Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal IT Steering Unit FITSU
Federal Intelligence Service FIS

Reporting and Analysis Centre for Information Assurance MELANI
www.melani.admin.ch

Current Threats on the Internet Perpetrators, Tools, Prosecution and Incident Response

Reto Inversini, Bern University of Applied Sciences,
in cooperation with Roman Hüssy.

19. January 2012

Content

Foreword

This document is addressed to persons entrusted with the protection of IT infrastructures and electronic information. The first part briefly outlines which threats currently exist, how they can be classified, and what perpetrators are behind them. The second part explains the foundations for establishing a CSIRT/CERT (Computer Security Incident Response Team / Computer Emergency Response Team). The last chapter presents the resources used by law enforcement authorities to crack down on botnets.

Threats

There is a wide range of threats emanating from the Internet against government, companies, and individuals. The following pyramid represents a rough categorisation:

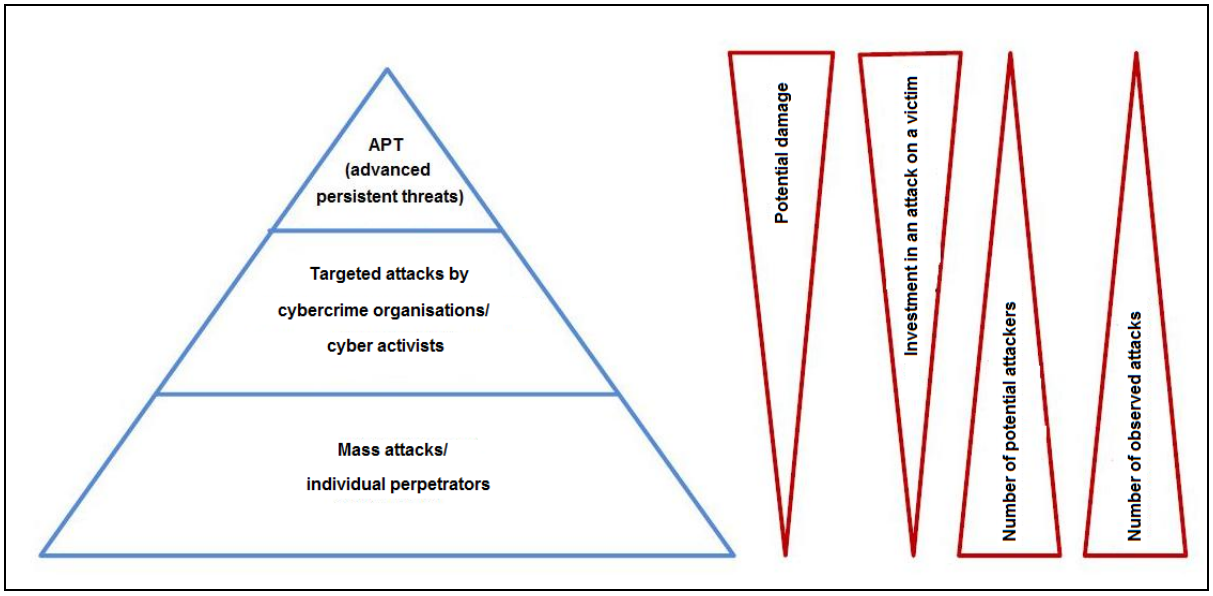

Figure 1: Threat pyramid, adapted from sans.org

At the tip of the pyramid is the most feared threat, the APT (advanced persistent threat). This threat results in very significant damage affecting a single organisation or country. The attacker is willing to invest a huge amount of time, money and knowledge in the attack and generally has substantial resources at his disposal. The attacker's goal is generally to remain undiscovered as long as possible, to entrench himself in the victim's network and to steal information of interest to him. Because of the high demands on resources, the number of potential attackers is relatively small. However, there are various known examples of successful attacks in the ATP category (e.g. Aurora/attack on Google).

The middle of the pyramid consists of the category of cybercriminals and cyber activists. Even though these have significantly fewer resources at their disposal, the threat they represent should not be underestimated. As a rule, the persistence of these attackers is somewhat less than in the case of APTs. It should be noted, however, that the boundaries between cybercrime and APTs are fluid. In particular, it must be assumed that intelligence services have access to criminal infrastructures or can bring about such access very easily where needed. Additionally, tasks can be assigned to such organisations so that any

participation can be denied in the event of discovery. The base of the pyramid consists of mass attacks and individual perpetrators. Even just in light of the enormous number of such attacks, this threat must be taken seriously despite the limited resources employed. Here again, the boundary to the next-higher level is porous, since mass attacks in particular are often perpetrated or at least commissioned by cybercrime organisations.

Classification of attackers

In the following, attackers are classified in terms of their possibilities and their motivation. This helps recognise which goals an attacker may pursue and with which resources and which degree of persistence. It should be noted that this is only a very rough approximation.

Intelligence services – advanced persistent threats

Name	Intelligence services/government organisations/advanced persistent threat
Description	A government organisation may act itself as an attacker, or it may commission the attack. As a rule, the goal is to obtain information (classic espionage or industrial espionage). In the event of a crisis or increased tensions, critical infrastructures may also be attacked or false information circulated in a targeted manner.
Motivation	Information gathering, disruption of critical infrastructures, false information
Technical resources	It must be assumed that everything technically feasible can in fact be carried out by a government organisation. The resources are very great, and specialists for all possible types of work are available or can be recruited.
Financial resources	Unlimited, at least as long as the outcome of the attack can be justified from the perspective of the attacker.
Rationality of approach	High
Persistence	High
Starting points for defence	Classification of data, well protected systems. Separation of network zones with very sensitive data from the Internet. Granting of access only on the basis of least privilege.
Starting points for prosecution	Analysis of malware used, close cooperation with other police organisations and other intelligence methods. Monitoring of incoming and outgoing

	network traffic.
Resistance to prosecution	Very high
Probable targets	• Systems with sensitive information • Critical information • Systems of key persons or decision-makers • Backdoors in inconspicuous systems that are difficult to discover • Often targets the confidentiality and integrity of systems • Targeted attacks against the confidentiality and integrity of systems. • DDoS attacks in the event of high political tensions or crises. These are usually carried out by para-governmental or non-governmental organisations with the government's acquiescence or by order of the government. • Critical infrastructures

Cyber activists

Name	Cyber activists
Description	Cyber activists use digital means to protest decisions by governments or companies that do not correspond to the ideals of the attackers. Examples of such groups are Anonymous or LULZ. Only illegal means are considered here, and a clear distinction is made from the – important and justified – phenomenon of digital protest carried out by legal means.
Motivation	The primary motivation is to make a statement, draw attention and/or damage the target.
Technical resources	The technical resources and capabilities vary strongly. In the event of major actions drawing a high level of attention, however, they may be very considerable (e.g. the attacks in connection with publication of US embassy cables on Wikileaks).
Financial resources	Limited. But since these activities are generally carried out on a voluntary basis, this is of little

	significance to the attacker.
Rationality of approach	Low to medium. Dependent on the organisational form of the group.
Persistence	Medium
Starting points for defence	Well protected systems. Protection of the integrity of high-visibility systems. Preparation for DDoS attacks, provision of appropriate tools and infrastructures (e.g. quarantine zone)
Starting points for prosecution	Cooperation with police organisations and intelligence services. Identification of accessories; often it suffices to send a signal that the acts are being prosecuted in order to weaken an attack.
Resistance to prosecution	Medium
Probable targets	• Systems with high visibility/level of attention • The attacks often target the availability, and sometimes integrity (defacement of websites)

Cybercriminal organisations – targeted attacks

Name	Cybercriminal organisations – targeted attacks
Description	Cybercriminal organisations may carry out targeted attacks that approach the level of an advanced persistent threat. They may attack government or private organisations with the goal of gathering information and reselling such information or using it for their own advantage. Very frequent targets include financial transaction systems. A very good example is the attacks on the national CO_2 register the beginning of 2011.[1]
Motivation	Primary goals include obtaining and reselling data (industrial espionage) or using financial transaction systems for one's own purposes.
Technical resources	Medium to high, depending on the organisation
Financial resources	Medium to high, depending on the organisation
Rationality of approach	High

[1] see MELANI semi-annual report chapter 3.1: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=en

Persistence	Medium
Starting points for defence	Well protected systems. Separation of network zones with very sensitive data from the Internet. Granting of access only on the basis of least privilege. Monitoring of incoming and outgoing network traffic.
Starting points for prosecution	Analysis of malware used, close cooperation with other police organisations and other intelligence methods. Observation of current cybercriminal organisations.
Resistance to prosecution	Medium to high. Prosecution disrupts the activities of attackers, however, so that they try to stay below the radar of law enforcement authorities.
Probable targets	• Systems with confidential information that have a high resale value. • Systems with financial information

Cybercriminal organisations – untargeted attacks

Name	Cybercriminal organisations, not targeted attacks
Description	This is cybercrime in its classic form. Attackers attempt to make financial gains by attacking end user devices. They try to obtain access data, carry out blackmail using DDoS attacks, or send spam via infected devices. The means of choice are often crimeware kits, with the help of which botnets can be built up.
Motivation	Solely financial
Technical resources	Medium; crimeware kits are often bought
Financial resources	Medium to high
Rationality of approach	High
Persistence	Low against individual target
Starting points for defence	Monitoring of incoming and outgoing network traffic in the case of companies and government organisations. Monitoring of ISP networks, notification of end users if an infected device surfaces. Provision of information to end users.

Starting points for prosecution	Sinkholing of domains used for cybercriminal organisations. Analysis of botnets and malware used. Analysis and prevention of money flows. Monitoring of money mules in order to identify these flows better.
Resistance to prosecution	Medium to high. Prosecution disrupts business, however, and is avoided by criminals to the extent possible.
Probable targets	• Poorly protected devices of end users • E-banking applications

Individual perpetrators

Name	Individual perpetrators
Description	Individual perpetrators act on their own accord, with limited resources.
Motivation	Depends on the attacker
Technical resources	Low
Financial resources	Low
Rationality of approach	Depends on the attacker
Persistence	Low to high, depending on the attacker
Starting points for defence	Well protected systems
Starting points for prosecution	Normal criminal prosecution
Resistance to prosecution	Low
Probable targets	• Weakly protected systems in the case of "script kiddies" • Visible targets with high level of attention in the case of acts of revenge

Tools

Alongside a large number of tools (port scanners, penetration testing tools, etc.) which may also be used for legal purposes, there are four specifically criminal tools that are examined briefly below. They have in common that they are used at all levels of the pyramid (see chapter on Threats).

Crimeware kits

A crimeware kit is a collection of tools for electronic attacks. Crimeware kits serve to develop malware and the infrastructure needed for malware to work, such as the establishment of command-and-control servers.

Botnets

Botnets consist of various infected computers which, via command-and-control servers, constitute a powerful attack tool for APTs and criminal organisations. It is also very probable that government attackers in individual cases make use of the services of criminal organisations and their botnets to carry out attacks. A botnet may encompass up to several million infected computers.

Command-and-control server infrastructures

Irrespective of the data an attacker is interested in, or whether the attacker wants to send spam, steal bank data, or engage in espionage, he must be able to issue commands to the infected devices and pick up data. Command-and-control server infrastructures are used for this purpose. This type of structure often also represents the greatest vulnerability of botnets, which is why criminal prosecution and observation for defence purposes should start there.

DDoS tools

In principle, there are two types of tools that can be used for DDoS attacks:

- Integrated in botnets, usually as a loadable module steered by a command-and-control server.

- User-controlled software generally relying on legal stress test tools. A typical example is LOIC[2] , which is popular among cyber activists such as Anonymous.

Protection by CSIRT/CERT organisations

Large companies are increasingly being attacked both in a targeted manner and across the board. For this reason, security organisations and architectures must be established to defend against these threats. To be able to react adequately to attacks, medium to large companies or companies that are especially exposed (e.g. high-tech companies) should have an organisation to deal with security incidents. One possible form is a CSIRT (Computer Security Incident Response Team) or CERT (Computer Emergency Response Team), which responds to security-relevant incidents in the company's own IT infrastructure.

[2] http://en.wikipedia.org/wiki/LOIC

A CISRT/CERT generally works according to the three main processes "Preparation", "Detection/Reaction", and "Protection":

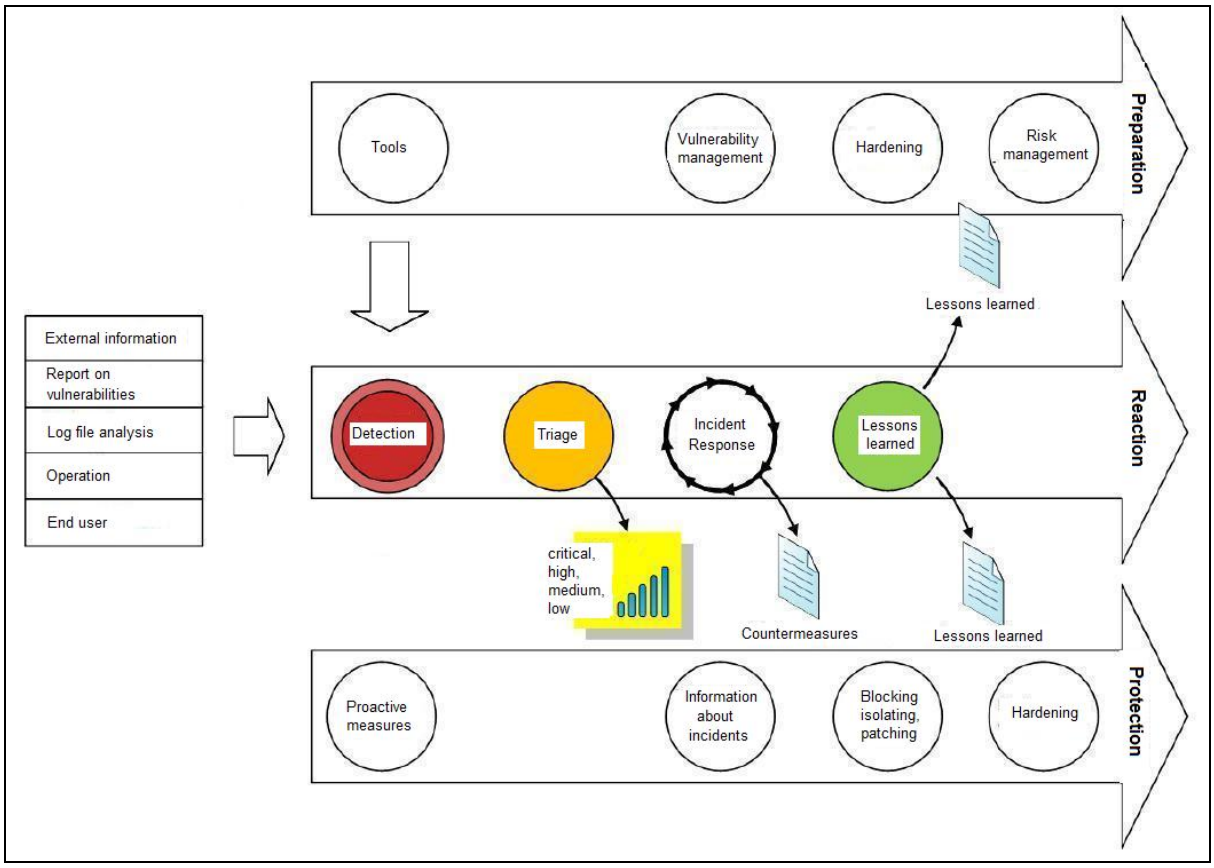

Figure 2: CSIRT/CERT processes, adapted from cert.org

The treatment of the actual security incident occurs in the Detection/Reaction process, which always follows the pattern "Detection – Triage – Reaction – Learn". The importance especially of learning from security incidents should not be underestimated, since it offers the possibility of critically examining the defence measures on the basis of concrete incidents and of making improvements where necessary. The information from actually occurring security incidents is one of the most important input sources for risk management in a company. There is no generally valid recipe for how to deal with incidents.

As a rule, every security incident is also different. It is therefore important to observe the following points in precise order:

1. Should forensic images of the compromised system be made? This requires a minimum level of equipment (write blocker) and training of the incident response team.

2. Is it necessary or useful to leave a few devices to the attacker so that he does not suspect that he has been discovered? Are there fears that the attacker might exact revenge if he is discovered?

3. How can the attack be contained? What is needed to do so? How can further infections or further loss of data be avoided?

4. Who has to be notified?

5. Containment of the attack (isolation, blocking on gateway systems, blocking of data, etc.).

6. Analysis of the attack (log file analysis to identify all infected devices if possible, reverse engineering of malware).

7. Enquiries to external information sources (e.g. MELANI)

8. Carry out regular meetings to exchange information, initially every 6 hours, later every 12 to 24 hours.

Points 3 to 8 should be understood as a cycle to be run through until the incident has been resolved.

The working tools needed for a CSIRT/CERT are systems for monitoring network traffic, system logs, and application logs. The use of intrusion detection systems (IDSs) or integrity testing systems may also be helpful. To obtain a sufficiently high level of protection from attackers, special safeguards for Internet access are indispensable. For instance, block lists and central virus scanners may be employed. Despite all these safeguards, however, it must be acknowledged that attacks may nevertheless be successful. In such a case, rapid detection of a successful attack and a good reaction are crucial in order to limit damage as much as possible.

Since the threats in dealing with information technology change continuously, the safeguards must be tested, updated, and adjusted on an ongoing basis. Additionally, appropriate basic and continuing training of CSIRT/CERT staff is of great importance. Operators of critical infrastructures in Switzerland are notified of current threats via MELANI's closed constituency.

Suppression of botnets by law enforcement authorities

In addition to the already established defence strategies such as the establishment and operation of Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs), criminal prosecution is of great importance. The Swiss banking centre is one of the trademarks of Switzerland. For this reason, it must be specially protected to ensure a high level of trust in Swiss banks. With the beginning of the Internet era, bank robberies are increasingly committed online. For several years now, there has been a strongly increasing trend with respect to cybercrime acts targeting banks and their clients. A large number of Western countries has already been affected by such attacks, including Switzerland. Over the past months, criminal groups have increasingly targeted financial institutions in individual countries on a sequential basis. Interestingly, criminals have changed their target upon discovery and media coverage of an attack wave and have then used the same attack pattern to attack banks in a different country. For instance, a criminal group attacked the clients of several banks in precisely one country. After the banks and the media drew attention to the ongoing attacks, the criminals switched countries and began targeting the banks there.

Notification of the population is of the utmost importance when Swiss infrastructures are targeted by a widespread cyber attack. This responsibility is already fulfilled by MELANI. MELANI also coordinates information among the affected companies. To combat cybercrime effectively, however, cooperation with Interpol, Europol and the authorities of the affected countries is necessary. Good coordination at the federal level is very important, since the infected computers (bots) are situated in different countries and are often steered by one or several command-and-control servers. The command-and-control servers are operated abroad in almost all cases (Germany, Netherlands, or Eastern Europe). To remove these from the network, appropriate processes must be established quickly. In addition to actual criminal prosecution, which sometimes is very difficult, the separation of discovered command-and-control server infrastructures and the sinkholing of malicious domains is a way to increase the price for successful attacks.

The smooth cooperation of law enforcement authorities, private and government CERTs/CSIRTs, intelligence services, and organisations for the defence of critical infrastructures (cyber defence) must be the focus, since the task can only be mastered jointly by various mutually independent organisations. It must be observed in this regard that while these individual organisations use different methods and have different views of the problem, they all share the common goal of preventing the Internet from deteriorating into a lawless zone in which only might makes right.