Handling an incident in CERT-EU

FIRST - 2017

Emilien LE JAMTEL
emilien.le.jamtel@cert.europa.eu
Introduction
CERT for European Institutions, Agencies, and Bodies.
Created in 2011.
Operational support to infrastructure teams.
Defence against targeted cyber threats.
Hub of information and skills.
Constituents

- Around 60 organisations
- From 40 – 40,000 users
- Separate, heterogeneous networks
- Cross-sectoral
  - Government, foreign policy, embassies
  - Banking, energy, pharmaceutical, chemical, food, telecom
  - Maritime, rail and aviation safety
  - Law enforcement (EUROPOL, FRONTEX, EUPOL) and justice
  - Research, hi-tech, navigation (GALILEO), defence (EUMS, EDA)
- High-value targets
• Step-by-step incident case
• Focus on tools and exchange of information
  • With external entities
  • Between CERT-EU teams

• Involved parties

Partners
First Response Team
Analysts
Threat Intelligence Team
Constituents
Chapter 1

Initial alert
Chapter 2
Sharing
Chapter 3
Hunting
• Log management tool: splunk

• IDS: SOURCEfire

• Cyber Threat Intelligence database: CERT-EU

• Monitoring:
CERT-EU Infrastructure

CERT-EU

Intelligence Sources
- Partners
- OSINT
- Monitoring

Cyber Threat Intelligence

AbuseHelper

Incident Handling Team

Constituent X

Constituent Y

Constituent Z

CERT-EU

DNS
Proxy
Email

SourceFire

FireEye

Splunk Indexer

Splunk Search Head

Incident Handling Team
Log Sources

Web traffic:
» DNS
» Proxy

Emails:
» Exchange
» Mimesweeper

Hosts:
» Sysmon
» Applocker
» McAfee

Appliances:
» Sourcefire
» Ironport
» FireEye

Future:
► Firewalls
► Active Directory
► Servers
► Reverse Proxy
Th0r Packages

- **Preparation**
  - YARA rules
  - Evil hashes
  - Custom filenames characteristics

- **Distribution**
  - GPO
  - Endpoint Management

- **Reporting and analysis**
  - Text/HTML report
  - Splunk app
Chapter 4

New evidence
- Constituents details
- CERT-EU deliverables
- Indicator search
- File Analysis
- Vulnerability scanning

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CERT-EU_THOR_Bundle_20160826.zip</td>
<td>THOR</td>
<td>![icon]</td>
</tr>
<tr>
<td>5577-crowdstrike_yara_master_20160826.zip</td>
<td>YARA rules</td>
<td>![icon]</td>
</tr>
<tr>
<td>CITAR-Flash-2016-007.zip</td>
<td>Flash-CITAR</td>
<td>![icon]</td>
</tr>
<tr>
<td>CITAR-014-Duke-and-Baron.zip</td>
<td>CITAR</td>
<td>![icon]</td>
</tr>
<tr>
<td>CIMBL-267.zip</td>
<td>CIMBL</td>
<td>![icon]</td>
</tr>
<tr>
<td>CIMBL-268.zip</td>
<td>CIMBL</td>
<td>![icon]</td>
</tr>
<tr>
<td>CIMBL-269.zip</td>
<td>CIMBL</td>
<td>![icon]</td>
</tr>
</tbody>
</table>
Investigation – Part 2

- **Partners**
  - Share dropped malware with Partners → Technical Reports

- **First Response Team**

- **Analyst Team**
  - Initial Mail + Workstation memory dump and forensics image → Analyse new evidences → Retrieve dropped malware → Create New IOCs Yara rules Snort Rules

- **Threat Intel Team**
  - New IOCs and rules put in CTI platform

- **Constituents**
  - Constituent A retrieve original mail and identify infected workstation → Send attachment to CERT-EU sandboxes - Customer Portal → Add new IOCs to MISP-EU
Chapter 5

Another infection?
## DNS logs findings

<table>
<thead>
<tr>
<th>#</th>
<th>from_splunk</th>
<th>query</th>
<th>id</th>
<th>feed_type</th>
<th>hits</th>
<th>first_seen</th>
<th>last_seen</th>
<th>actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ipa.eu</td>
<td>dpsu.gov.ua</td>
<td>CSIT-15112</td>
<td>cs_w_report (malicious_domain)</td>
<td>3</td>
<td>01/09/2016 08:42:56</td>
<td>01/09/2016 08:42:56</td>
<td>Report to CTI Toggle as done</td>
</tr>
<tr>
<td>2</td>
<td>ipa.eu</td>
<td>opa.eu</td>
<td>CSIT-15112</td>
<td>cs_w_report (malicious_domain)</td>
<td>3</td>
<td>01/09/2016 08:42:56</td>
<td>01/09/2016 08:42:56</td>
<td>Report to CTI Toggle as done</td>
</tr>
<tr>
<td>3</td>
<td>ipa.eu</td>
<td>opa.eu</td>
<td>dcleaks.com</td>
<td>cs_w_report (malicious_domain)</td>
<td>2</td>
<td>01/09/2016 01:12:59</td>
<td>01/09/2016 01:12:59</td>
<td>Report to CTI Toggle as done</td>
</tr>
<tr>
<td>4</td>
<td>ipa.eu</td>
<td>psu.gov.ua</td>
<td>CSIT-15112</td>
<td>cs_w_report (malicious_domain)</td>
<td>77</td>
<td>01/09/2016 00:06:15</td>
<td>01/09/2016 23:46:22</td>
<td>Report to CTI Toggle as done</td>
</tr>
<tr>
<td>5</td>
<td>ipa.eu</td>
<td><a href="http://www.dcleaks.com">www.dcleaks.com</a></td>
<td>224fe9f4-63c6-11e6-a9a9-0050568e34e1</td>
<td>cs.w_report (malicious_domain)</td>
<td>2</td>
<td>01/09/2016 01:12:58</td>
<td>01/09/2016 01:12:58</td>
<td>Report to CTI Toggle as done</td>
</tr>
</tbody>
</table>

## Proxy logs findings

<table>
<thead>
<tr>
<th>#</th>
<th>from_splunk</th>
<th>dest</th>
<th>id</th>
<th>feed_type</th>
<th>hits</th>
<th>d_clients</th>
<th>first_seen</th>
<th>last_seen</th>
<th>actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><a href="http://www.europeanlawmootcourt.eu">www.europeanlawmootcourt.eu</a></td>
<td>CSIT-15112</td>
<td>cs_w_report (malicious_domain)</td>
<td>18</td>
<td>2</td>
<td>01/09/2016 11:56:39</td>
<td>01/09/2016 17:05:36</td>
<td>Report to CTI Toggle as done</td>
<td></td>
</tr>
<tr>
<td>i</td>
<td>from_splunk</td>
<td>query</td>
<td>id</td>
<td>feed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>-------------</td>
<td>-------</td>
<td>----</td>
<td>------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>europa.eu</td>
<td>sikol.heidiandrobwedding.com</td>
<td>5718da8a-15f0-4883-b4b6-15ffac110003</td>
<td>cti (malicious_domain)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Event:**
- **eventtype:** dns_logs (dns, network, resolution)
- **feed_type:** cti (malicious_domain)
- **from_splunk:** europa.eu
- **id:** 5718da8a-15f0-4883-b4b6-15ffac110003
- **ioc:** sikol.heidiandrobwedding.com
- **query:** sikol.heidiandrobwedding.com
- **splunk_server:** europa.eu
- **src:** 10.1.8.136
- **Time:** 2016-04-18T17:08:33.000+02:00

**Observable:**
- **Type:** hostname
- **Kill Chain:** Command and Control
- **value1:** sikol.heidiandrobwedding.com
Drill-Down

Search on Proxy logs

New Search

splunk_server=* .europa.eu tag=proxy 'got_surrounding_time_interval(2016-05-20T12:25:10.038+02:00, "5s")'

Events (218)

Format Timeline

Zoom Out

+ Zoom to Selection  × Deselect

Hide Fields

All Fields

Selected Fields

host 1
source 1
tag 2
Chapter 6
And now what?
Technical Products

Incident Reports
- Incident Timeline
- Technical details
- Recovery

Advisories
- Technical description
- Detection Mechanism
- Prevention
- Reaction

Feeds
- IOCs
- Detection rules

IT administrators
Incident Response teams
SOC teams
Near Real time
Strategic Products

Security Brief
- One page
- Commented threat
- New TTPs

Threat Landscape
- Threat evolution
- Adversaries profiling
- Sectorial
- High-level course of action

CIO / CEO
Policy makers

Periodic Bulletin
Epilogue
What we didn’t speak about

- Red Team
- Vulnerability Assessment services
- Bugbounty program
- Research and whitepapers
- Automation framework (AH)
- Workshops / trainings
- …
https://cert.europa.eu/
https://github.com/certeu/