Welcome to

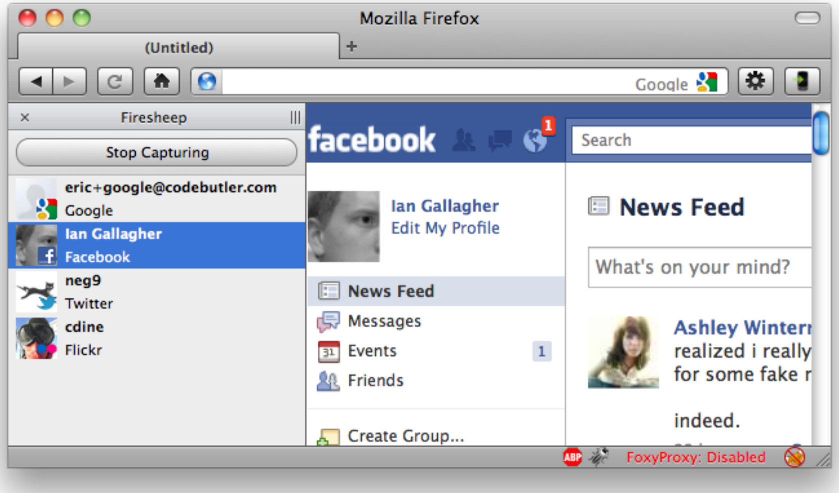
IT-sikkerhed: Finding malware signs

PROSA Superhelteseminar 2016

Henrik Lund Kramshøj hlk@zencurity.dk

Slides are available as PDF, kramshoej@Github

Goals of today



eric+google@codebutler.com
Google
Ian Gallagher
Facebook
neg9
Twitter
cdine
Flickr

Ian Gallagher
Edit My Profile

News Feed

What's on your mind?

Ashley Winterr
realized i really
for some fake r

indeed.

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

Kl 10:30-13:00

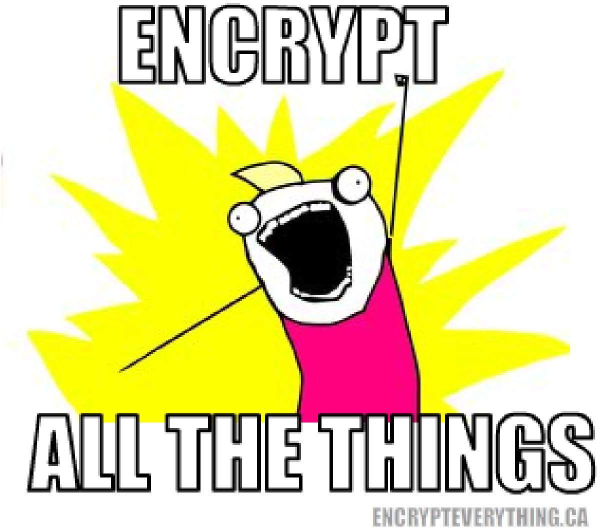
Less presentation, more talk. more real data

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: IMAP**S**, POP3**S**, HTTP**S** 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

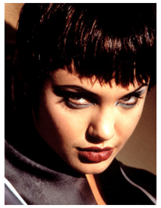
Use hackertools to detect and identify

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!

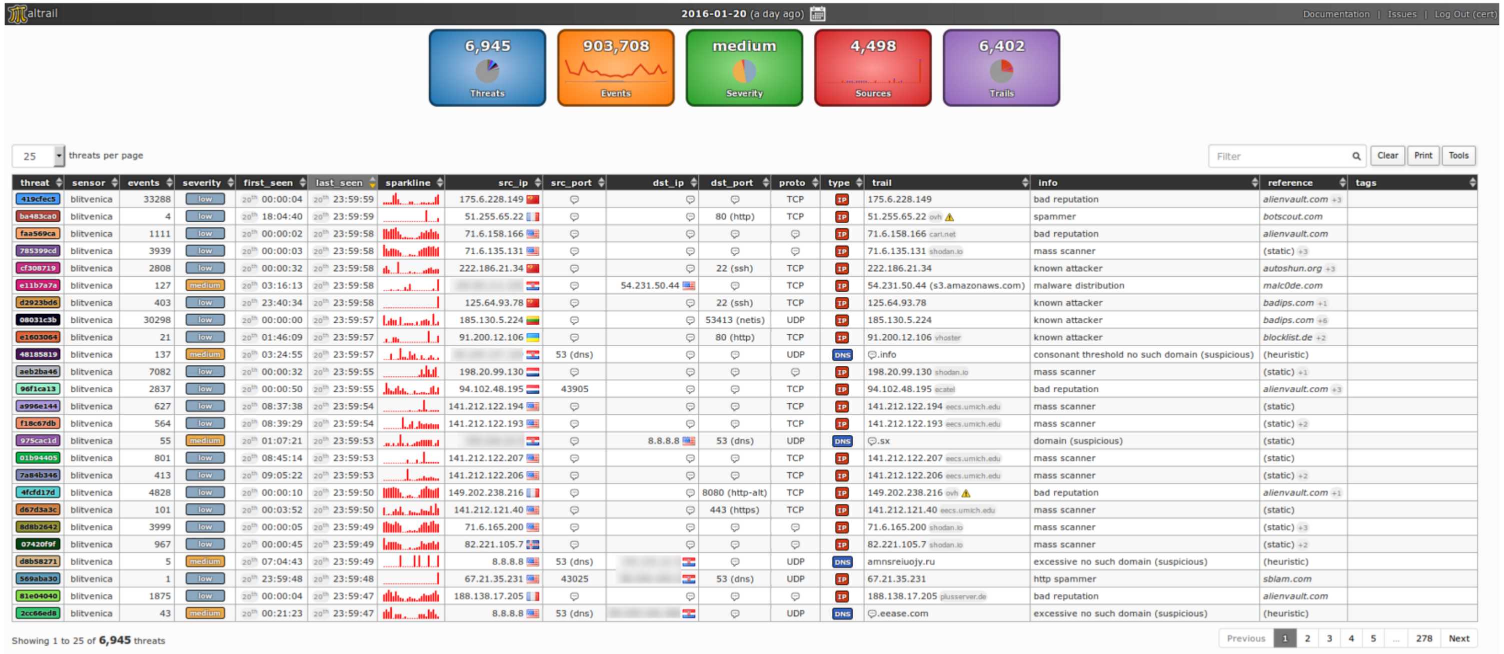


- Python programming language, download and run programs
- Web technologies, start a web server
- Download projects from Github, read instructions
- Generic server Ubuntu Linux `http://www.ubuntu.com/`
- Pentest, Hacking and Demo Kali Linux `http://www.kali.org`

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).



2016-01-20 (a day ago)

6,945 Threats | 903,708 Events | medium Severity | 4,498 Sources | 6,402 Trails

25 threats per page

threat	sensor	events	severity	first_seen	last_seen	sparkline	src_ip	src_port	dst_ip	dst_port	proto	type	trail	info	reference	tags
419cfec5	blitvenica	33288	low	20th 00:00:04	20th 23:59:59		175.6.228.149	🗨	🗨	🗨	TCP	IP	175.6.228.149	bad reputation	alienvault.com +3	
ba483ca0	blitvenica	4	low	20th 18:04:40	20th 23:59:59		51.255.65.22	🗨	🗨	80 (http)	TCP	IP	51.255.65.22 ovh ⚠	spammer	botscout.com	
faa569ca	blitvenica	1111	low	20th 00:00:02	20th 23:59:58		71.6.158.166	🗨	🗨	🗨	🗨	IP	71.6.158.166 cari.net	bad reputation	alienvault.com	
785399cd	blitvenica	3939	low	20th 00:00:03	20th 23:59:58		71.6.135.131	🗨	🗨	🗨	🗨	IP	71.6.135.131 shodan.io	mass scanner	(static) +3	
cf308719	blitvenica	2808	low	20th 00:00:32	20th 23:59:58		222.186.21.34	🗨	🗨	22 (ssh)	TCP	IP	222.186.21.34	known attacker	autoshun.org +3	
e11b7a7a	blitvenica	127	medium	20th 03:16:13	20th 23:59:58		[redacted]	🗨	54.231.50.44	🗨	TCP	IP	54.231.50.44 (s3.amazonaws.com)	malware distribution	malc0de.com	
d2923bd6	blitvenica	403	low	20th 23:40:34	20th 23:59:58		125.64.93.78	🗨	🗨	22 (ssh)	TCP	IP	125.64.93.78	known attacker	badips.com +1	
08031c3b	blitvenica	30298	low	20th 00:00:00	20th 23:59:57		185.130.5.224	🗨	🗨	53413 (netis)	UDP	IP	185.130.5.224	known attacker	badips.com +6	
e1603064	blitvenica	21	low	20th 01:46:09	20th 23:59:57		91.200.12.106	🗨	🗨	80 (http)	TCP	IP	91.200.12.106 vhoster	known attacker	blocklist.de +2	
48185819	blitvenica	137	medium	20th 03:24:55	20th 23:59:57		[redacted]	53 (dns)	🗨	🗨	UDP	DNS	🗨.info	consonant threshold no such domain (suspicious)	(heuristic)	
aeb2ba46	blitvenica	7082	low	20th 00:00:32	20th 23:59:55		198.20.99.130	🗨	🗨	🗨	🗨	IP	198.20.99.130 shodan.io	mass scanner	(static) +1	
96f1ca13	blitvenica	2837	low	20th 00:00:50	20th 23:59:55		94.102.48.195	43905	🗨	🗨	TCP	IP	94.102.48.195 ecatel	bad reputation	alienvault.com +3	
a996e144	blitvenica	627	low	20th 08:37:38	20th 23:59:54		141.212.122.194	🗨	🗨	🗨	TCP	IP	141.212.122.194 eecs.umich.edu	mass scanner	(static)	
f18c67db	blitvenica	564	low	20th 08:39:29	20th 23:59:54		141.212.122.193	🗨	🗨	🗨	TCP	IP	141.212.122.193 eecs.umich.edu	mass scanner	(static) +2	
975cac1d	blitvenica	55	medium	20th 01:07:21	20th 23:59:53		[redacted]	🗨	8.8.8.8	53 (dns)	UDP	DNS	🗨.sx	domain (suspicious)	(static)	
01b94405	blitvenica	801	low	20th 08:45:14	20th 23:59:53		141.212.122.207	🗨	🗨	🗨	TCP	IP	141.212.122.207 eecs.umich.edu	mass scanner	(static)	
7a84b346	blitvenica	413	low	20th 09:05:22	20th 23:59:53		141.212.122.206	🗨	🗨	🗨	TCP	IP	141.212.122.206 eecs.umich.edu	mass scanner	(static) +2	
4fcfd17d	blitvenica	4828	low	20th 00:00:10	20th 23:59:50		149.202.238.216	🗨	🗨	8080 (http-alt)	TCP	IP	149.202.238.216 ovh ⚠	bad reputation	alienvault.com +1	
d67d3a3c	blitvenica	101	low	20th 00:03:52	20th 23:59:50		141.212.121.40	🗨	🗨	443 (https)	TCP	IP	141.212.121.40 eecs.umich.edu	mass scanner	(static)	
8d8b2642	blitvenica	3999	low	20th 00:00:05	20th 23:59:49		71.6.165.200	🗨	🗨	🗨	🗨	IP	71.6.165.200 shodan.io	mass scanner	(static) +3	
07420f9f	blitvenica	967	low	20th 00:00:45	20th 23:59:49		82.221.105.7	🗨	🗨	🗨	🗨	IP	82.221.105.7 shodan.io	mass scanner	(static) +2	
d8b58271	blitvenica	5	medium	20th 07:04:43	20th 23:59:49		8.8.8.8	53 (dns)	[redacted]	🗨	UDP	DNS	amnsreiuojy.ru	excessive no such domain (suspicious)	(heuristic)	
569aba30	blitvenica	1	low	20th 23:59:48	20th 23:59:48		67.21.35.231	43025	[redacted]	53 (dns)	UDP	IP	67.21.35.231	http spammer	sblam.com	
81e04040	blitvenica	1875	low	20th 00:00:04	20th 23:59:47		188.138.17.205	🗨	🗨	🗨	🗨	IP	188.138.17.205 plusserver.de	bad reputation	alienvault.com	
2cc66ed8	blitvenica	43	medium	20th 00:21:23	20th 23:59:47		8.8.8.8	53 (dns)	[redacted]	🗨	UDP	DNS	🗨.eease.com	excessive no such domain (suspicious)	(heuristic)	

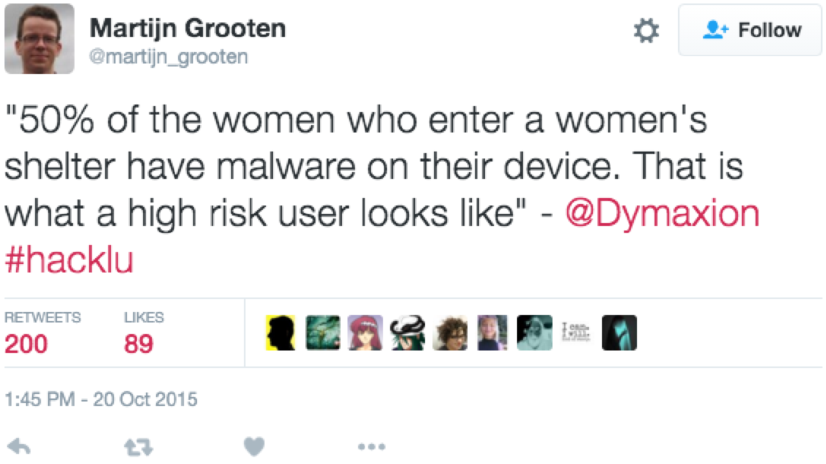
Showing 1 to 25 of **6,945** threats

`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



Martijn Grooten
@martijn_grooten

"50% of the women who enter a women's shelter have malware on their device. That is what a high risk user looks like" - @Dymaxion #hacklu

RETWEETS 200 LIKES 89

1:45 PM - 20 Oct 2015

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

Maltrail - 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 hlk@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