

/dev/random

Can't sleep, hackers will eat me!



Search



About Me ▾

Disclaimer

Tools ▾

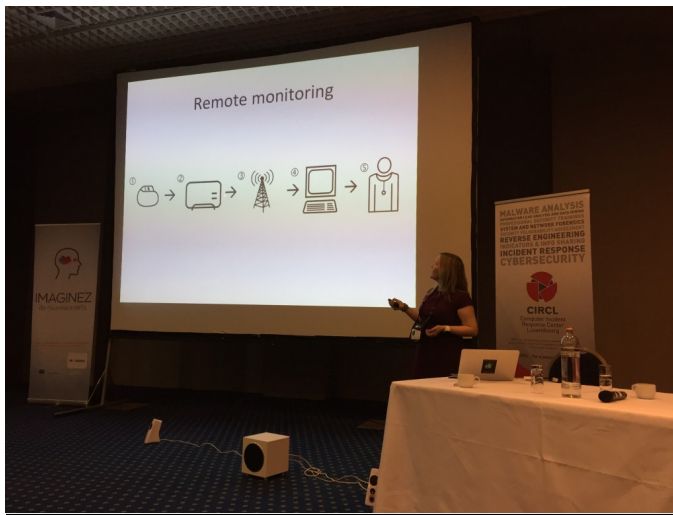
Hack.lu 2015 Wrap-Up Day #1

October 20, 2015 22:08 | 40 Comments | Xavier



Today started the 11th edition of hack.lu in Luxembourg. Being one of my preferred event, I drove to Luxembourg this morning direction to the Alvisse Parc hotel! The first day started with a security breakfast and a round table. **Marie Moe** talked about medical devices. The topic was "How to improve cyber safety of medical devices". Marie talked more precisely about pacemakers. She has one and her life depends on it. That's why she's very concerned about the security around those devices.

Pacemakers have remote monitoring features over wireless. For Marie, they have potential threats: Is the device vulnerable? Is the access point used vulnerable? Is the network compromised? Is the vendor server compromised? They are huge chances that the answer to those questions is yes. Other hackers, like **Barnaby Jack**, already disclosed some results in the same way. Another type of medical devices which was in the news recently: drugs pumps. They were **vulnerable** to remote attacks too.



Why medical devices are so exposed? By the way they are used/deployed in hospitals. They use legacy technologies, are not updated, they are often seen as blackboxes and use proprietary software and protocols. According to Marie, we must give more focus on medical devices to improve the security. How? By doing more security researches, by increasing vendors' awareness and by increasing the security risk monitoring. For more information about medical (as well as other connected) devices, have a look at **I am The Cavalry** which is an organization that is focused on issues where computer security intersects public safety and human life.

Marie's presentation was followed by a panel discussion but I left to attend the Malcolm workshop proposed by **Sébastien Larinier** and **Thomas Chopitea**. **Malcom** is an open source tool written in Python. This tool is used to better understand malware communications between malware samples and their C&C by sniffing or reading PCAP's and sharing IOC via an API. I already read a lot about this tool but never had a chance to play with it.

Powered by



Follow Me



Upcoming Events

Here is a list of events that I will attend and cover via Twitter and wrap-ups. Ping me if you want to meet! The list is regularly updated.



Recent Posts

The Truth is in Your Logs!

Physical Access == Pwn3d!

[SANS ISC Diary] Unity Makes Strength

Managing Palo Alto Firewalls Custom URL Categories

[SANS ISC Diary] Enforcing USB Storage Policy with PowerShell

Popular Posts

The Truth is in Your Logs!

2,039 views

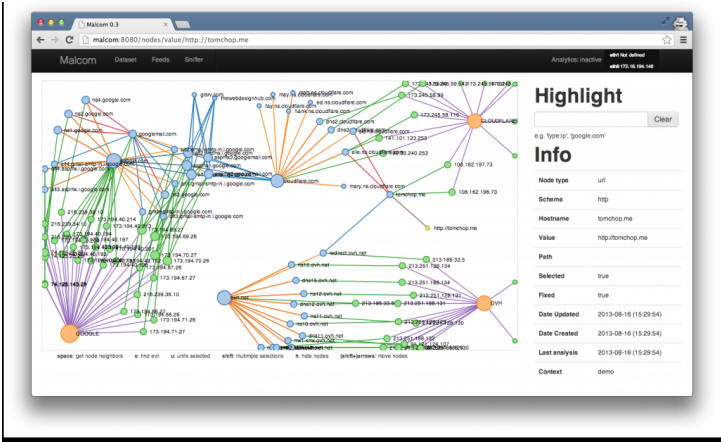
Physical Access == Pwn3d!

360 views

Managing Palo Alto Firewalls Custom URL Categories

205 views

Show me your SSID's, I'll Tell Who You Are!



For a first contact, I enjoyed it and I decided to install it on my own network for malware analysis. The goal of this workshop was to present the features of Malcom with different scenarios and plugins and explain the public API interaction and plugin development. See it as a “*high level wireshark*”. It has multiple components: web app, feed engine, analytics engine, sniffer engine. The feed engine is really nice and help you to integrate external source of IOC’s into your Malcom instance to improve the detection of malicious activities. The workshop was well organized and we had exchanged interesting point of view and improvements for the next version.

Paul Rascagnères was present multiple times on the schedule this year. For the first time, he was asked to be a keynote speaker and receive a “green light” from the organizer about the topic. By knowing Paul, we could expect something funny and we were not disappointed! His keynote was called “*Internet of Tchotchke*”. Based on the **urban** dictionary, a “*tchotchke*” is a small piece of worthless crap, a decorative knick knack with little or no purpose. He presented some researches about connected objects like wearable stuffs, sensor, Arduino’s, etc. For a world premiere, Paul presented his connected underwear fully equipped with sensors:

- Humidity and temperature sensors
- Flex sensor to have telemetry of the underwear usage
- Buzzer to alert the user
- Radare2 support
- Bluetooth

“*Connect all the things*” they said? Paul did it! This was awesome and will be remembered for a long time...

179 views

Sending Windows Event Logs to Logstash

126 views

dns2tcp: How to bypass firewalls or captive portals?

125 views

Forensics: Reconstructing Data from Pcap Files

87 views

Vulnerability Scanner within Nmap

77 views

Keep an Eye on SSH Forwarding!

Email Tracking for Dummies

Recent Tweets

#CCC is alive! src_ip="151.217.0.0/16" - > 245 hits in my logs since 26th Dec... 11 hours ago

Usually, we're looking for a password... Here, I found one and I'm looking to who it belongs ;-) 13 hours ago

Any idea why all cmds return "Rex::TimeoutError Operation timed out" in a valid #Meterpreter session!? #LazyTweet 16 hours ago

xortool.py: a tool to guess the key length and key of a XOR'd file (kitploit.com/2013/02/xortool...) 19 hours ago

Anybody has access to a #Barracuda spam firewall? I've a question... (Please RT) 2 days ago

Follow Me on Twitter

Time Machine

Time Machine

Select Month

"SecurityFocus Vulnerabilities"

Vuln: Google Chrome Prior to 47.0.2526.106 Multiple Remote Code Execution Vulnerabilities

Vuln: libxml2 CVE-2015-7500 Denial of Service Vulnerability

Vuln: Mozilla Firefox Multiple Security Vulnerabilities



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

Then, Paul reviewed some hardware is tested and tried to abuse like...

- Wireless door bell
- ATM skimmer
- Encrypted hard drive
- Linux embedded devices (OpenWRT)

But... maybe the most obscure object that you could imagine to see in a "connected" version: a sex toy sold by **Marc Dorcel**! I let you imagine many different ways to abuse this toy for the good or the bad!



Paul concluded his keynote on more serious facts. For him, we already saw real cases of embedded system abuse? Good examples are the recent Cisco SYNful knock, payment terminal fake firmware, hacking team BIOS compromise. Paul see more and more attacks of the same time in the future. Can we still trust our hardware already today, routers, gateways. Is it the next trend?

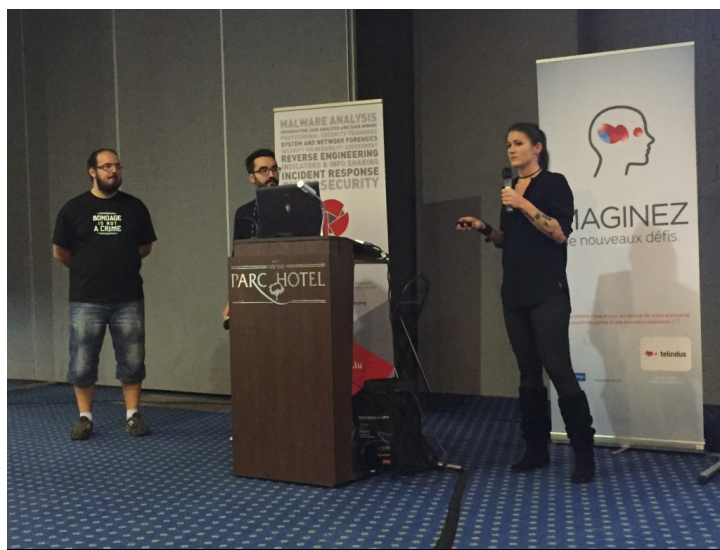
After the lunch, the first lightning talk sessions was organized before a new set of speaker. I like the

quick presentation of **Pretty Easy Privacy** by Leon Schumacher. A very interesting tool, have a look at it! The first speaker of the afternoon was **Eleanor Seitta** with her talk called “*Security Design and High-Risk Users*”. It was not a technical presentation but contained a lot of interesting ideas. Our environment is based on fundamental mistake: people built computers to make tasks, then computers were connected to networks to make them perform more tasks, computer are owned and we pay people to fix them. etc... This is a recurring issue and the approach is wrong. That’s what explained Eleanor. She defined big principles like “security“, “security design“.



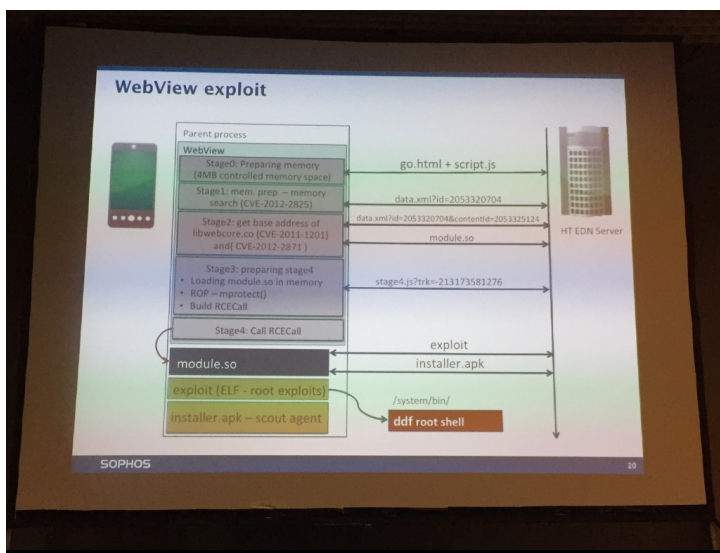
She explained how to map security tasks to the SDLC (“Software Development Life Cycle”). The next step was to define the threat modelling. Keep in mind that more you wait, more it will cost! About the security systems, don’t forget that they will be used by humans! Here is a link to Eleanor’s [presentation](#), it is worthwhile to read

Then Paul came back on stage with his friends **Marion Marshalek** and **Joan Calvet** with “*Totally Spies!*”. Those three malware researchers have a broad knowledge of the multiple campaigns of attacks based on well-known malicious codes called Bunny, Babar, Casper, etc.



They reviewed the story of most of those malwares, when and how they were detected, what were their features, targeted systems, etc. Interesting but less funny than Paul’s keynote.

Attila Marosi presented a talk about Hacking Team: “*How they infected your Android device by 0-days*”. Hacking team RCS (“Remote Control System”) – product for law enforcement agencies (only!) and for all brands of mobile devices. Attila reviewed the big leak that affected hacking team in July 2015. Just to remind you, some numbers: 400GB, 53 GIT repos, 6 0-day exploits, documentation, company emails. Email is a good source of information. The hacking team’s leak helped to understand how works the market of 0-days.



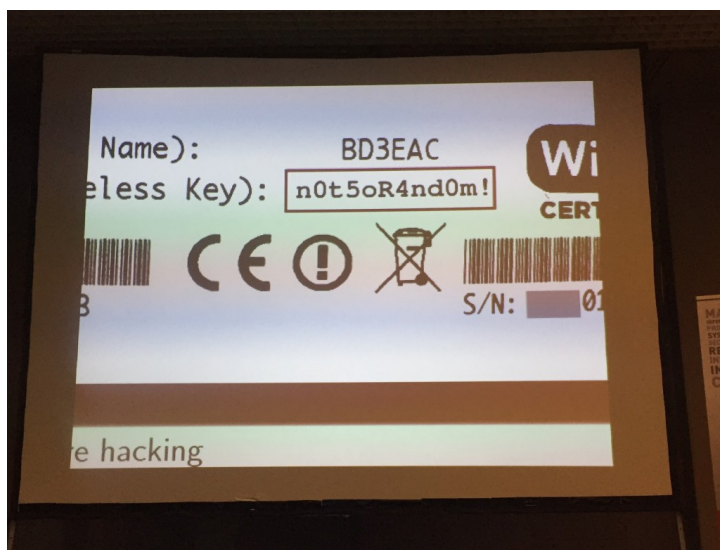
About the RCS agent on Android, the infection process was explained and what are the collected information. Installed as an admin application, it hooks the media server system to intercept all audio content (including phone conversations). Other traditional evidences are also collected (screenshots, location, clipboard content, exfiltration of data). To infect a device, they are two main ways. The boring one: a rogue email with a malicious link which is not always easy to trigger user interaction). The second one is more funny: hijack the network flows (play MitM) via public WiFi or ISP and inject content on the fly. A demo should be performed but, due to crappy wireless connectivity, it was not possible (tip for the speaker: always have a recorded video of your demos!). What is more scaring? Millions of vulnerable devices (4.0 Ice Cream Sandwich, 4.3 Jelly Bean) are still in the wild and the **webview** exploit is now publicly available. Many devices cannot be updated!

After a refreshment break, Ronan Mouchoux and **Thomas Chopitea** presented “*How digital forensics met threat intelligence*”. Threat Intelligence relies on feeds: “*If you’re blind, feed providers are one-eyed*”. They explained multiple concepts related to TI and presented interesting facts and reviewed classic definitions:

- threat = intent x capability x opportunity
- risk = vulnerability x threat x impact

The process is the following: Environment -> Data -> Information -> Intelligence and intelligence is a cyclic process. The DFIR process is based on four components: Prepare -> Respond -> Restore -> Learn. For some threats, we can be pro-active. Example with blackmailing: why not scan for emails and search for sources inside the mails? Another one: Cryptolocker is a malware which communicates with C2 using time-based DGA ("*Domain Generated Algorithm*"). If we are able to reverse the DGA process, why not block all the domains for the next two years? Thomas & Ronan gave multiple examples and also which tools can be used to improve our daily job (MISP, FIR, CRITS) but also standards (MITRE, IETF, OpenIOC, Yara, Veris, etc). A final remark from the speakers: stop providing free audits to the bad guys! As example, they demonstrated how IP addresses of C2 changed after Mandiant released the report about APT-1!

The next talk was “*Scrutinising WPA2 password generating algorithms in wireless routers*” by Eduardo Novella. The talk was about to find how the WPA/WPA2 keys written on routers are generated.



Interesting topic was very broad and Eduardo had too many slides for his allowed time slot! I started by explaining how the WPA 4-way handshake is working then he jumped into the analysis of a router firmware. The first step is to get a copy of the firmware. How? Direct download from the manufacturer, by exploiting the device, by discovering HW debug interfaces or desoldering the chip. Once the firmware acquired, it's time to perform some reverse engineering to understand the key generation process. After slides and slides of assembler code, Eduardo reviewed some well-known router models that he pwned. He performed a massive job with this research!

Then, a recordman came on stage: **Saumil Shah**! He is the guy who spoke most at hack.lu! He presented his research around steganography and his tool called Stegoploit (*"Delivering drive-by exploits with only images"*). I already attended this presentation in Amsterdam during the last edition of HITB. See my [wrap-up](#) for more details. This talk was amazing!

The last presentation for this first day was the one of Paul Jung: *"Learn from malwares, a practical guide of spear phishing for Red Teams"*. A classic phishing attack is based on a 4-steps process:

This website uses cookies to improve your experience. By using our services, you agree to our use of cookies. [Accept](#) [Learn more](#)



For me, this was the best talk of the day, nothing brand new but it was clearly explained and, at each step, counter-measures were proposed to reduce the attack surface.

First, ask google or use tools like *"The Harvester"*, find the mail format and grab addresses (linkedin.com is a nice tool for this). Test the mail relay to validate emails, only 1 tcp connections on the firewall. We can also easily abuse **SPF**... spoofing is indeed possible at body level. How to protect? Monitor your mail gateway, configure anti-bruteforce, deny mails from unknown domains, use **SPF** at least and work on spoofing scenarios.

Then bypass inbound controls. Paul gave interesting tips to obfuscate URL but also many ways to bypass classic antivirus checks or, more and more present in organizations, sandbox systems. Amongst classic evasive checks, Paul gave interesting tips like:

- Trying to load a missing DLL
- Detect if the target computer is in a Windows domain or not
- Some code sample to bypass Cuckoo

Finally, he explained how to bypass outbound controls. Ex: use WinInet which support proxies! Very useful in big organizations. This was a really nice talk based on real facts and techniques. The first day ended with a nice social event and a walking dinner.

Keep an eye on <http://archive.hack.lu/2015/> where slides should be available soon. Stay tuned for the day 2 tomorrow!

 Like  Share  4 Tweet  StumbleUpon  Pin It

Posted in: [Security](#), [Event](#) | Tagged: [Security](#), [Event](#), [Luxembourg](#), [hack.lu](#)

Profile

Sign in with Twitter Sign in with Facebook

or

Comment

Name

Email

Not published


Website

Post It

- 40 Replies
- 0 Comments
- 40 Tweets
- 0 Facebook
- 0 Pingbacks

Last reply was 2 months ago



1.  @kerouanton

View 2 months ago

@xme Your wrap-ups are always great, thanks for caring about those who didn't made it to hack_lu 😊

2.  @cbrocas

View 2 months ago

@MarieGMoe perfect ! Thanks Marie, will be in the room, wish you the best 😊 @xme



3. @MarieGMoe

[View 2 months ago](#)

@cbrocas @xme The more detailed (and more personal) presentation is on today at 13:30
#hacklu



4. @cbrocas

[View 2 months ago](#)

@xme so strange : peacemakers monitoring was scheduled on wednesday afternoon, no ?
Would be so sad I missed it ... :-/

[← Previous Post](#)[Next Post →](#)