



Welcome to

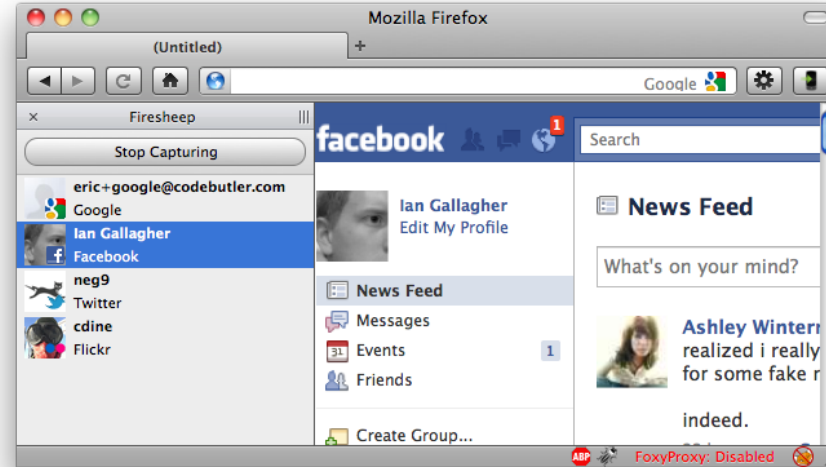
IT-sikkerhed: Finding malware signs

PROSA Superhelteseminar 2016

Henrik Lund Kramshøj hk@zencurity.dk

Slides are available as PDF, [kramshoej@Github](https://github.com/kramshoej)

Goals of today



Do you have malware?

Is your hardware infected?

How do we help ordinary people become secure - again

Please give feedback and join me in discussions, dialogue 😊

Plan for today



KI 10:30-13:00

Less presentation, more talk. more real data

Less me talking (only) and more 2.0 social media interaction

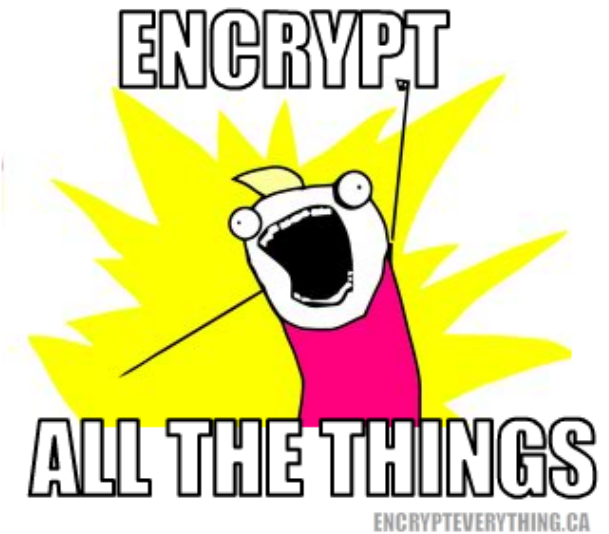
Trying to fit in demo and workshop-like stuff

Generic advice



Recommendations

- Lock your devices, phones, tables and computers
- Update software and apps
- Do NOT use the same password everywhere
- Watch out when using open wifi-networks
- Multiple browsers: one for Facebook, one for banking apps?
- Multiple laptops? One for private data, one for work?
- Think of the data you produce - where is it stored
- Use pseudonyms and aliases, do not use your real name everywhere
- Enable encryption: IMAPS, POP3S, HTTPS and full disk encryption
- Use Tor <http://torproject.org/>



The current situation



Personal computers like laptops suck at security

Mobile devices suck even more at security - less CPU/MEM/storage

Internet of Things (Thrash?) are insecure in many cases

Malware is rampant - all type of devices are being infected

Goals: Internet Ninjas



Real super heroes are just ninjas

By knowing the internet, technologies and possibilities

Using technology and knowledge make it seem magical

In reality preparedness and defense in depth go a looooong way

Common sense is not magic, structured methods are king

Challenges



Identifying infected systems

Lots of new malware, virus, vulnerabilities and hacking

Dataloss ransomware, theft

Loss of confidentiality, 2014: 700 million lost accounts

Your boss wants: No cost, and please show us great results

Solutions



Automate your job

Use hackertools to detect and identify

Categories, sort, prioritize, group problems - solve more

Measure, collect and present - make it pretty

Learn from devops, Elasticsearch Logstash Kibana D3.js

Hackertools are for everyone!



- Python programming language, download and run programs
- Web technologies, start a web server
- Download projects from Github, read instructions
- Generic server Ubuntu Linux <http://www.ubuntu.com/>
- Pentest, Hacking and Demo Kali Linux <http://www.kali.org>

You can learn to work these for good - or bad, dont do that 😊

Case: Maltrail



Maltrail is a malicious traffic detection system, utilizing publicly available (black)lists containing malicious and/or generally suspicious trails, along with static trails compiled from various AV reports and custom user defined lists, where trail can be anything from domain name (e.g. `zvpprsensinaix.com` for **Banjori** malware), URL (e.g. `http://109.162.38.120/harsh02.exe` for known malicious **executable**), IP address (e.g. `185.130.5.231` for known attacker) or HTTP User-Agent header value (e.g. `sqlmap` for automatic SQL injection and database takeover tool). Also, it uses (optional) advanced heuristic mechanisms that can help in discovery of unknown threats (e.g. new malware).



<https://github.com/stamparm/maltrail>

Lets get to work!



- Get Maltrail working, should already be running
- Get access to Maltrail
- Produce some data
- Review data

Use-cases for Maltrail



- Family and friends, *My computer is acting strangely*
- Your kids, when you get some
- Stalking victims
- Abuse victims, large percentage in women shelters infected
- @work - help identify infected systems quickly

Quick, cheap, few resources needed, easy to deploy - great!

Censorship



- You are using my network 😊
- I can read your traffic
- I can redirect your traffic
- I can censor your traffic or your DNS

Avoiding Censorship



- Change DNS server
<http://censurfridns.dk/>
- Use DNSSEC Trigger and get a nice built-in DNS just for you
<https://www.nlnetlabs.nl/projects/dnssec-trigger/>
- Use a VPN

Conclusions and discussion



- How many laptops/devices seems to be infected?
- What does infected mean?
- What is allowed in YOUR network?

Questions?



Henrik Lund Kramshøj hlik@zencurity.dk

Need DDoS testing or pentest, ask me!

You are always welcome to send me questions later via email

Did you notice how a lot of the links in this presentation use HTTPS - encrypted