

SPARKS Events Series

Ionuț-Daniel BARBU

Romanian Association for Information Security Assurance

Cristian PASCARIU

Electronic Arts Romania

SPARKS #2

SPARKS #2 was the second conference in the SPARKS events series. This Security and Hacking meeting took place on April 14, 2014 at TechHub, Bucharest. That fact that this is intended as a place to meet security enthusiasts after work was confirmed also by this second event. The participants already felt connected and the atmosphere was a very productive one. As a consequence the number of questions was higher than the last time and discussions were also lucrative.

SPARKS #2 has begun with a very captivating presentation concerning the advantages and disadvantages of bug bounty programs. The discussion was structured on two important branches, observing the main points of view.

On one hand, from the hacker, ethical or not, perspective, the dispute looks as follows - the two options being: performing a penetration test and providing the results to the targeted company, therefore having the chance of obtaining an amount of money depending on the target's policy. The other approach could have been publicly disclosing the results and gaining the recognition of the communities.



Ionut Cernica

Section IV - Book Reviews and Conferences Analysis

On the other hand there are several companies implementing bug bounty programs. This state that, after signing an agreement, a user can legally perform security penetration tests against target's assets. This, of course has advantages and disadvantages as it can attract also hackers and large amounts of money to be paid.

In our opinion, Ionut Cernica held a very interesting presentation on this matter as he provided his own experience. He took part in various bug bounty programs for well-known companies such as Facebook, PayPal etc. The advantages in this situation was, as expected, the financial part. Companies have the tendency not to admit their assets' vulnerabilities therefore not keeping their part of the agreement. As a summary, we strongly recommend security enthusiasts to attend any presentation held by Ionut Cernica, Security Engineer at SafeTech Innovations.

The second presentation showed vulnerabilities in the mobile devices field. It is already well known that mobile device security becomes a very important branch of IT security due to bring-your-own-device programs. As a consequence, mobile communications companies are taking countermeasures on this matter. I am referring to both device producers such as Apple, Samsung, Nokia and also telecommunications service companies: Orange, Vodafone etc. The first impression was of a very well chosen title "Z.E.R.O - Zero Errors Rarely Occur". During his speech, Bogdan Alecu, System Administrator at Levi9 captivated the audience by constantly asking whether we knew that free calls can still be placed. Furthermore, the CVE-2014-1286 was detailed disclosing one of Apple's vulnerabilities. This reveals the possibility of performing a denial of service attack against Apple mobile devices. Apple's knowledge base site publicly disclose these vulnerabilities. As stated on this site, for the protection of customers, Apple does not disclose, discuss, or confirm security issues until a full investigation has occurred and any necessary patches or releases are available.

SPARKS #3

SPARKS #3, the third conference in the SPARKS events series, took place on June 2, 2014 at TechHub, Bucharest. Once more, this has proved to be the place to meet members of the security community after work.

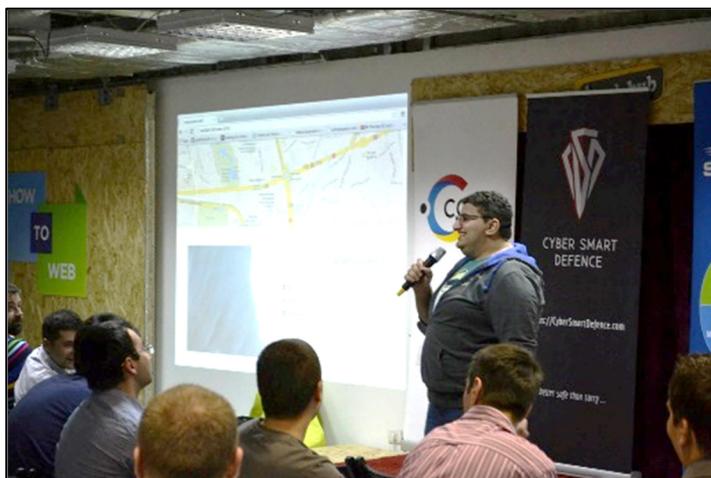


Ionut Popescu

Section IV - Book Reviews and Conferences Analysis

We are starting to get the feeling that we are already connected so the fact that after the presentations people stay for knowledge sharing sessions is quite normal. This time, the discussions were more intrusive, targeted and honest. The attendants are encouraged to speak their minds. As a consequence the number of questions was higher than the last time and discussions with regards to the subjects were also lucrative.

SPARKS #3 has begun with a deeply technical captivating presentation where Ionut Popescu took us step by step through shellcode development both for Linux and Windows. He marketed the presentation as a 101 course for writing your own code. As usual for this conference, the prerequisites are not so demanding, so even if an attendee was not skilled in shellcode writing, by the end of the presentation he would have gathered a general idea and basic knowledge on this matter. Additionally, the speaker, Penetration Tester for KPMG Romania introduced the audience to assembler programming languages. Ionut is a former software developer very passionate about security field. His research includes low level aspects of programming. Additionally, his studies include MCTS Windows internal certification. As a “white hat” hacker he is involved in one of the largest Romanian security forums - Romanian Security Team.



Vali-Marius Malinoiu

The second session of this event was held by Vali-Marius Malinoiu, a security enthusiast with very good presentation skills. Although the contents discussed were not so technical, he won the audience with his speech. Along the 30 minutes, Vali told the story of “A hacker who went fishing”. It is worth underlining that the hacker went fishing, not phishing. What Vali did, was placing a friend’s mobile device as bait somewhere in Bucharest for no reason. Actually, his purpose was to prove a point. He started his presentation by asking what we would do in case of phone loosing. He also was enquiring whether we have a back-up plan.

To be more precise, Vali developed an Android Remote access tool bases on a client server structure. After installing the client on the mobile device and configuring the software, he placed the phone in a public restaurant and left it there. Not surprisingly, the device was taken and the installed software started to do its job. What this means is that every 10 minutes, the device silently takes a photo and sends it to the server. Additionally, it attaches the location. It is worth mentioning that the location is obtained

Section IV - Book Reviews and Conferences Analysis

through Google Services and not directly by GPS. As a consequence, the energy consumption is notably low. Furthermore, to reduce the risk of being uninstalled, the software is installed as a default service, making it hard to detect as a running application. Lastly, Vali informed us that for setting everything up, the device must be rooted. His project can be found on GitHub and can prove to be useful in an unfortunate event.

As expected, by the end of the presentations, the attendants started sharing ideas and experience so this SPARKS session also finished in a very friendly manner. Already a custom, SPARKS accommodates both security home practitioners and corporate employees. The attendance was free of charge which made it available to a wide variety of technical fellows from university students, IT employees, security specialists to just passionate people. However for administrative purposes, prior registration and confirmation was required. For further details and for future events we strongly recommend the conference's web page: *sparks.ccsir.org*.

In the end of this article we would thank to Andrei Avadanei, the leader of the organizing team. This proves to be recurrent in Bucharest Information Security community. To conclude, we are really looking forward to the next month meeting.

Source: sparks.ccsir.org

Photos: cristiannicolau.wordpress.com