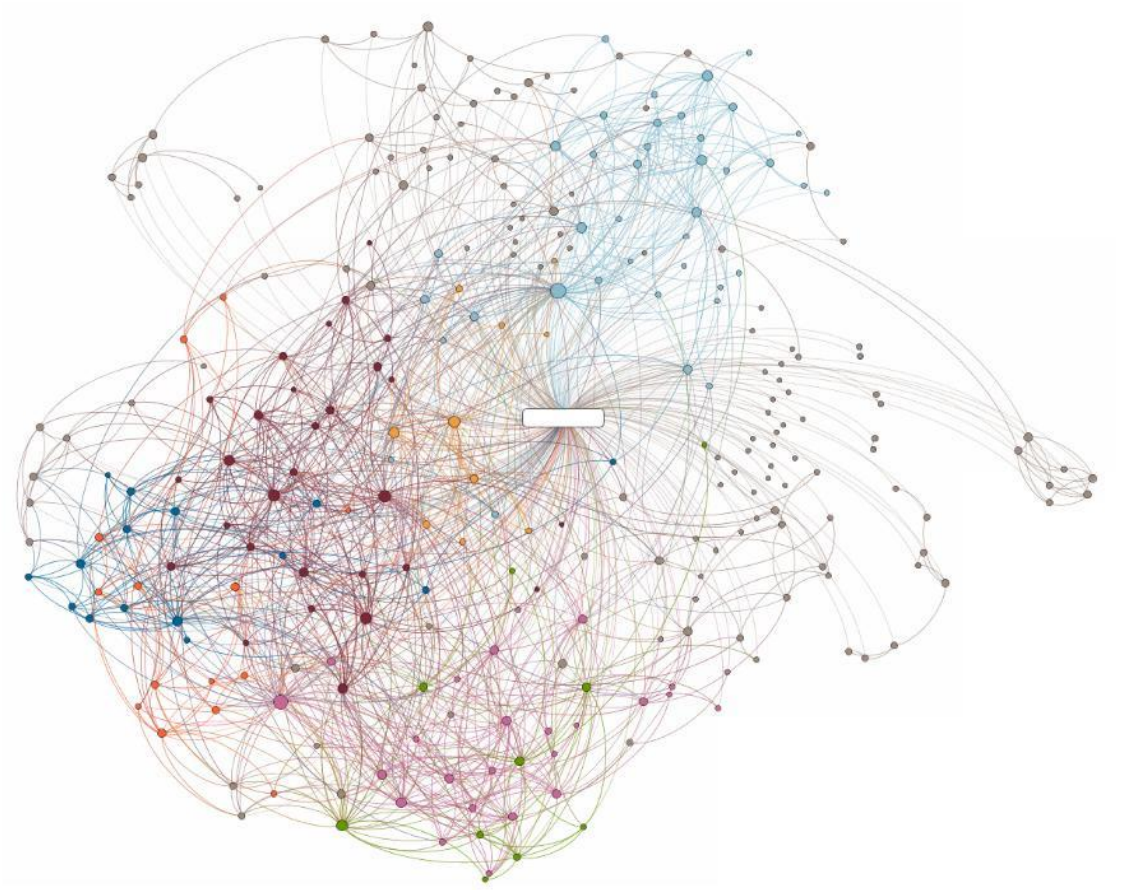

Establishing External Contact

Toolset, Document for students

September 2014

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Acknowledgements

Contributors to this report

We would like to thank all our ENISA colleagues who contributed with their input to this report and supervised its completion, especially Lauri Palkmets, Cosmin Ciobanu, Andreas Sfakianakis, Romain Bourgue, and Yonas Leguesse. We would also like to thank the team of Don Stikvoort and Michael Potter from S-CURE, The Netherlands, Mirosław Maj and Tomasz Chlebowski from ComCERT, Poland, and Mirko Wollenberg from PRESECURE Consulting, Germany, who produced the second version of this documents as consultants.

Agreements or Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors: Anna Felkner, Tomasz Grudzicki, Przemysław Jaroszewski, Piotr Kijewski, Mirosław Maj, Marcin Mielniczek, Elżbieta Nowicka, Cezary Rzewuski, Krzysztof Silicki, Rafał Tarłowski from NASK/CERT Polska, who produced the first version of this document as consultants and the countless people who reviewed this document.

Contact

For contacting the authors please use CERT-Relations@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Copyright Notice

Table of Contents

1 What Will You Learn

The communication and exchange of information is one of the crucial aspects of a CERT's work. The more effectively information is shared and exchanged between interested parties, the faster security incidents can be mitigated and the less the damage that occurs. Thus, it is very important to have at hand and to know how to use sources of contact information, networks of contacts and other channels for the distribution and sharing of data.

The goal of this exercise is to enhance your skills in establishing contacts with other CERTs, administrators of ISPs and other parties responsible for the mitigation of security incidents in their networks around the globe. You will be asked to identify and contact the proper authorities about real incidents. After finishing the exercise, you should be able to establish and develop networks of contacts faster and more effectively.

2 Exercise Task

2.1 Session One

8.2.1 You have received a number of logs indicating remote attacks. Your task will be to inform administrators of networks causing these attacks about the problem and ask them to mitigate it. Begin with identifying the right contacts.

We suggest starting with querying the who is databases of regional Internet registries (RIRs). They keep information about the network providers being assigned a given range of IP addresses. In turn, the providers can usually make the information more granulate by adding information about subnets and their networks. Note, that each regional registry has its own separated database which covers the address space administered by that registry. Currently, there are five regional Internet registries:

- ARIN: American Registry for Internet Numbers (http://www.arin.net/) covers North America and parts of the Caribbean;
- RIPE NCC (http://www.ripe.net/) for Europe, Middle East and Central Asia;
- APNIC: Asia-Pacific Network Information Centre (http://www.apnic.net) for Asia and the Pacific;
- LACNIC: Latin American and Caribbean Internet Address Registry (http://www.lacnic.net/) for Latin America and parts of the Caribbean; and
- AfriNIC: African Network Information Centre (http://www.afrinic.net/) for Africa.

The registries offer who is services via web interfaces and standard who is protocol.

Since it is not possible to determine which RIR to ask just by looking at the IP address (or at least not without sufficient prior experience), numerous services exist which can do this for you by querying multiple servers to find the correct one. One of the services we recommend for this is Domain Dossier from CentralOps.net, located at http://centralops.net/co/DomainDossier.aspx. While this service offers multiple other functionalities, for the time being we settle for network who is lookup. Look for contacts listed in 'cert-nfy' (RIPE, APNIC), 'tech-c', 'OrgAbuseEmail' (ARIN) or similar, as well as for any contacts the server refers to directly as 'abuse'.

Another approach is to use the domain name and user contact information for the domain. Note that this can be much less accurate, because:

- many institutions can get network or hosting services from a single provider and so do not bother to have reverse DNS entries, thus sharing a single provider's domain – in many cases they will, however, have different entries in RIR who is databases;
- the domain name system is hierarchical and sometimes the different levels of a domain name can be confused; and
- some domain registries hide pieces of information that are considered private and protected by local law (eg, the name and last name of a private person can be treated as personal data).

Note that, in any case, going after the domain owner should eventually bring you to the person responsible for a particular host – in the worst case, they should be able to redirect you one hop further – but usually it takes longer than going from the network provider's end.

When looking up the domain owner, do not confuse registrar with registrant. Although the terms sound similar, the first one is actually the organization where the domain was registered, while the latter is the domain owner.

Contact information for a domain is kept in a domain whois database – a separate one for each top-level domain. Most registries provide lookup tools for their databases via a web frontend and sometimes also via a standard whois interface. The quality and format of the information returned varies greatly. Again, Domain Dossier has a tool that does lookups at the appropriate servers for you (when available). This time use the 'domain whois record' feature.

Yet another way to look for administrative contacts is to look for a web page of the company. You may try entering the hostname into the browser directly or guess the name by adding 'www' to various parts of the domain name. For example, for a hostname 'melkor.nask.waw.pl' you would be successful with www.nask.waw.pl.

Warning! When visiting unknown web pages, consider using a disposable system, eg, a virtual machine which you do not mind getting infected. This is especially true when visiting potentially infected sites.

Once you find the web page, try to find out what kind of a company you are dealing with. Is it a hosting provider? An ISP? If you find yourself at either of these, you will probably look for an abuse department or a network operating centre of some kind and ask them to provide the customer's data or relay your information to him. If you stumble across an online store, or other site which does not seem to provide further network services, you have probably found the customer yourself. Just look for any contact information on the web page.

Last, but not least, consider passing the information on to a local CERT. CERTs have proved to be successful in getting to the right people by knowing the local situation, language and culture. Usually they have also built up a tight local network of trusted contacts that you may not be able to reach otherwise. If you are unable to locate the IRT contact in RIPE or APNIC databases, you may want to use one of the lists of CERT teams:

- http://www.first.org/members/teams/index.html - members of the Forum of Incident Response and Security Teams, the global forum for CERTs (sorted alphabetically);
- https://www.trusted-introducer.org/teams/country_LICSA.html - a list of recognized European CERTs, maintained by Trusted Introducer (sorted by country);
- http://www.egc-group.org/ - European Government CERTs Group;
- http://www.enisa.europa.eu/activities/cert/background/inv - Inventory of CERT activities in Europe by ENISA; and
- http://www.apcert.org/about/structure/members.html - members of APCERT, a forum of CERTs from the Asia-Pacific region.

Note the different constituencies of different CERT teams. Although some teams have country-wide responsibility and will be happy to accept and relay information about malicious activity anywhere in their country, some are limited to government or military institutions or even single companies or universities.

Whenever possible, try to make notes of phone numbers too.

When you have finished gathering contact information, consult with the trainer and other students.

Your next step is to write formal incident reports to the addresses you have found and send them by email. You should start the report by identifying yourself and the company and/or team you are working for. You may skip this only when you have long-established and informal relationships with the recipient – but do not do so for the sake of this exercise. The report should also contain:

- a clear description of the attack and what you think caused it;
- evidence of the attack – log samples including detailed time information, full email with headers, etc.; and
- a request for actions – you should state clearly what you want the recipient to do (e.g., stop the customer from carrying out further abuse, take down an offending host, etc.).

Once you have prepared the report, discuss it with the trainer.

If you have PGP/GPG available, always sign your mail. Note that encryption is not necessary unless you are sending sensitive information such as a cracked password, strings to access a vulnerable site, etc. Also, you would need to have a public key for the recipient or agree with him or her on a pass-phrase for symmetric encryption beforehand.

After hitting the 'Send' button, you are done with the first session, but not done with your exercise. Ask the teacher for the details of the second session when you will discuss the results. Until then, make sure you monitor your mailbox, reply to any inquiries you may receive from the administrators if you can, and take notes of any responses, tracking any numbers, etc., you may receive.

2.2 Session Two

Share your experience from the contacts:

- How many emails did you send?
- How many replies did you get?
- What kinds of replies did you get – automated, personalized, asking for clarification, or confirming resolution?
- How much time did it usually take to get a reply back?
- In how many cases do you believe you managed to resolve the incident?
- In cases where you did not receive any reply, what do you think was the reason?

Discuss your findings and opinions with the other students and the teacher.

In some cases, the teacher might ask you to follow-up with a phone call. Do you still have the numbers you noted?

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu