemented the first Latin American fiber network in 2005.
Regarding CAIS

- Coordination CSIRT of Brazilian research and education network since 1997.
- CAIS works in detection, resolution and prevention of network security incidents.
Motivations to create a network CAIS Sensor

• Highly diversified environment, networks, technologies and maturity of customer’s security teams.

• Increasing our capacity to detect malicious activities.

• Understanding and support better the security actions from our clients.
CAIS Sensor Requirements

- Plug and play
- Scalable
- Free software
- Easy administration
What is CAIS Sensor?
How does the CAIS Sensor analyze traffic?
How does the CAIS Sensor analyze traffic?
How does the CAIS Sensor Works?

Master Server

Engine (Suricata)  Engine (Suricata)  Engine (Suricata)

+ HTTPS + IP + Query
What does the Master Server do?

- Sensor management
- Sensor’s system updates management
- Statistics on malicious activities detected
- Information about sensor’s “health”
- System general administration
Regarding Engines (Suricata)

- Friendly user interface
- Plug and play
- Less technical knowledge required
- Low maintenance and support
  - Send detections by email
  - Send statistics and status data
  - Update requests
The CAIS Sensor (Screenshots)
The CAIS Sensor (Screenshots)

<table>
<thead>
<tr>
<th>Type</th>
<th>Source</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>General rules</td>
<td>Emerging Threats</td>
<td>Provide general rules</td>
</tr>
<tr>
<td>Customized rules</td>
<td>CAIS</td>
<td>Provide specific rules, on demand.</td>
</tr>
<tr>
<td>Rule Exceptions</td>
<td>CAIS</td>
<td>Disable rules without need generate new release.</td>
</tr>
<tr>
<td>URL Blacklist</td>
<td>CAIS / APWG / Fraud Catalog Service, etc.</td>
<td>Identify malicious URLs access</td>
</tr>
<tr>
<td>IP Blacklist</td>
<td>CAIS / Shadow Server, etc.</td>
<td>Identify malicious IP access, like C&amp;C</td>
</tr>
<tr>
<td>Networks</td>
<td>CAIS</td>
<td>Each client has its own network, so the each one variable HOME_NET must be unique, for greater assertiveness.</td>
</tr>
<tr>
<td>System updates</td>
<td>CAIS</td>
<td>New sensor system's versions and features, and corrections.</td>
</tr>
</tbody>
</table>
Engine(Screenshots) – Installation Menu

- Network interface configuration.
- Select network pickup interface.
- Put the token.
- Restart Services.
Implementation of CAIS Sensor

- 27 RNP Points of Presence
- 17 Customers
- 44 Sensors Installed
Statistics – Average Analyzed Traffic
Statistics

Malicious activity flow

- Incoming: 91%
- Outgoing: 9%

Most attacked ports

- Port 23: 43%
- Port 80: 15%
- Port 22: 10%
- Port 177: 4%
- Port 5358: 3%
- Others: 25%
Statistics - Main types of malicious activity detected

<table>
<thead>
<tr>
<th>Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDoS Attempts (protocol xdmcp)</td>
<td>702,345</td>
</tr>
<tr>
<td>DDoS Attack (protocol NTP)</td>
<td>535,204</td>
</tr>
<tr>
<td>Malwares</td>
<td>236,985</td>
</tr>
<tr>
<td>DDoS Attack (protocol SNMP)</td>
<td>102,478</td>
</tr>
</tbody>
</table>
Statistics – Types of detected events

- BITCOIN MINER
- DDoS
- Torrent
- BOT
## Statistics - Botnets

<table>
<thead>
<tr>
<th>Botnet</th>
<th>Botnet</th>
<th>Botnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>nicaze.net</td>
<td>Zeus</td>
<td>XcodeGhost</td>
</tr>
<tr>
<td>PCRat/Gh0st</td>
<td>Kelihos</td>
<td>Bladabindi/njrat</td>
</tr>
<tr>
<td>Beacon</td>
<td>Feodo</td>
<td>Palevo</td>
</tr>
<tr>
<td>DealPly</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Next Steps

• Optimize reports

• Integrate with other sources (URLs blacklist, IPs blacklist, others)

• Increase number of sensors in educational institutions and RNP customers

• Finalize and expand the partnership model
Questions ?
Thank You!

The Brazilian Academic and Research Network

Rildo Souza
Security Analyst
rildo.souza@rnp.br