CyberCamp 2014 (5-7 December)

report for COINS by Andrii Shalaginov @ HiG
andrii.shalaginov@ccis.no

December 10, 2014

The event was mostly targeted on the cyber security community in Spain. Several sessions were run in parallel, including conferences, technical workshops, companies presentations, hackatron, security challenges, SCADA protection, etc. The total amount of visitors reached 40000 people. Multiple security specialists from the world-biggest companies shared their experience related to work in IT Security sphere, hacking and protection against various threats in the modern ICT society. The key benefit of the CyberCamp is that it covered covered different filed for the people with different level of skills and knowledge, which means that anyone could find area of interest.

The 1^{st} day was the registration and introduction day. The founder of the GNU Project[1] back in 1983 Richard Stallman gave a talk on the "Free software and Privacy". It was a debate on the preservation of human rights while using propriety software that dictates how the information of users is handled. Stallman mentioned that the free software is not quite the same as an open-source software. Also it is hard to bring attention of users since some of them just do not care about preservation of own rights. There were identified four user rights that defines free software: freedom of running the software, look into its source code, edit and improve and distribute it via the GNU license.

On the 2^{nd} day Joanna Rutkowska from the Invisible Things Lab[2] gave a speech "Builders, Breakers, and the rest of the Menagerie" about the secure operating systems. She is one of the founders of the Qubes OS Project [3], which offers a considerably strong to desktop computers by means of Compartmentalization. This OS uses virtualization to separate the program run. The benefit of such approach is that the security breach on one of the compartment will not affect other compartments. In overall, the Qubes OS sandboxes each application in order to restrict the access to others.

The next presentation was by Marc Heuse "Van Hauser", one of the founders of The Hacker's Choice group [4], about the importance of motivation and different social factors in becoming a valuable hacker. This talk was targeted rather on motivation to be a good hacker than on the particular hacking lessons. Heuse gave an insight on the differences in hacking community in 90th and now. The main point was that the specialization of hackers is too narrow right now, not like 20 years ago, and it is challenging to find anyone with the same skills and in the same area. So, it is important to create a network and share the idea. Moreover, the main driving force of the community is the visionary projects such that Medusa. Finally, he stated that one of the key factors is existence of the experience-sharing points like it was with e-magazine [5].

[1] `https://gnu.org`
[2] `http://theinvisiblethings.blogspot.com.es`
[3] `https://qubes-os.org`
[4] `https://thc.org`
[5] `http://www.phrack.org`

Following talk was by the malware analyst Marion Marschalek who work at the Cyphort. One of the most interesting topic was the concept of the "7 sins of malware", where she presented the common "flaws" of malware that makes it possible to detect zero-day samples successfully. The since are: So, we can see that the duration of life of a malware is determined by the how well it breaks the common patterns.

The final important talk this day was given by the security specialist at Google Fermin J. Serna, who worked before for Microsoft and started the hacking career in 1990th. He is know for his blog[6] where multiple tutorials on vulnerabilities and attacks are presented. So, this presentation was mainly about the life road of the known hacker.

The 3^{rd} day started with an insight into the history of JavaScript since 1996 by Stefano D. Paola who discussed why the language became so popular and what is the security implications to end-user and service providers. It can be seen that there have been developing wide range of new features and libraries for JS, yet this brings new attacks and vulnerabilities making the sensitive user information more vulnerable. First, Stefano explained the Same-Origin Policy (SOP) for the same protocol, host and port that was originally used in JS to protect the execution of unwanted scripts from external sources. Also he concentrated on the ways of performing the XSS attacks not only on the client side, but also on the server side. Second, several JS frameworks were exposed. Among them are Angular JS that allows to sandbox the execution of JS itself, NodeJS for designing network application both on the server and client side and QuakeJS is a port of Quake into JS that, however, reveals new attacks agains user data. The final part of the presentation was targeted on the review of Firefox OS[7] features that is a new concept of OS. Yet, again the main drawback of FirefoxOS is that vulnerable extensions might be installed even with thorough security evaluation process on the market side. So, the plugins and extensions may contain the bugs produced by vendors making the user data vulnerable even if the bowser itself is very secure and an audit was performed on it.

The following presentation was performed by Javier Marcos who works as a security engineer at Facebook. This presentation was particularly interested because Javier described how the Security defence works at the company. In particular he focused on the *Red Teams*, whose task is mainly to penetrate the infrastructure without revealing any specific attack details to other teams. So, the will try to hack the system when they want with arbitrary tools. While the task of the *Blue Teams* is to protect the network from possible attacks, prevent them and try to fix possible vulnerabilities. Beside this there were announced several projects carried out by Facebook recently. The first one is osquery[8], the low-level monitoring tool that provides a convenient way of gathering system information via SQL-like style of requests. The official pages of the Facebook for security [9] and CTF[10] event were announced.

The conclusion talk was from Spanish Ministry of Defence, who presented a way of performing active APT against the criminals and what are the major collaborations that they established with other agencies. Also it was quite interesting overview of the last APT performed against the countries and businesses including the attack on Estonian infrastructure in 2007, operation "Red October" and others. Finally, the role of the NATO CCDCOE center in Estonia was given.

[6] `http://zhodiac.hispahack.com/`
[7] `http://mozilla.org/firefox/os`
[8] `http://osquery.io/`
[9] `https://facebook.com/protectthegraph`
[10] `https://www.facebook.com/officialctf`