The German Anti-Botnet Initiative – Sven Karge

1 Project Aim and Objectives

The German Anti-Botnet Initiative presented by the association of the German Internet industry eco at the IT summit on 8 December 2009 is a private industry initiative aimed at supporting citizens in protecting their IT systems. The aim of the initiative is to ensure that customers whose personal computers have become part of a botnet without them being aware of it are informed by their providers about this situation and at the same time are given competent support in removing the malware. The German Federal Government welcomes and supports eco's initiative as a successful example of responsibility taken on by private industry for the entire society. The Federal Office for Information Security (BSI) provides its technical expertise to help this initiative.

2 Brief description

The concept is to build a central support center in Germany consisting of a website and a user help desk with telephonic support. With the help of this help desk, Internet users whose PCs have been taken over by a trojan and are part of a botnet which has been confirmed by their Internet access providers can as a start begin to disinfect their PCs themselves by using the offered online tools and by getting support from a help desk assistant upon providing a personal ticket number. The goal of the project described herein is to establish processes to enable affected end users to clean their PCs themselves as much as possible and to offer a help desk service telephone number (at the cost of a local call) provided by the ISPs to their customers for the purpose of removing malicious code. This is supposed to pull the rug underneath the feet of the botnets acting in or from Germany.

The German Anti-Botnet Initiative:
1. Identifies the customers with infected PCs
2. Informs the customers
3. Offers support in the form of the support center

Spamtraps and honeypots are used to find infected PCs. For this purpose, only attacks from infected PCs are evaluated. In no case does an evaluation of the Internet traffic through deep packet inspection or similar methods take place. In other words, user behavior is not recorded or evaluated.

After the first year of support center operations, the expected security gain is considerably less infected PCs in Germany compared to the present status quo. The main goal is to remove Germany from the top ten ranking of countries from which botnet activities originate.

3 Background of the initiative

Internationally, Germany is within the top 10 ranking of countries from which malicious online activities through botnets originate.1 A considerable percentage of all computers worldwide are infected with malicious code and are part of the zombie networks (botnets) spread around the world which are used for global spam and phishing mail as well as DDos attacks, key logging, man-in-the-middle attacks, as well as economic espionage. According to experts and ISPs, the infection

rate in Germany is high, not least because the majority of PC infections are now so called drive-by infections. Even though Germany has steadily reduced the sending of spam from computers in this country by continuous measures taken by the Internet industry which have been in place since the fall of 2008 in cooperation with the German Federal Office for Information Security, Germany is still in the top 10 in the area of general malicious activities (compared to countries with anti botnet initiatives like Japan, Australia and South Korea which are not in the top 10).

4 Support center process flow

The overall process is mainly as follows:

(a) Providers operate honeypots and spamtraps. Only the providers can identify their customers from the IP-address at that particular point in time.

(b) Providers inform the particular customers according to the process determined by the providers themselves. In the first phase, the customers are informed that they have been infected with malicious software (bot). The customers are referred to the central help website where disinfection instructions are available.

(c) If the customer does not succeed there, he/she can contact his/her provider. The provider can then decide if the customer needs to be referred to the call center for further help with removing the malware. In this case, the provider gives the customer a pseudonym created trouble ticket number which contains coded information about the infection.

(d) The process is set up so

- The affected users are initially informed by their ISPs that they can download certain tools from the project help website and that they can carry out steps described there.
- If the user does not succeed on his own, the user is given a ticket number which will allow him/her to get help telephonically from the help desk.
- Should that also fail to lead to the desired success, the caller is forwarded to a specialist, going from a level 1 to a level 2 support, who will then give further suggestions on what to do. Moreover, level 2 support will work out action suggestions for level 1 support and as the case may be continually update and improve it. The detailed concept will include detailed suggestions for this.

5 Support center project website

The central project website provides the respective tools for downloading as well as instructions, and therefore its quality, functionality as well as security are crucial for managing the volume of calls received by the help desk.

The website contains detailed step by step instructions as well as the respective tools to enable the end user to disinfect his/her own computer.

The tools available for downloading on the website are determined by eco in accordance with the German Federal Office for Information Security. Collaboration with antivirus makers makes sense here.

The website (including the detailed disinfection instructions) is created by eco in collaboration with the participating ISPs and, as the case may be, supporting antivirus program makers. Since the respective removal tools and the cleaning instructions have to be checked and updated, eco will maintain the website on an ongoing basis and beyond the duration of the project.

6 Telephonic support at the support center

6.1 Inbound help desk only format

The help desk is planned as an inbound only help desk. The incoming calls are made exclusively by customers identified by their ISPs as infected, and who have received a ticket number from their ISPs

for this purpose.
In order to enhance end user acceptance, the service telephone call will be billed as a local call. In this respect, 0900 numbers that are scalable are an option, or 0180-1 or -3 numbers billed at the local rate, or a number like 119119, ultimately a simple local number should inspire the highest trust. For the purpose of customer service, as the case may be, an interactive voice response system can be added to handle peaks, ask questions and automatically convey to the ticket system what has already been done by the customer.
For financial reasons, the plan is to run the basic help desk (the first level support is managed by competent, trained staff familiar with the material) via a competent outsourced help desk, and to keep a few specialists (second level support) centrally located at eco.
In order to keep the incoming call volume manageable, not every user should call the help desk directly. In order to avoid a high call volume and offer high quality customer service, the help desk number should not be available to the general public. Only affected ISP customers who have a ticket number should be able to call.

6.2 The ticket system: Generating the ticket number in accordance with data privacy regulations as well as by attack type
Every referring ISP should generate the ticket number to include the individual ISP-ID-code so that only that particular ISP can connect to the personal customer data. If the ISP has information about the type of malware (spam mailing, portscan and possibly the virus type), the ISP can opt to include that additional information that would be helpful for the cleaning process on the ticket number. In order to avoid duplicates as a result of entry errors or ticket numbers generated by others, the ticket numbers should include a security feature such as a checksum.

6.3 Help desk schedule
The general availability of the help desk is planned for Mondays through Fridays from 09:00 am to 09:00 pm as well as Saturdays from 09:00 am to 09:00 pm whereas weekdays during 09:00 am to 05:00 pm will initially be manned by a core team since the highest call volume is expected after work hours and on Saturdays. The help desk schedule can be adjusted as needed.

7 Support center staffing - First and Second Level Support
The calls are first processed by the first level support. The task of first level support is to walk the customer through the steps for the most part determined by eco and the second level support and to help the customer install and run the software to remove the malicious code.
Difficult cases are forwarded to second level support. Moreover, second level support is also supposed to continually update first level support procedure.

8 Customer contact procedure - Customer reachability and previous response quota
Previously, the response quota from customers to infection notifications was rather small (possibly the email contact addresses of the customers were wrong or notifications were mistaken for advertisement and deleted), so the processes to get the customers to clean their computers to remove malicious software are currently being optimized. Since each ISP has different customer contact procedures, the ISPs are supposed to determine themselves how they will set up the notification and request for action procedure. Depending on the ISP service portfolio, there are many alternatives.
The following are examples on how to notify the customer about the infection:
- Email the customer

- Letter to the customer
- Call
- SMS
- Other technical options within the framework of software updates
- Inserted portal website with information about the infection (similar to an inserted website with WLAN-hotspots). The customer receives a text that his/her computer is infected. The access, however, is not denied.

9 Scope & ISP project coverage

On the ISP side, the largest German Internet Access Providers should participate in the project: 1&1 (including the previous Freenet connections), QSC, Netcologne, KabelBW, DeutscheTelekom, Vodafone, Hansenet, Telefonica , UnityMedia as well as Kabel Deutschland,
and Versatel. So far 5 of these ISPs have declared their interest to participate in the project.

Together, the listed ISPs have over 23 million DSL customers and cover the German broadband market almost completely2. Even if only the top 5 ISPs participated, that would mean that the central anti-botnet support center would cover over 80% of DSL customers in Germany.

10 Legal aspects and challenges

Due to the ticket system implemented in this project, participating ISPs will not enter personal customer information into a central data base. Should it be necessary in exceptional cases to enter personal information into a central data base/CRM-system for allocation reasons, only the project management and the second level senior help desk agents should be permitted access to it. In regards to this approach it is planned to request a statement from the Federal Data Protection Commissioner.
We would like to emphatically point out for clarification purposes that the help desk employees do not access the customer computer directly or with remote hands but rather walk the customer through the procedure over the phone.

11 Project duration and funding

The project duration is 18 months counting a maximum of 6 months for the planning and building phase and 12 months of help desk operations. The start-up budget and funding for the project is 2 Million €, provided by the German government (Federal Ministry of the Interior). The Federal Office for Information Security (BSI) provides its technical expertise to support eco and take care of the strategy and implementation of the initiative for granting the funding. Additionally eco and its participating ISPs supports the initiative by identifying and informing customers with infected PCs.
At the end of this period, eco will secure the continuation of the project to meet demands for another year. The project website providing the instructions for the disinfection as well as tools will be in any case continued to be maintained and operated.

12 Project phases and time line

a.) Phase 1: Developing a detailed concept (March - May)
b.) Phase 2: Developing the support center and operating online (June - July)
c.) Phase 3: Developing and operating the telephonic support (August, launch of operation Sept 15th)
d.) Phase 4: Project evaluation (Mid of 2011).