**Minutes of 39th TF-CISRT Meeting**
**23 – 24 May 2013**
Bucharest, Romania.
This meeting was hosted by Agency ARNIEC/RoEduNet.

**Table of Contents**

## 1. Welcome and Apologies

Lionel Ferette welcomed attendees to the open session of the 39th meeting of TF-CSIRT.

## 2. Approval of Agenda

The agenda was approved as circulated.

## 3. Minutes of Last Meeting and Terms of Reference

### - Minutes

The minutes of the last meeting were approved as circulated. There were no open actions to be addressed.

### - Terms of Reference

Lionel Ferette updated attendees on the TF-CSIRT Terms of Reference (ToR). A major update to the ToR was approved in 2012, but since that time some improvements had been suggested by the TF-CSIRT Steering Committee. The identified problem areas were:

- Confused vocabulary around use of 'member' and 'representative'.
- Some unnecessary restrictions around attendance and participation.
- Mismatches between TI processes and the TF-CSIRT ToR.

A small number of changes have been proposed, including the introduction of the term 'delegate' for participants that are not official representatives of members.

ACTION20130523-01: Nicole Harris to circulate the revised terms of reference and ask Full Members to vote on its acceptance.

## 4. Megatron Tool. Göran Pestana, CERT-SE.

Megatron is an abuse-handling tool used by CERT-SE to collect and process information about bad hosts on the Internet. It is a java tool with a MySQL database, and has been in production since 2009. CERT-SE are processing over 10 million log lines and storing over 50000 log records. This results in over 50 abuse warnings per week. It is intended as a broadly automated system, although a handler approves mails before they go to ensure they make sense. The mailing system automatically creates a ticket-ID to support reporting.

CERT-SE performs data decoration to support the megatron tool, where information is incomplete. This includes adding ASN, country code, city (latitude, longitude), and hostname from various sources. A log record is then bound to an organization, such as governmental agencies, municipalities, health care organizations, infrastructure companies etc.

Megatron provides RSS feeds and various standard export features.

The Megatron tool is open source and can be downloaded at: https://download.cert.se/megatron/. CERT-SE also provides a visual version of the data called Megamap (also available as open source), which is useful for management style reporting. The map can be seen at: https://www.cert.se/.

Question: is there a policy for archiving data?
A:CERT-SE has no formal policy but archive on a yearly basis.
Question: what is the difference between Megatron and Abuse Helper?
A: Megatron could use Abuse Helper as a source. Megatron is more of a standalone tool for a CERT, whereas Abuse Helper is more distributed. Both have slightly difference use cases.
Question: what tools used for generating statistics?
A: CERT-SE has not had much requirement for in-depth data mining as yet, statistics tend to be lightweight.
Question: Can you use Megamap without Megatron.
A: Yes, Megamap is just reading the JSON files.

## 5. ENISA cybercrime exercises project. Miroslaw Maj.

Miroslaw Maj reported on the progress made within ENISA on two projects:

- AWA: Alerts, Warnings and Announcements. This is currently in the second stage of a four-step project, and is stocktaking through surveys and questionnaires amongst CERTS. The end goal is a good practice guide, which should be available for download from the UNISA website by the end of the year. A surveymonkey survey has been prepared and will be circulated to the TF-CSIRT list. CERTS are encouraged to complete the survey.
- CybEX – Cybercrimes Exercises. ENISA is working on a set of scenarios to ensure that the exercises they use are based on real cybercrime situations. Current topics include: computer forensics, electronic evidence, cybercrime trace (social networks), Advanced Persistent Threat, VS-Room – Visualization, and Cooperation of LEA.

Attendees were invited to participate in the process via a call for contributors. Contributors will be asked to suggest exercises, and review and comment on exercises as they are developed.

ACTION20130523–02: Don Stikvoort to circulate Alerts, Warnings and Announcements Survey to the TF-CSIRT list.

## 6. NISHA - Network for Information Sharing and Alerting. Przemek Jaroszewski.

NISHA (http://nisha-network.eu/the-project) as a network is about awareness and outreach rather than operational details for CERTS. Security news from reliable sources is a recognised need. NISHA is a platform for sharing research and alerts available to external people, including the media. It is also a place where information can be repurposed, including language translation etc.

The service is based on CouchDB with Drupal providing the portal for users and administrators.

The EU project is now coming to a close and has produced a prototype. CERT Hungary, CERT.PT, CERT Polska and University of Gelsenkirchen are looking at a future joint project to support the network.

Attendees were asked to act as information providers, information brokers and to help support a 'snowball effect' of use. NISHA has looked at legal aspects such as the licenses that information on the site is made available under.

### 7. Dutch practice for Responsible Disclosure. André Oosterwijk.

The Dutch National Cyber Security Centre started looking at responsible disclosure in order to provide the best advice to organizations and to incident reporters (in terms of what is allowed / not allowed). They started by interviewing reporters, organizations, and government officials and carried out some basic online investigation. There is a fine balance between making information available and moving towards possible legal / criminal repercussions.

Another part of the process was also to improve the feedback to and involvement of reporters when reports are made. These individuals are typically very skilled and a resource that should be used, not one that you should be afraid of.

Organisations can often react in a poor way to vulnerability reports and make poor decisions in terms of how they work with the reporters and fix the problems.

?? lost some text.

### 8. Incident Type Classification. Don Stikvoort.

??

ACTION20130523-03: Don to circulate classification documentation to the TF-CSIRT list.

### 9. The ENISA Internet Mapping Project. Rossella Mattioli.

Rosella gave a short background overview of previous ENISA work, including the 2010 Secure Routing Technologies report. This report demonstrated that there are only a few security mechanisms implemented for internet routing on the IP layer. A further 2011 report on Good Practices in Resilient Internet Interconnection demonstrated ENISA's focus on resilience as

In 2012, Hurricane Sandy proved to be a resilience challenge. Data centres effected in New York created domino effect with global significance. Another example of divers cutting an internet cable in Egypt has similar impact. A further example was the Spamhaus DDOS attack in March 2013. ENISA are looking at these issues and the overall impact on internet resilience. Natural phenomena had by far the biggest impact in terms of average duration of incidents, followed by malicious attacks.

The ENISA 2013 Internet Mapping project is addressing the IP routing layer first and aims to create a baseline set of results that can be shared and compared with CERTS under an appropriate non-disclosure agreement. From here ENISA will expand outwards to create a broader view of internet resilience. The tool will be used locally to help organizations map their own constituencies.

ENISA are calling for input in to what CERTs would like to see included in this study.

### 10. Planspiel. Wilfried Wöber.

Planspiel was a scripted cyber security exercise carried out in June 2012 based on a creditable attack / outage scenario, with the intention of involving all parties up the escalation tree including public administrators and industry representatives. The focus was on cross-sector interdependencies. Over 50 people took part as active players for the exercise, with over 100 people acting as exercise managers and an additional 100+ observers. A running log of the events of the day was kept.

Lesson learnt from running the exercise were:

- Need for more human resources and split responsibility;
- Need for more internal communication and preparedness;
- Highlighted the incompatibility of the federal model for dealing with emergencies in the cyber environment;
- Need to manage effective PR for the exercise.

### 11. Google Webmaster Monitoring Service. Dimitrios Margaritis.

Dimitrios gave a quick overview of the Google Webmaster Monitoring Service. Webmaster tools usually are used to provide information about errors and availability information for web sites. Webmaster tools can provide info for pages containing malicious code and also allow users to register as a webmaster for all websites on sub-TLD level. Overall, the service can be used a useful tool to support monitoring of malware and other site 'health' problems.

### 12. Update from CERT-RO.

Romania is currently number 6 on the CyberDefcon World Host Report in terms of countries with infected websites and botnets, creating a significant problem for local CERTS. There are between 100,000 – 500,000 IPs or URLS reported daily to CERT-RO. During 2012, there were several significant attacks that had ramifications affecting all of Romania. Romania has become a proxy for the transition of malware due to the lack of security culture, but this is changing. Romania is participating in the National CyberCrime Defence Center Project, which is a European project for establishing and training cyber-security teams. They also participate in the ACDC project.

Romania has a national CSIRT (CERT-RO), an educational CERT (RoCSIRT), and a government CSIRT (CORIS), although all of these organizations are recently set up. Issues faced for organizations in Romania include a lack of technical personnel, a lack of dedicated personnel at big ISPs and the fact that the security community is still young.

### 13. Team Cymru: CSIRT Battle Royale

Dave Monnier gave an update on Team Cymru and their activities. Team Cymru act as an internet 'first responder', as well as providing infrastructure monitoring, training and CSIRT

support.

Trends to date show the Russian federation as the most attacked location, followed by the United States. There are few DDOS attacks in to places like South America, Australia, Canada and Africa. Places with best infrastructure tend to also be the source for most malware, as it offers the best opportunities for 'well-hosted' attacks. Internet population per country tends to follow the same trend (e.g. Germany has high population on the internet, excellent infrastructure, high malware volumetrically). Overall, Switzerland has the least problems from attacks.

### 14. RIPE66 Update. Wilfried Wöber.

Wilfried gave a brief update on RIPE66, which occurred from 13th – 17th May 2013 in Dublin. Slides from the event can be found at https://ripe66.ripe.net. Some of the areas of interest include:

- Bulk Data Anonymization: this has caused problems as the necessary anonymization to meet data protection requirements has made data less useful. Wilfried asked for input on algorithms that preserve relationships across anonymization.
- Discussions on the future of IRT Object (further discussions on the TF-CSIRT would be useful).
- A proposal to relax double authentication to create route objects in the Internet Routing Registry (IRR). This was quickly rejected.
- A proposal to internationalize the IRR and all associated tools, UIs and APIs.
- Idea of providing abuse contact data exchange between RIPE NCC and national CERTS.
- Further discussions on BCP38 and Open DNS Resolvers (rate-limiting for bind9/10).

### 15. Network Security Monitoring Working Group. Jan Vykopal.

Jan proposed a new working group on network security monitoring. This group would be for sharing best practice, discussing new tools and providing a platform for closer cooperation. The group would then in turn present in to the main TF-CSIRT meetings. As an example, Jan gave a short update from CSIRT-MU.

The working group would need to think about whether it wants to have a webpage, mailing list, registration, chair, extra space at meetings etc. There are issues about whether this should be held in parallel (e.g. at the same time as RTIR) or separately and how this will work logistically.

There was broad support from the meeting for establishing such a group, and particularly the content that such a group would discuss. The existence of a similar group within FIRST was queried, but this has now been disbanded. It could be 'hijacked' in terms of continuation and participation.

It was suggested that each of the working groups (RTIR, Security Monitoring, and CSO?) should have a standing slot on the main TF-CSIRT agenda

ACTION20130523-04: Nicole Harris to coordinate a 'test run' of the Security Monitoring working group for the September 2013 meeting.

### 16. Council of the European Union. Anthony de Jacquier and Sebastian Leonnet.

Anthony and Sebastian gave a brief overview of the CERT work for the Council of the European Union (http://www.consilium.europa.eu/homepage). As an organization, they are a high target for attacks but don't necessarily have the capability to deal with all of the traffic centrally so a high priority is best practice documentation for local teams. They hope to become a TI listed team shortly.

### 17. TRANSITS I and II Update. Don Stikvoort

Don gave a brief update on the progress of TRANSITS courses. One of the benefits of attending a TRANSITS course beyond the training itself is meeting other CERTs that are experiencing similar problems. The next TRANSITS I course will be 28th and 29th November 2013.

TERENA and FIRST are in the process of establishing an MoU giving FIRST the right to use TRANSITS outside of Europe with a fairly low license fee per training event.

### 18. Date of Next Meeting, AOB and Close

The next (40th) meeting of TF-CSIRT will be on 26th and 27th September 2013 in London, United Kingdom.

**Action List**

| Reference | Who | Action | Status |
|---|---|---|---|
| 20130523-01 | Nicole Harris | Circulate the revised terms of reference and ask Full Members to vote on its acceptance. | Open |
| 20130523-02 | Don Stikvoort | Circulate Alerts, Warnings and Announcements Survey to the TF-CSIRT list. | Open |
| 20130523-03 | Don Stikvoort | Circulate classification documentation to the TF-CSIRT list. | Open |
| 20130523-04 | Nicole Harris | Coordinate a 'test run' of the Security Monitoring working group for the September 2013 meeting. | Open |

**List of Participants**

| | | |
|---|---|---|
| Shehzad | Ahmad | DKCERT (DTU) |
| Wim | Biemolt | SURFnet/SURFcert |
| Eduard | Bisceanu | CERT-RO |
| Tonny | BjÌürn | DKCERT (DTU) |

| | | |
|---|---|---|
| Vladimir | Bobor | TS-CERT |
| Hielke | Bontius | NCSC-NL |
| Romain | Bourgue | ENISA |
| Matej | Breznik | SI-CERT |
| Nicolae-Dorel | Constantinescu | STS |
| Matthew | Cook | ESISS (Loughborough University) |
| Dumitru | David | CERT-RO |
| Antony | De Jacquier | Council of the European Union |
| Serge | Droz | SWITCH |
| Andrea | Dufkova | ENISA |
| Alexandre | Dulaunoy | CIRCL - Computer Incident Response Center Luxembourg |
| Jacqueline | Dulmaine | CERT.be |
| Mihai | Dumitru | Cronus eBusiness |
| Michael | Dwucet | CERT-Bund - Federal Office for Information Security (BSI) |
| Gabriel | Ene | CERT RO |
| Lionel | Ferette | TF-CSIRT |
| Carlos | Fuentes | IRIS-CERT/RedIRIS |
| Sven | Gabriel | Nikhef/EGI CSIRT |
| Radu | Ghidiceanu | ANISP |
| Popescu | Hadrian | Agency ARNIEC/RoEduNet |
| Michael | Hamm | CIRCL - Computer Incident Response Center Luxembourg |
| Nicole | Harris | TERENA |
| Daniel | Ionita | CERT-RO |
| Adrian | Istrate | Agentia ARNIEC/RoEduNet |
| Przemek | Jaroszewski | CERT Polska/NASK |
| Razvan-Julian | Jiga | DGCTI-MAI |
| L. Aaron | Kaplan | CERT.at |
| Tomas | Kokolevsky | CSIRT.SK |
| Andrea | Kropacova | CESNET |
| Sebastien | LEONNET | Council of the European Union |
| Toomas | Lepik | CERT-EE |
| Nunik | Lestari | Indonesia Government Computer Security Incident Response Team |
| Antonio | Liu | The Trusted Introducer (TI) - DFN-CERT |
| Miroslaw | Maj | Cybersecurity Foundation |
| Dimitrios | Margaritis | CERT-EU |
| Marko | Maric | HR-CERT - Croatian National CERT |
| Detlev | Matthies | DFN-Cert |
| Jamie | Mcloughlin | JANET(UK) |
| Maciej | Miâostan | PIONIER-CERT/PSNC |
| Barbulescu | Mihai | Agency ARNIEC/RoEduNet |
| Cristian | Mihuti | MILLENNIUM IT SRL |
| Ovidiu | Mogosan | CERT-RO |

| | | |
|---|---|---|
| Dave | Monnier | Team Cymru |
| Marius | Nastase | Romtelecom |
| Liviu | Nicolescu | CERT-RO |
| Andre | Oosterwijk | NCSC-NL |
| Raul | Opruta | Agency ARNIEC/RoEduNet |
| Sami | Orasaari | CERT-FI |
| Catalin | Patrascu | CERT-RO |
| Goran | Pestana | CERT-SE |
| Florin | PETRE | Agentia ARNIEC/RoEduNet |
| Patrick | Pichler | ACOnet-CERT |
| Leila | Pohjolainen | Funet CERT |
| Iulian | Popa | International Relations and Security Studies Doctoral School |
| Michal | Prokop | CSIRT.CZ |
| Margrete | Raaum | UiO-CERT |
| Daniel | Roethlisberger | SWITCH |
| ÌÉsa | Roos | Handelsbanken |
| mihai | rotariu | CERT-RO |
| Steve | Santorelli | Team Cymru |
| Jacques | Schuurman | XS4ALL |
| Adam | Smutnicki | WCNS/EGI-CSIRT |
| Don | Stikvoort | Trusted Introducer |
| Erika | Stockinger | CERT-SE |
| Alexandru | Stoian | Cert-RO |
| Manuel | Subredu | RoEduNet |
| Alexander | Talos-Zens | ACOnet |
| Varis | Teivans | CERT.LV |
| Dan | Tofan | CERT-RO |
| Marius | Urkis | LITNET CERT |
| Jaap | van Ginkel | SURFcert University of Amsterdam |
| Erik | Vanderhasselt | CERT.be |
| Dimitra | Vitsa | FORTHcert |
| Valeriu | Vraciu | RO-CSIRT/RoEduNet |
| Jan | Vykopal | CSIRT-MU |
| Wilfried | WÌ¦ber | UniVie / ACOnet-CERT |