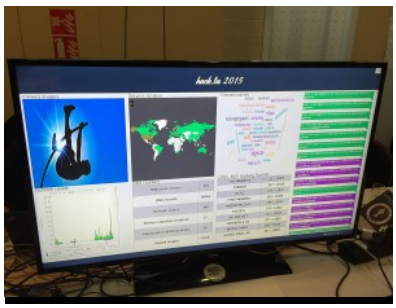
Hack.lu 2015 Wrap-Up Day #3

October 22, 2015 20:14 | 9 Comments | Xavier



I just drove back to home after the 11th edition of hack.lu. As always, it was an amazing event organized by, amongst others, many team members of the CIRCL. So, let's write a quick wrap-up for this third day. Some talk will be less covered due to interesting chat sessions with a lot of infosec peers.

Like yesterday, this day started with a high level talk: "*Why Johnny can't unpack?*" by shift. The goal was to explain how to improve the analysis of pieces of malware. In a "road to attribution" process, we have three phases: get pwned, find who's behind the attack then unpack. But this last step can be complex and time consuming.

For better results, we need to increase the unpacking rate with a reliable, scalable solution and a stealth infrastructure. Shift explained also the different tools that he used to build his environment with pro & con and the challenges he faced. The sandbox is based on a modified version of Qemu. This was not my domain and we lost in the slides.

Then, a more entertaining talk: "*Forging the USB Armory*" by Andrea Barisani and Daniele Bianco. It seems that many people already knew the USB Armory in the audience. Personally I own one for a few months: it's an amazing device. This tiny computer with the size of an USB key can be considered as an "*hardware netcat*". You can use it for many daily tasks like:

- SSH proxy
- Mass storage
- Password manager
- Authentication token

And many more! It runs a Linux operating system.It's a SoC ("*System on a Chip*") based on compact USB powered board with a fast CPU, secure boot, standard connectivity and fully open source! Andrea explained the story of the project, how the PCB was designed and the challenges they faced and also some issues like the "*5-seconds delay*" issue due to bad copper USB connectors. The USB Armory uses the Freescale i.MX53 processor which supports advanced security features like secure boot and ARM TrustZone. Amongst the other tools, Andrea made a really cool demo of the tool they developed for (but not restricted to) the USB Armory: INTERLOCK. It's an open source file encryption front-end.

The next talk was presented by Sophia D'Antoine: "*Binary Constraint Solving with LLVM*". LLVM is collection of modular and reusable compiler and toolchain technologies. Sophia explained how to use specific tools to find execution path via side channel analysis. This talk was really out of my knowledge but kudos to Sophia for mastering her topic.

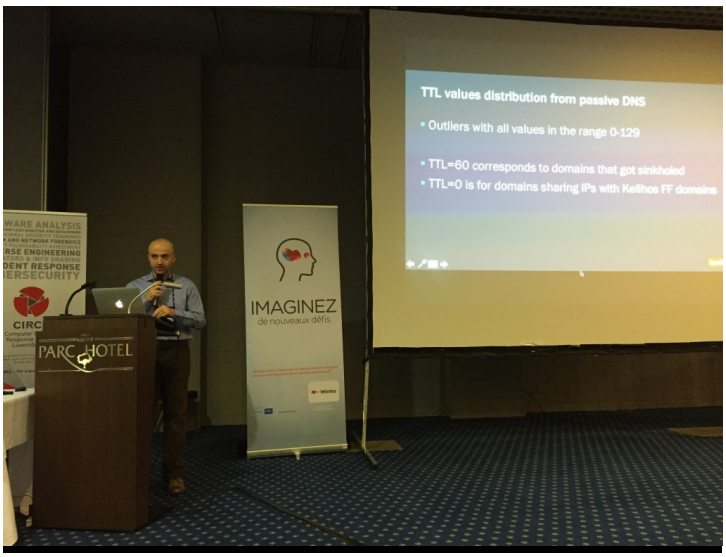
Netanel Rubin presented "*They hate us 'cause they ain't us – How we broke the Internet*". Strange title but after a few slides it was very clear: The topic of secure coding is everywhere: in books, brochures, websites. Secure coding is a code development practice and mitigate basic vulnerabilities made by security experts for non-security experts. There are trainings available but why all developers pass the same training? Such trainings focus on input sanitization but avoid false assumptions and logical vulnerabilities. Netanel demonstrated this by reviewing case studies. For each of them, he explained how the tool/application was pwn3d.

- Case 1 : MediaWiki (which runs Wikipedia and 25K other sites). MediaWiki relies on external livs for many tasks. Netanel explained how a RCE was found.
- Case 2: vBulletin (the most popular forum platform). It used serialize() which is a very dangerous function in PHP.
- Case 3: Bugzilla: This time, Perl was abused via a specific feature: called lists.
- Case 4: Magento (the e-commerce solution)
- Case 5: WordPress (70M of websites!)

Netanel's conclusion: secure coding does not guarantee secure code. It provides another layer of security. Hire hackers to do code review, pentesting and… do not rely on your trainings! IMHO, the

best talk of today!

After the lunch and a funny session of PowerPoint Karaoke with many bamboos (private joke for those who attended), back to the talk. Dhia Mahjoub presented "*A Collective View of Current Trends in Criminal Hosting Infrastructures*". Dhia is working for OpenDNS and DNS is a very nice protocol to gather juicy data, they have access to a huge amount of information. Dhia reviewed many information collected via the OpenDNS servers which helped to map malwares and C&C to hosts. He reviewed some of the wellknown exploit-kits and explained where and how they are hosted/distributed. He was also able to build a list of companies hosting malicious code.



Introduction to Crema, a LangSec inspired programming language by

The next speaker was Jacob Torrey who make an introduction to a new programming language called Crema. Very similar to C, it forces programmers to more accurately express their intend and the result is an improved security. Why a new language? The Internet security is failing due to many input handling issues at all layers. Jacob compared developpers handling inputs to 16 years old people driving a Ferrari… It's dangerous and not easy to master!vBy using Crema, your software will magically be easier to analyse and safer.

After the last coffee break, Aaron Zauner presented his research about the usage of the TLS protocol in SMTP communications: "*No need for Black Chambers: Testing TLS in the E-mail Ecosystem at Large*". Why this talk? not a lot of research against TLS for email (compared to HTTPS). Gmail is used by millions of people but they're also millions of mail relays around the Internet. Recap about ports used by mail: 25, 110, 143, 465,587, 993 & 995.

The methodology used in the research was a classic approach. Aaron used masscan for discovery and X509 cert collection. A customised sslyze was also used. More than 10 billions of TLS handshake were captured. What about the results?

- 20M scans

Vuln: Libxml2 'xmlParseConditionalSections()' Function Denial of Service Vulnerability

Bugtraq: [oCERT 2015-012] Ganeti multiple issues

Bugtraq: WebKitGTK+ Security Advisory WSA-2015-0002

Bugtraq: libtiff bmp file Heap Overflow (CVE-2015-8668)

Bugtraq: libtiff: invalid write (CVE-2015-7554)

More rss feeds from SecurityFocus

Many other results and graph were reviewed by Aaron. Interesting stuff! A few words were given about the abuse-process used during this research. Indeed, while you scan the Internet, you must be prepared to wake up angry people. They received 89 complaints, 52 automated IDS messages and 16 blacklist requests. You can also expect a lot of spam!

And finally, the closing speaker was Werner Tillmann with "*Improving Flash Exploits Analysis*". Flash has been targeted by many exploits recently and 2015 was really a bad year for Adobe. Some organisations decided to disable support of swf files and Mozilla decided to block the plug-in in the latest releases of their browser. Werner gave a very nice number: 245 vulnerabilities were solved by Adobe in 2015! But how do you analyse a swf file? As the Angler exploit kit is using Flash, it can be a good idea to analyze them. But it takes time and the available tools were not efficient enough for Werner. That's why he developed his own toolbox in Python. He released the first version for hack.lu! The code is available here.

That's all folks! See you in 2016 for the next edition and don't forget that the slides are available online.

← Previous Post Next Post →