ACDC

Advanced Cyber Defence Centre for Europe

Dr.-Ing. Christian Keil

DFN-CERT Services GmbH, Sachsenstr. 5, 20097 Hamburg, Germany, keil@dfn-cert.de

Keywords

Botnet detection, ACDC, Information sharing, Botnet mitigation

Abstract

The Advanced Cyber Defence Centre (ACDC) is an EU-supported pilot project aiming to fight botnets. To achieve this, it promotes an integrated solution that comprises several components tackling the botnet problem from multiple sides: detecting threats in networks as well as on websites and end-user devices, correlating and sharing data via a centralised repository, and providing data and support to all affected parties. Depending on the individual incident, the affected parties can include the end customer responsible for an infected machine as well as his ISP and hosting provider, Computer Emergency Response Teams (CERTs), Law Enforcement Agencies (LEAs), antivirus companies, and researchers. In this talk we will take a look at the architecture of ACDC and the comprising components and explore how you can benefit from and contribute to the project.

The botnet problem

Botnets have evolved into a pervasive threat to users and current networks. Abusing legitimate services to amplify their traffic, the botnets' masters can direct hundreds of Gigabits of DDoS attacks at their fingertips as observed in attacks on CloudFlare's Prince (2014), and analysed by Rossow (2014). Mobile devices are joining the ranks of the bots through trojanised apps, for example to generate revenue with premium services as observed by Symantec's Mullaney (2012) or send SMS spam as reported by Cloudmark's Conway (2012). While declining in volume, email spam, to a substantial degree sent by botnets, still makes up around 70 % of total email traffic according to Kaspersky, see Gudkova (2014), and Symantec (2013).

Advanced Cyber Defence Centre

A problem at such scale calls for a solution that facilitates detection, information correlation and sharing, as well as mitigation at scale. The goal of the Advanced Cyber Defence Centre (ACDC) project is to build such a solution in an EU-supported pilot project with 28 partners from 14 countries. Started in February 2013 with partners such as Internet Service Providers, CERTs, IT providers, National Research and Education Networks (NRENs), academia and critical infrastructure operators, ACDC aims to integrate existing solutions into a running pilot in 2015. The solutions are organized into five tool groups that illustrate the architecture and workflows in the project.

ACDC is built around a Centralised Data Clearing House (CCH) that acts as a central data hub for correlation and information exchange as seen in Figure 1. This is fed by observations of bot behaviour from sensors of three different kinds.

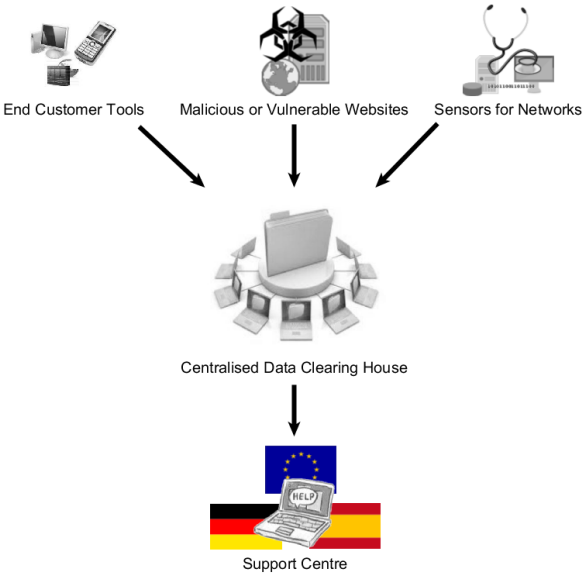

Figure 1: ACDC Tool Groups

End customer tools are software components used by end customers either running on their hardware like desktop computers, laptops, or mobile phones, or as plugins for example in webmailers or blogging software. They enable an end customer to submit suspicious information to the CCH, including for example spam messages or possibly infected files.

The malicious or vulnerable websites group subsumes tools to detect, analyse, and submit information about websites that either are already infected or vulnerable for an infection.

Sensors for networks include software mainly run by organisations with access to a larger block of ip address space. These include tools like darknets, traffic flow analysis, and honeypots to identify suspicious traffic.

The CCH is desinged to accept this diverse kind of information from a large set of sensors and, after enriching via correlation, forward the information to the responsible ISP or CERT. They in turn contact the owner of the infected machines and direct them for further information to the support centres. For CERTs this is envisioned to be based on the information provided by the Trusted Introducer Service (TI) so that every TI-accredited CERT will be able to obtain the data on their constituencies IP addresses.

The national support centres, nine are planned to be established during the project, offer

all information necessary for disinfection for end users. This includes disinfection tools as well as support in handling these. The basic support level provides tools and information about different infections and current threats but this can scale up to telephone support for direct help in disinfecting a compromised system.

Benefit and Contribute

But how can you benefit from and contribute to ACDC? Besides following the project via the website `www.acdc-project.eu` and the social media accounts linked there with information on the project but also current trends and threats, you can become an ACDC member or sign a Letter of Intent.

Becoming a member of ACDC allows you to access all the features offered by ACDC. You will be able to query the clearing house for compromised systems in your networks and be able to exchange intelligence with the ACDC community. There will also be a special access for academia to obtain suitably anonymized data for botnet research.

Signing a Letter of Intent gives you early access to all of this and allows you to shape the future of ACDC with us. You will be given access to results and have the opportunity to provide feedback that will be used to better tune ACDC's solutions to your environment. It also allows you to participate in the ACDC experiments, for example by providing or hosting tools for botnet detection. Since the success of such a project is dependent on reliable, high quality data, ACDC is always looking for partners that are willing to setup and operate sensors and provide data to the clearing house. The CCH already supports a broad range of formats with new formats being implemented if there is a demand.

References

Conway, A. (2012), 'Android Trojan Used To Create Simple SMS Spam Botnet'.
URL: *http://blog.cloudmark.com/2012/12/16/android-trojan-used-to-create-simple-sms-spam-botnet/*

Gudkova, D. (2014), 'Kaspersky Security Bulletin. Spam evolution 2013'.
URL: *\url{https://www.securelist.com/en/analysis/204792322/Kaspersky_Security_Bulletin_Spam_evolution_2013}*

Mullaney, C. (2012), 'Android.Bmaster: A Million-Dollar Mobile Botnet'.
URL: *http://www.symantec.com/connect/blogs/androidbmaster-million-dollar-mobile-botnet*

Prince, M. (2014), 'Technical Details Behind a 400Gbps NTP Amplification DDoS Attack'.
URL: *http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack*

Rossow, C. (2014), Amplification Hell: Revisiting Network Protocols for DDoS Abuse, San Diego, California.
URL: *http://www.internetsociety.org/sites/default/files/01_5.pdf*

Symantec (2013), Internet Security Threat Report 2013, Technical Report 18.
URL: *http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf*

Author Biography

Dr.-Ing. Christian Keil studied Computer Science and Engineering with a focus on Scientific Computing and wrote his dissertation at the Hamburg University of Technology. He is the principal researcher of the DFN-CERT, which was historically the CERT of the German Research Network only and nowadays provides key security services to industry as well. His main areas of work include early warning systems, network and meta data analysis, DDoS and botnet behaviour, and mobile security.