EMM @ CERT-EU

Freddy Dezeure
Head of CERT-EU
• About CERT-EU

• EMM @ CERT-EU

• Use cases
• EU Institutions’ own CERT
• Supporting all EU institutions, bodies and agencies
• Defence against sophisticated, targeted cyber threats
• Hub of information and skills in prevention, detection and response
https://cert.europa.eu/
• Public Portal ([https://cert.europa.eu](https://cert.europa.eu))
  – 1800+ Sources
  – Automatic gathering of information on cyber threats
  – Clustering of breaking news
  – RSS enabled on all screens
  – 3000 daily users

  – 3000+ Sources
  – Additional filters
  – Editorial interface for high power users (clients and partners)
  – 30 daily users
<table>
<thead>
<tr>
<th>Title</th>
<th>Articles</th>
<th>Last update</th>
<th>Start</th>
<th>Sources</th>
<th>Peak</th>
<th>Current rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Russia 'intervened to promote Trump' – US intelligence</td>
<td>20</td>
<td>Dec 10, 2016 2:18:00 PM</td>
<td>Dec 10, 2016 4:27:00 AM</td>
<td>9</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ThyssenKrupp : secrets stolen in 'massive' cyber attack</td>
<td>22</td>
<td>Dec 10, 2016 1:36:00 AM</td>
<td>Dec 8, 2016 11:57:00 AM</td>
<td>14</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Zeus Variant Floki Bot Targets PoS Data</td>
<td>16</td>
<td>Dec 8, 2016 10:57:00 PM</td>
<td>Dec 7, 2016 7:26:00 PM</td>
<td>8</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Obama orders review of election hacks as Trump doubts Russia's role</td>
<td>18</td>
<td>Dec 9, 2016 11:59:00 PM</td>
<td>Dec 9, 2016 6:03:00 PM</td>
<td>17</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Ransomware attacks against businesses increased threefold in 2016</td>
<td>15</td>
<td>Dec 9, 2016 10:34:00 PM</td>
<td>Dec 8, 2016 12:53:00 PM</td>
<td>12</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>New Mirai variant 'hijacked TalkTalk routers'</td>
<td>41</td>
<td>Dec 10, 2016 11:02:00 AM</td>
<td>Dec 5, 2016 6:17:00 PM</td>
<td>22</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Russian Police Arrested Hackers Suspected of Central Bank Attack</td>
<td>40</td>
<td>Dec 9, 2016 7:06:00 PM</td>
<td>Dec 2, 2016 8:59:00 PM</td>
<td>29</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>IBM begins beta testing to teach Watson more to combat cybercrime</td>
<td>13</td>
<td>Dec 10, 2016 2:04:00 PM</td>
<td>Dec 6, 2016 1:55:00 PM</td>
<td>7</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Experts Propose Cybersecurity Strategy for Nuclear Facilities</td>
<td>11</td>
<td>Dec 10, 2016 12:48:00 PM</td>
<td>Dec 7, 2016 10:02:00 PM</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
</tbody>
</table>
• What are the questions and answers?

Before lunchtime please

• Detect stories on which the Commission(er) may have an interest
• Validate and peer review them
• Collect more information and write a brief
• Obtain agreement before SPP meets the press
Russia 'intervened to promote Trump' – US intelligence
Articles: 20 | Last update: Dec 10, 2016 2:18:00 PM | Start: Dec 10, 2016 4:27:00 AM | Sources: 9 | Peak: 1 | Current rank: 1

Russia interfered in U.S. election to help Trump win: report
After Washington Post cites a secret CIA assessment, President-elect’s camp lambasts the spy agency....

ThyssenKrupp: secrets stolen in 'massive' cyber attack
Articles: 22 | Last update: Dec 10, 2016 1:36:00 AM | Start: Dec 8, 2016 11:57:00 AM | Sources: 14 | Peak: 1 | Current rank: 2

Trade secrets stolen from steel maker ThyssenKrupp in cyber attack
• Open source information, hand-picked and commented

• Distribution:
  – 300 people on technical, managerial and political level
  – CSIRT network
One of the Newsfeeds I most rely upon - It's from CERT-EU

cert.europa.eu/cert-filteredi …
cert.europa.eu/cert-clustered …
cert.europa.eu/GraphTest/clus … #infosec
How can we push critical guidance to the community?

- Write White Papers / Critical Advisories
- Validate internally and with peers
- Release publicly
- Amplify with Tweets
SECURITY ADVISORIES

IKEv1 vulnerability in CISCO devices (CERT-EU Security Advisory 2016-138)
The advisory recommends integrity checks and provides detection guidance for the IKEv1 vulnerabilities discovered by CISCO in its devices.
Monday, September 26, 2016 9:38:00 AM CEST

Critical Adobe Flash Player vulnerabilities (APSB16-29) (CERT-EU Security Advisory 2016-137)
Adobe has released security updates for Adobe Flash Player for Windows, Macintosh, Linux and ChromeOS to address multiple critical vulnerabilities.
Thursday, September 15, 2016 4:08:00 PM CEST

Pegasus Spyware targeting iOS devices CERT-EU Security Advisory 2016-136 - Updated
Three critical zero–day vulnerabilities were discovered, impacting Apple iOS and OS X devices. This advisory presents recommendations for end–users and Mobile Device Management administrators.
Wednesday, August 31, 2016 3:14:00 PM CEST

Leak of hacking tools targeting Fortinet devices CERT-EU Security Advisory 2016-135
On 13th of august, a previously unknown group called "Shadow Brokers" publicly released a large number of hacking tools they claimed were used by the "Equation Group". The targeted devices include Fortinet devices. This advisory presents risk mitigation recommendations.
Tuesday, August 30, 2016 4:21:00 PM CEST

In a number of EU institutions, bodies and agencies, processes have been established to respond to cyber–security incidents. Such processes involve the handling of personal data and therefore they must be subject to a formal notification to the relevant Data Protection Officer. The present document offers a model and recommendations for such a notification. It is intended to be used by cyber–security incident response teams of EU institutions, bodies and agencies.
Tuesday, January 6, 2015 4:44:00 PM CET
golden ticket protection

A privacy reminder from Google

To be consistent with data protection laws, we're asking that you take a moment to review key points of our Privacy Policy, which covers all Google services and describes how we use data and what options you have. We'll need you to do this today.

REVIEW NOW

PDF: Kerberos Golden Ticket Protection - CERT-EU
Miguel SORIA-MACHADO, Didzis ABOLINS

PDF: Protection from Kerberos Golden Ticket - CERT-EU

PDF: Windows Pass-the-ticket attack - Forensic Methods
May 27, 2014 - CERT-EU Security White Paper 2014-07 Pass The Golden Ticket v1.0 ... embedded in the protected core of the ticket and not on the policy set ...
• What will you give me if I inform you about a problem in your constituency?

• Validate the responsible disclosures
• Alert constituents and follow up
• Publish the name of the discloser in the Hall of Fame
We list here the individuals and organizations that explicitly helped us in improving the security of the EU Institutions, Agencies, and Bodies by reporting security issues and vulnerabilities discovered.

Alec Blance (blancealec1@gmail.com) www.facebook.com/alec.blance
Reported a XSS Vulnerability
Friday, December 2, 2016 3:02:00 PM CET

SaifAllah benMassaoud « FB/WhiteHatSecuri & @benmassaou »
Reported a number of Cross-Site Scripting (XSS) and Active Content Attacks
Friday, December 2, 2016 3:01:00 PM CET

Evan Ricafort (@evanricafort) www.evanricafort.com
Reported a XSS vulnerability
Wednesday, November 23, 2016 4:51:00 PM CET

Md. Nur A Alam Dipu (depu1994@gmail.com)
Reported a XSS vulnerability
Friday, November 18, 2016 8:57:00 AM CET
Evan Ricafort 🇺🇸 @evanricafort · Nov 23
I got listed in Europa (CERT-EU) Hall of Fame reporting a vulnerability.
cert.europa.eu/cert/newslette...
#infosec #security #hacking #xss

https://cert.europa.eu/cert/newslet
• We want this too!
Each workgroup can access ONLY its own resources.

In each workgroup there are analysts, managers, editors.
Public Website
• First contact with JRC 3 July 2011
• First set of keywords and themes end July 2011
• First version portal on test server 16 August 2011
• Web portal live 22 September 2011
• Continuous improvement

Private Website
• Currently 25 peers & partners
• Setting up a new group: 30’
• Additional, in-house, capacity for development
• Essential tools in CERT-EU’s work
• World-wide impact
• Supports our networking with Peers & Partners
• We want more:
  – Social media monitoring
  – Twitter in/out
https://cert.europa.eu/