The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents.

CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg.
CIRCL Services

- Incident ticket creation for reported **ICT incidents** via different media (e.g. international CSIRT channels, national incident reports,...)

- Incident identification and **triage**

- **Technical investigation** including information correlation (e.g. security vulnerability/incidents matching, similar incident resolution, malware reversing, system and network forensic...)

- Incident coordination might also include **vulnerability handling**, responsible vulnerability disclosure (e.g. the software originating the incident) or incident response training

- Services availability to organizations/citizen incorporated in Luxembourg
Sharing indicators

• In order to improve sharing of Indicators of Compromise (IOCs), MISP was introduced in 2013:

  • Sharing indicators about targeted attacks.
  • Improve detection time of unknown malware.
  • Avoid reversing similar malware (focusing on new analysis).
MISP overview

Legend:
- Operated by CIRCL
- Operated by NATO/NCIRC
- Operated by other organizations
What kind of attributes are shared in MISP?

- Hashes of malware (MD5, SHA1, SHA256).
- IP addresses, ASN numbers.
- Hostnames and domain names.
- Patterns in file, disk or memory.
- Named pipes, mutexes.
- Malware family.
- Vulnerability related (CVE Numbers).

These indicators can be used to search for potential compromised systems in network logs (proxy, firewall), system log.
What are other benefits?

- Attackers and adversaries can be lazy. They reuse infrastructures and techniques.
- You can find relationships between the attackers’ campaigns and the indicators.

<table>
<thead>
<tr>
<th>domain</th>
<th>ip-dst</th>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td>icanhazip.com</td>
<td>188.123.34.203</td>
<td>C&amp;C</td>
</tr>
<tr>
<td></td>
<td>5.44.15.70</td>
<td>C&amp;C</td>
</tr>
<tr>
<td></td>
<td>188.255.212.27</td>
<td>C&amp;C</td>
</tr>
<tr>
<td></td>
<td>217.23.194.237</td>
<td></td>
</tr>
<tr>
<td></td>
<td>31.42.170.198</td>
<td></td>
</tr>
<tr>
<td></td>
<td>93.184.71.88</td>
<td></td>
</tr>
<tr>
<td></td>
<td>194.28.190.84</td>
<td></td>
</tr>
<tr>
<td></td>
<td>195.34.206.204</td>
<td></td>
</tr>
<tr>
<td></td>
<td>46.180.147.50</td>
<td></td>
</tr>
<tr>
<td></td>
<td>91.187.75.75</td>
<td></td>
</tr>
<tr>
<td></td>
<td>109.86.176.37</td>
<td></td>
</tr>
<tr>
<td></td>
<td>31.28.115.88</td>
<td></td>
</tr>
</tbody>
</table>
Sharing indicators not detected by AntiViruses

- Indicators are often shared before they are detected by A/V.
- Dridex malware sample in April 2015:
Statistics

- 145732 attributes in MISP for private sector.
- 27920 correlated attributes (at least shared between two events).
- 117 international companies and organizations are on the MISP platform.
Future

- Pseudonimity
- STIX Import
- TAXII for sharing between instances
- Improvements in the API
- Request Policy Zone Configuration export
- VirusTotal integration
- SMIME
- New attributes

What else do *you* need?

For bugs or features requests:
https://github.com/MISP/MISP/issues
Conclusion

• Fetching indicators from MISP and searching internally is already a quick win.
• Contributing is not required but it’s enhancing the global view on who already seen/worked on such attack.
• Small incidents can be the origin of ”complex targeted attacks”.
• All the CERTs can request an access to the platform
• Sharing of indicators can be also done anonymously via CIRCL if required.
Contact

- info@circl.lu
- https://www.circl.lu/
- OpenPGP fingerprint: 3B12 DCC2 82FA 2F5B 709A 09E2 CD49 44E6 CBCD