Our Incident Response Plan goes something like this...
WORKSHOP 16
17:00 - 18:00

Jordi Guijarro
and
Javier Berciano
CSUC
1 hour

CSIRT-KIT Project

CSIRT-KIT Project (CSUC-CSIRT, CERTSI [INCIBE], ES-CERT UPC) Computer Security Incident Response Teams (CSIRTs) are responsible for receiving and reviewing incident reports, and responding to them as appropriate. These services are normally performed for a defined constituency such as a corporation, institution, educational or government network, region or country, or a paid client. CSIRT services generally fall into three categories – reactive (e.g vulnerability alerts, incident handling); proactive (e.g. intrusion detection, auditing and information dissemination); and security quality management (e.g. risk analysis, disaster recovery planning, and education and training). During the session, we’ll explore and “play” with a collection of CERT’s daily used opensource tools for handling security incidents. (A live image will be provided where tools like RTIR, IntelMQ, Nfsen, and Pakiti are included).
Problems

- Missing cooperation
- Incomplete monitoring
- Non-existent experience
- No emergency plan
- Very low awareness
TF-CSIRT Mission

The mission of TF-CSIRT is to facilitate and improve the collaboration between the European CSIRT community to make cyberspace a better place.
Your Security Response Toolkit

This site offers a proposed collection of tools in a plug&play live image to provide first steps to new incident handling teams. Information on this site reflects the experience of a number of European CSIRTs, with tools used and supported by active CSIRTs.

START!

CSIRT-KIT workshop

@jordiguijarro @jberciano borja.guaita@csuc.cat

WITH COLLABORATION OF

CSUC - Consorci de Serveis Universitaris de Catalunya
INCIBE - Instituto Nacional de Ciberseguridad
ESCERT - European Security Certification Expertise and Resource Team
Tools ecosystem: Csirt-kit inspiration!
Disk Image (OVA)
**Incident handling information**

*IntelMQ* is a solution for CERTs for collecting and processing security feeds, pastebins, tweets and log files using a message queuing protocol.

https://intelmq.org/
- Automatic feeds injection and processing
- Easy to configure and change (Python)
- GUI (IntelMQ Manager)
- Opensource
- Various output results («enrichment» with expert bots)
  - ASN lookup
  - Abuse contact
  - Whois
  - GeoIP
  - DNS lookups
  - Filters.

https://intelmq.org/
https://intelmq.org/
Malware Information Sharing Platform

http://www.misp-project.org/
Facilitate the storage of technical and non-technical information about malware and attacks

Create automatically relations between malware and their attributes

Store data in a structured format (allowing automated use of the database to feed detection systems or forensic tools)

Generate rules for Network Intrusion Detection System (NIDS) that can be imported on IDS systems (e.g. IP addresses, domain names, hashes of malicious files, pattern in memory)
Objective

- Share malware and threat attributes with other parties and trust-groups
- Store locally all information from other instances (ensuring confidentiality on queries)
- Create a platform of trust - trusted information from trusted partners
- Improve malware detection and reversing to promote information exchange among organizations (e.g. avoiding duplicate works)
MISP (Malware information Sharing Platform)

Source: http://circl.lu/services/misp-malware-information-sharing-platform/
Model

Incident affecting strategic company

IOC without victim information

Threat Intelligence

User 1

User 2

User N

Web access without misp

Federation with strategic company misp

CERTSI

MISP

MISP

Company
Ransomware spread through a “Certified mail” campaign.

**Event ID:** 173

**Org:** INCIBE

**Date:** 2016-08-30

**Analysis:** Completed

**Distribution:** All communities

**Description:** Ransomware spread through a “Certified mail” campaign impersonating Correos (Spanish national postal service)

**Published:** Yes

**Related Events**

- 2016-06-01 (144)
- 2016-04-27 (2564)
- 2015-02-12 (829)

<table>
<thead>
<tr>
<th>Date</th>
<th>Org</th>
<th>Category</th>
<th>Type</th>
<th>Value</th>
<th>Comment</th>
<th>Related Events</th>
<th>IDS</th>
<th>Distribution</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-08-30</td>
<td></td>
<td>External</td>
<td>link</td>
<td><a href="https://www.hybrid-analysis.com/sample">https://www.hybrid-analysis.com/sample</a></td>
<td>Analysis of Corp_Certificado.js</td>
<td>No</td>
<td>Inherit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016-08-30</td>
<td></td>
<td>Internal</td>
<td>link</td>
<td><a href="https://ympont.in/coro.eu/RTF/Search">https://ympont.in/coro.eu/RTF/Search</a></td>
<td>Incidencias en rtr</td>
<td>No</td>
<td>Organisation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016-06-02</td>
<td></td>
<td>Internal</td>
<td>text</td>
<td>[CCBC7EC0]</td>
<td>campaign.tag</td>
<td>No</td>
<td>Organisation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016-06-02</td>
<td></td>
<td>Internal</td>
<td>text</td>
<td>[ae0-df]<em>[1]+[ae0-df]</em>[correos11]</td>
<td>hostname-mangling</td>
<td>No</td>
<td>Organisation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016-08-30</td>
<td></td>
<td>Payload</td>
<td>domain</td>
<td>dogus.edu.tr</td>
<td>Compromised domain</td>
<td>Yes</td>
<td>Inherit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016-08-30</td>
<td></td>
<td>Payload</td>
<td>domain</td>
<td>correosserver17.org</td>
<td>Malicious domain registered 2016-08-30</td>
<td>Yes</td>
<td>Inherit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### IB-16-20238 Indicators of Compromise Associated with Mi...

**Event ID:** 3305  
**Uaid:** 5810467e-4160-43ad-94be-2e10c8a998dc  
**Org:** NCBE  
**Contributors:**  
**Tags:**  
**Date:** 2016-10-26  
**Threat Level:** Low  
**Analysis:** Complex  
**Distribution:** All communities  
**Description:** IB-16-20238: Indicators of Compromise Associated with Mirai Botnet  
**Published:** Yes

#### DB Table

<table>
<thead>
<tr>
<th>Date</th>
<th>Org</th>
<th>Category</th>
<th>Type</th>
<th>Value</th>
<th>Comment</th>
<th>Related Events</th>
<th>IDS</th>
<th>Distribution</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-10-26</td>
<td></td>
<td>Network activity</td>
<td>hostname</td>
<td>report suckeditterjoh.cf</td>
<td>Command and Control</td>
<td></td>
<td>Yes</td>
<td>Inherit</td>
<td></td>
</tr>
<tr>
<td>2016-10-26</td>
<td></td>
<td>Network activity</td>
<td>hostname</td>
<td>network.org</td>
<td>Command and Control</td>
<td></td>
<td>Yes</td>
<td>Inherit</td>
<td></td>
</tr>
<tr>
<td>2016-10-26</td>
<td></td>
<td>Network activity</td>
<td>hostname</td>
<td>lsatmaoritterjoh.cf</td>
<td>Command and Control</td>
<td></td>
<td>Yes</td>
<td>Inherit</td>
<td></td>
</tr>
<tr>
<td>2016-10-26</td>
<td></td>
<td>Network activity</td>
<td>hostname</td>
<td>ir.lisiteo.work</td>
<td>Command and Control</td>
<td></td>
<td>Yes</td>
<td>Inherit</td>
<td></td>
</tr>
<tr>
<td>2016-10-26</td>
<td></td>
<td>Network activity</td>
<td>hostname</td>
<td>youre.lisiteo.work</td>
<td>Command and Control</td>
<td></td>
<td>Yes</td>
<td>Inherit</td>
<td></td>
</tr>
<tr>
<td>2016-10-26</td>
<td></td>
<td>Network activity</td>
<td>hostname</td>
<td>network.santastargrandsy.cox</td>
<td>Command and Control</td>
<td></td>
<td>Yes</td>
<td>Inherit</td>
<td></td>
</tr>
<tr>
<td>2016-10-26</td>
<td></td>
<td>Network activity</td>
<td>hostname</td>
<td>report.santastargrandsy.cox</td>
<td>Command and Control</td>
<td></td>
<td>Yes</td>
<td>Inherit</td>
<td></td>
</tr>
<tr>
<td>2016-10-26</td>
<td></td>
<td>Network activity</td>
<td>hostname</td>
<td>new.swinginwithme.ru</td>
<td>Command and Control</td>
<td></td>
<td>Yes</td>
<td>Inherit</td>
<td></td>
</tr>
<tr>
<td>2016-10-26</td>
<td></td>
<td>Network activity</td>
<td>hostname</td>
<td>fuckus.tbsupport.com</td>
<td>Command and Control</td>
<td></td>
<td>Yes</td>
<td>Inherit</td>
<td></td>
</tr>
</tbody>
</table>
Moonlight - Targeted attacks in the Middle East

Event ID: 3309

Org: Hvad

Date: 2016-10-27

Threat Level: Low

Analysis: Compromised

Distribution: All communities

Description: Moonlight - Targeted attacks in the Middle East

Published: Yes

Related Events: 2016-02-11 (2123)

### Filters
- All
- File
- Network
- Financial
- Proposal
- Correlation

#### Details
- **Date:** 2016-10-27
- **Org:** Hvad
- **Category:** External analysis
- **Type:** link
- **Value:** http://blog.vectornetworks.com/blog/moonlight-middle-east-targeted-attacks

#### Related Events
- **Type:** Yes
- **IDS:** Inherit
- **Distribution:** Inherit

- **Date:** 2016-10-27
- **Org:** Hvad
- **Category:** Network activity
- **Type:** domain
- **Value:** allwtnetwicem.com

- **Date:** 2016-10-27
- **Org:** Hvad
- **Category:** Network activity
- **Type:** domain
- **Value:** otherwtnetwicem.duckdns.org

- **Date:** 2016-10-27
- **Org:** Hvad
- **Category:** Network activity
- **Type:** domain
- **Value:** fun1.dyuu.com

- **Date:** 2016-10-27
- **Org:** Hvad
- **Category:** Network activity
- **Type:** domain
- **Value:** fun2.dyuu.com

- **Date:** 2016-10-27
- **Org:** Hvad
- **Category:** Network activity
- **Type:** domain
- **Value:** fun3.dyuu.com

- **Date:** 2016-10-27
- **Org:** Hvad
- **Category:** Network activity
- **Type:** domain
- **Value:** fun4.dyuu.com

- **Date:** 2016-10-27
- **Org:** Hvad
- **Category:** Network activity
- **Type:** domain
- **Value:** fun5.dyuu.com
Investigation Ticketing system

Request Tracker for Incident Response (RTIR) builds on all the features of RT and provides pre-configured queues and workflows designed for incident response.

https://bestpractical.com/rtir/
RTIR: Request tracker for Incident Response

To manage «easily»:

- Incident Requests
- Incidents
- Investigations
- Blocks
Network forensics

NfSen allows you to keep all the convenient advantages of the command line using nfdump directly and gives you also a graphical overview over your netflow data.

- NFDUMP Graphical interface
- BSD license

http://nfsen.sourceforge.net/
**NFSEN - Stat TopN “proto udp”**

**Netflow Processing**

<table>
<thead>
<tr>
<th>Source</th>
<th>Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>netflows</td>
<td>proto UDP</td>
</tr>
</tbody>
</table>

**Options:**

- List Flows
- Stat TopN
- Top: 10
- Stat: Flow Records, order by flows
- Check: proto
- Check: srcPort
- Check: srcIP
- Check: dstPort
- Check: dstIP
- Limit: Packets, > 0
- Output: long, IPv6 long

**nfldump**

```
proto udp
```

**Aggregated flows 473543**

Top 10 flows ordered by flows:

<table>
<thead>
<tr>
<th>Date first seen</th>
<th>Duration</th>
<th>Proto</th>
<th>Src IP Addr:Port</th>
<th>Dst IP Addr:Port</th>
<th>Flags</th>
<th>Tos</th>
<th>Packets</th>
<th>Bytes</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-11-30</td>
<td>12:15:00:289</td>
<td>UDP</td>
<td>14869.705</td>
<td>14975.689</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2015-11-30</td>
<td>12:15:00:289</td>
<td>UDP</td>
<td>14975.689</td>
<td>14869.705</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2015-11-30</td>
<td>12:14:21:050</td>
<td>UDP</td>
<td>14975.689</td>
<td>14975.689</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2015-11-30</td>
<td>12:14:21:050</td>
<td>UDP</td>
<td>14869.705</td>
<td>14975.689</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2015-11-30</td>
<td>12:14:56:064</td>
<td>UDP</td>
<td>14912.933</td>
<td>15020.563</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2015-11-30</td>
<td>12:14:56:064</td>
<td>UDP</td>
<td>15020.563</td>
<td>14912.933</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2015-11-30</td>
<td>12:15:10:148</td>
<td>UDP</td>
<td>14960.192</td>
<td>14975.689</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2015-11-30</td>
<td>12:15:10:148</td>
<td>UDP</td>
<td>14975.689</td>
<td>14960.192</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2015-11-30</td>
<td>12:13:54:800</td>
<td>UDP</td>
<td>15037.516</td>
<td>14869.705</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2015-11-30</td>
<td>12:13:54:800</td>
<td>UDP</td>
<td>14869.705</td>
<td>15037.516</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2015-11-30</td>
<td>12:14:56:064</td>
<td>UDP</td>
<td>14912.933</td>
<td>15020.563</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2015-11-30</td>
<td>12:14:56:064</td>
<td>UDP</td>
<td>15020.563</td>
<td>14912.933</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Summary: total flows: 1157243, total bytes: 2842765995600, total packets: 4332609600, avg bps: 1471178148, avg pps: 280274, avg bpp: 656

Total flows processed: 9163755, Blocks skipped: 0, Bytes read: 879770224
Sys: 1.970s flows/second: 4650002.4 Wall: 11.670s flows/second: 785235.4
Operational intelligence

Use Elastic to search, monitor, analyze and visualize machine data.

https://www.elastic.co/
### DNS Servers

<table>
<thead>
<tr>
<th>Server IP</th>
<th>Number Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>84.88.0.3</td>
<td>3,875,903</td>
</tr>
<tr>
<td>2001:40b0:1:1122:ce5ca0000:03</td>
<td>401,746</td>
</tr>
</tbody>
</table>

### DNS Query Types

<table>
<thead>
<tr>
<th>Transaction Type</th>
<th>No Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>IN A - EDC</td>
<td>891,440</td>
</tr>
<tr>
<td>IN A - E</td>
<td>489,046</td>
</tr>
<tr>
<td>IN A -</td>
<td>455,102</td>
</tr>
<tr>
<td>IN AAAA - EDC</td>
<td>415,237</td>
</tr>
<tr>
<td>IN A - ED</td>
<td>356,809</td>
</tr>
</tbody>
</table>

### Suspicious Requests Table

<table>
<thead>
<tr>
<th>Client IP</th>
<th>Query</th>
<th>Attack Type</th>
<th>Requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>aquapuremultiservicios.es</td>
<td>malicious</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>l.nfl.es</td>
<td>dyre</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>mellurbis.es</td>
<td>phishing</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>sutaxivigo.es</td>
<td>phishing</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>energiasolarcanarias.es</td>
<td>phishing</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>sybaristravel.es</td>
<td>phishing</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>term-service01.esy.es</td>
<td>phishing</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>ads-team-safety.esy.es</td>
<td>phishing</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>clipsexx.esy.es</td>
<td>phishing</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>ssl-unlock-pages.esy.es</td>
<td>phishing</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

### Attack Types

- Phishing
- Malicious
- Locky
- Attackpage
- Dyre
Q&A

Thanks!

https://www.csirt-kit.org