Resources of CSIRT (Tools and Services of CIRT/CSIRT)
FIRST Services
Security Incident Response Team (SIRT) Services Framework.
<table>
<thead>
<tr>
<th>Services Area</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident management</td>
<td>Incident handling</td>
</tr>
<tr>
<td></td>
<td>Incident Analysis</td>
</tr>
<tr>
<td></td>
<td>Incident Mitigation and recovery</td>
</tr>
<tr>
<td>Analysis</td>
<td>Artifact Analysis</td>
</tr>
<tr>
<td></td>
<td>Media Analysis</td>
</tr>
<tr>
<td></td>
<td>Vulnerability / Exploitation Analysis</td>
</tr>
<tr>
<td>Information assurance</td>
<td>Risk Management</td>
</tr>
<tr>
<td></td>
<td>Compliance Management</td>
</tr>
<tr>
<td></td>
<td>Operating Policies Support</td>
</tr>
<tr>
<td></td>
<td>Business Continuity and Disaster Recovery Planning Support</td>
</tr>
<tr>
<td></td>
<td>Technical Security Support</td>
</tr>
<tr>
<td></td>
<td>Patch management</td>
</tr>
<tr>
<td>Situational Awareness</td>
<td>Sensor Operation</td>
</tr>
<tr>
<td></td>
<td>Fusion and Correlation</td>
</tr>
<tr>
<td></td>
<td>Development and Curation of Security Intelligence</td>
</tr>
<tr>
<td>Outreach/ Communications</td>
<td>Security Awareness Raising</td>
</tr>
<tr>
<td></td>
<td>Cybersecurity Strategic Policy Advisement</td>
</tr>
<tr>
<td></td>
<td>Knowledge Sharing and Publications Dissemination</td>
</tr>
<tr>
<td>Capability Development</td>
<td>Organizational Metrics</td>
</tr>
<tr>
<td></td>
<td>Training and Education</td>
</tr>
<tr>
<td></td>
<td>Lesson learned analysis</td>
</tr>
<tr>
<td></td>
<td>Conducting Exercises</td>
</tr>
<tr>
<td></td>
<td>Development of Vulnerability Discovery/Analysis/Remediation/Root Cause Analysis</td>
</tr>
</tbody>
</table>
SALAMA
SLAMA CIRT

Services
The Basic Services Offered by a National CIRT

National CIRT

Service

SERVICE AREA

INCIDENT MANAGEMENT
- Incident handling
- Incident analysis
- Incident mitigation and recovery

ANALYSIS
- Artifact analysis

SITUATION AWARENESS
- Development and curation of security Intelligence

INFORMATION ASSURANCE
- Risk Management

OUTREACH AND COMMUNICATION
- Security Awareness Raising
- Knowledge Sharing and Publications Dissemination

Consulting and Technical Assistance Department

Awareness And Communication Department

Incident Response Center
Mapping FIRST framework and ITU Approach

Service Area

Service

Function

- Incident Validation and Classification
- Incident Tracking
- Information Collection
- Coordination and reporting

- Impact Analysis
- Mitigation Analysis
- Recovery Analysis

- Containment
- Restore confidentiality, integrity, availability

- Surface Analysis
- Reverse Engineering
- Run Time Analysis
- Comparative Analysis

- Source Identification and Inventory
- Source Content Collection and Cataloging
- Information sharing

- Risk Assessment
- Risk Assessment Advice

- Public Service Announcements
- Publication/Dissemination of Information

- Incident Handling

- Incident Analysis

INCIDENT MANAGEMENT

- Incident mitigation and recovery

ANALYSIS

- Artifact analysis

SITUATIONAL AWARENESS

- Development and curation of security intelligence

INFORMATION ASSURANCE

- Risk Management

OUTREACH / COMMUNICATION

- Technical Security Support
- Security Awareness Raising

- Knowledge Sharing and Publications Dissemination

National CIRT
SLAMA CIRT

Tools
The Basic Services Offered by a National CIRT

SERVICE AREA

INCIDENT MANAGEMENT
- Incident handling
- Incident analysis
- Incident mitigation and recovery

ANALYSIS
- Artifact analysis

SITUATION AWARENESS
- Development and curation of security Intelligence

INFORMATION ASSURANCE
- Risk Management

OUTREACH AND COMMUNICATION
- Security Awareness Raising
- Knowledge Sharing and Publications Dissemination

National CIRT

Consulting and Technical Assistance Department

Awareness And Communication Department

Incident Response Center
Cyber Threat Intelligence System
Request Tracker for Incident Response (RTIR)

- [https://www.bestpractical.com/rtir](https://www.bestpractical.com/rtir)
- Purposely-built for CSIRT
- Developed in cooperation with many security teams to ensure it meets the needs of incident response.
Alerting and Reporting

Open Technology Real Services (OTRS)

- [http://www.otrs.com/software](http://www.otrs.com/software)
- The Flexible Open Source Service Management Software
Alerting and Reporting

osTicket

- http://osticket.com
Alerting and Reporting

CSIRT Portal

• Focal point where people will go and look for information on the CSIRT
• The portal will facilitate the distribution of information to the constituents.
• It will display latest security news, vulnerability news, advisories, etc.
Cyber Threat Intelligence System
Active Monitoring
Active Monitoring

https://github.com/Snorby
Active Monitoring
Cyber Threat Intelligence System
HoneyNet Platforms
HoneyNet Platforms

Abuse Watch Alerting & Reporting Engine (AWARE)

is a solution for cyber threats monitoring through various external sources.

Honeypot Research Network (HORNET) : HoneyNet Platform
T-POT: Honeypot platform

http://dtag-dev-sec.github.io/
Cyber Threat Intelligence System
Public Feeds

• Example of sites that provide free data feed on reported Internet abuse incidents:
  • Defacement
    o http://www.zone-h.org/archive/special=1
  • Phishing
    o https://www.phishtank.com/asn_search.php
  • Malware
    o https://www.malwaredomainlist.com/mdl.php
  • Botnet
    o https://zeustracker.abuse.ch/monitor.php
Public Feeds

• [http://map.norsecorp.com/#/](http://map.norsecorp.com/#/)

• [https://intel.malwaretech.com/pewpew.html](https://intel.malwaretech.com/pewpew.html)
Public Feeds

• Web defacement
  • [http://www.zone-h.org/archive/special=1](http://www.zone-h.org/archive/special=1)
Public Feeds

• Phishing
  • https://www.phishtank.com/asn_search.php
## Public Feeds

- **Malware**

<table>
<thead>
<tr>
<th>Date (UTC)</th>
<th>Domain</th>
<th>IP</th>
<th>Reverse Lookup</th>
<th>Description</th>
<th>Registrant</th>
<th>ASN</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016/03/06 09:35</td>
<td>marketing-material.iworld.com</td>
<td>173.255.216.191</td>
<td>lbs9-191.members.lynode.com</td>
<td>compromised site leads to Angler EK</td>
<td>Registrar Abuse Contact <a href="mailto:Abuse@web.com">Abuse@web.com</a></td>
<td>64099</td>
</tr>
<tr>
<td>2016/03/06 09:35</td>
<td><a href="http://www.saint-louis-viry.fr/infoprod/flags/documents-a-t%C3%A9l%C3%A9charger.html">www.saint-louis-viry.fr/infoprod/flags/documents-a-télécharger.html</a></td>
<td>5.135.11.9</td>
<td>-</td>
<td>compromised site leads to Angler EK</td>
<td><a href="mailto:support@alcyonweb.fr">support@alcyonweb.fr</a></td>
<td>16276</td>
</tr>
<tr>
<td>2016/03/06 14:13</td>
<td>opao.org.es/ck76hgf</td>
<td>217.160.232.13</td>
<td>clientesv.com</td>
<td>-</td>
<td>Lucky ransomware</td>
<td>-</td>
</tr>
<tr>
<td>2016/03/06 14:13</td>
<td>ministerepuissancejeunesse.pu.bm/6097h9q4qs</td>
<td>69.99.31.133</td>
<td>box333.bluehost.com</td>
<td>Lucky ransomware</td>
<td>Registrar Abuse Contact <a href="mailto:abuse@dyndot.com">abuse@dyndot.com</a></td>
<td>45009</td>
</tr>
<tr>
<td>2016/03/06 13:40</td>
<td>lihmarr.choul/lebermouffut.fr/79qhiwq</td>
<td>80.55.123.70</td>
<td>70.123.65.06.rev.sfr.net</td>
<td>Lucky ransomware</td>
<td><a href="mailto:domains@sfr.com">domains@sfr.com</a></td>
<td>13557</td>
</tr>
<tr>
<td>2016/03/08 10:58</td>
<td>Pre.viruses.org/4u89n765.exe</td>
<td>208.131.141.2</td>
<td>rageresearch.com</td>
<td>trojan</td>
<td>Gene Mathis / <a href="mailto:gom@uc.mithis.com">gom@uc.mithis.com</a></td>
<td>29653</td>
</tr>
<tr>
<td>2016/03/08 10:58</td>
<td>reda.com/4ju8n765.exe</td>
<td>198.63.208.35</td>
<td>vserv.cifetz.com</td>
<td>trojan</td>
<td>-</td>
<td>14585</td>
</tr>
<tr>
<td>2016/03/08 10:59</td>
<td>stappeaagency.free.fr</td>
<td>212.27.63.112</td>
<td>perso112-q5.free.fr</td>
<td>trojan</td>
<td>stockageonline.net</td>
<td>12232</td>
</tr>
<tr>
<td>2016/03/08 10:51</td>
<td>izey-carls.r/tu89n76b.exe</td>
<td>46.236.47.134</td>
<td>rnu047134.wabreuz.nl</td>
<td>trojan</td>
<td>-</td>
<td>34239</td>
</tr>
<tr>
<td>2016/03/07 21:39</td>
<td>softwarebd.com/73qgb334</td>
<td>59.152.100.158</td>
<td>-</td>
<td>trojan Lucky</td>
<td>-</td>
<td>63996</td>
</tr>
</tbody>
</table>
Public Feeds

• Botnet
• https://zeustracker.abuse.ch/monitor.php
Semi-Public Feeds

• Data feeds provided to non-profit organisation or specific community such as CSIRT
  • Shadow Server
  • Team Cymru
    o http://www.team-cymru.org/CSIRT-AP.html
Commercial Feeds

• Data feeds provided with paid subscription
  • Zone-H (defacement)
    o www.zone-h.org
  • Netcraft (phishing)
    o http://www.netcraft.com/anti-phishing/phishing-site-feed
  • Cyveillance (phishing and dropsites)
    o https://www.cyveillance.com/home/security-solutions/data
  • Team Cymru (botnet and malicious IP)
    o https://www.team-cymru.com/reputation-feed.html
  • Emerging Threat (malicious IP & domain)
Example of Cyber Threat Intelligence System
Collective Intelligence Framework

CIF

- Private Feed/Data
  - Your own data source can be added
- CIF Server
- Public Feeds/Data
  - Use Any public threat intel
- Pushed Daily Feeds
- Using CIF clients
- Mitigation Equipment (dnsSinkHole, Firewall, IDS)
- Users Querying indexed Feeds
Collective Intelligence Framework
CIF
Collective Intelligence Framework (CIF)

The image shows a dashboard with three sections:

1. **BOTNET IPS**
2. **MALICIOUS IPS**
3. **MALWARE DISTRIBUTION**

Each section displays a world map with various colors indicating the severity and distribution of cyber threats around the globe.

Below the maps, there is a table with columns labeled:
- source
- source_info
- severity
- country
- country_code
- data_type
- feed_ars

The table contains data for specific IP addresses, listing them in rows with corresponding values in each column.
REMnux: A Linux Toolkit for Reverse-Engineering and Analyzing Malware

MALWARE AND MEMORY FORENSICS
Example of Digital Forensic Tools
Digital Forensic Tools

The Interactive Disassembler (IDA)

https://www.hex-rays.com
Digital Forensic Tools

**Cuckoo Sandbox** is a malware analysis system.

**VirusTotal** is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

**Malwr**: Automated Malware Analysis Sandboxes and Services
The Basic Services Offered by a National CIRT

SERVICE AREA

INCIDENT MANAGEMENT
- Incident handling
- Incident analysis
- Incident mitigation and recovery

ANALYSIS
- Artifact analysis

SITUATION AWARENESS
- Development and curation of security intelligence

INFORMATION ASSURANCE
- Risk Management

OUTREACH AND COMMUNICATION
- Security Awareness Raising
- Knowledge Sharing and Publications Dissemination
Example of Security Assessment tools
Security Assessment tools

https://www.kali.org/
Security Assessment tools

https://www.tenable.com/
static code analysis

rips-scanner.sourceforge.net/
The Basic Services Offered by a National CIRT

National CIRT

- Incident Response Center
- Consulting and Technical Assistance Department
- Awareness And Communication Department

SERVICE AREA

INCIDENT MANAGEMENT
- Incident handling
- Incident analysis
- Incident mitigation and recovery

ANALYSIS
- Artifact analysis

SITUATION AWARENESS
- Development and curation of security Intelligence

INFORMATION ASSURANCE
- Risk Management

OUTREACH AND COMMUNICATION
- Security Awareness Raising
- Knowledge Sharing and Publications Dissemination
Example of Alerts, Warnings and Announcements Tools
Alerts, Warnings and Announcements Tools

https://www.phplist.com/
Alerts, Warnings and Announcements Tools

https://www.ncsc.nl/incident-response/taranis.html

Tracking, analyzing and describing threats and vulnerabilities