

Welcome to

IT-sikkerhed 2014

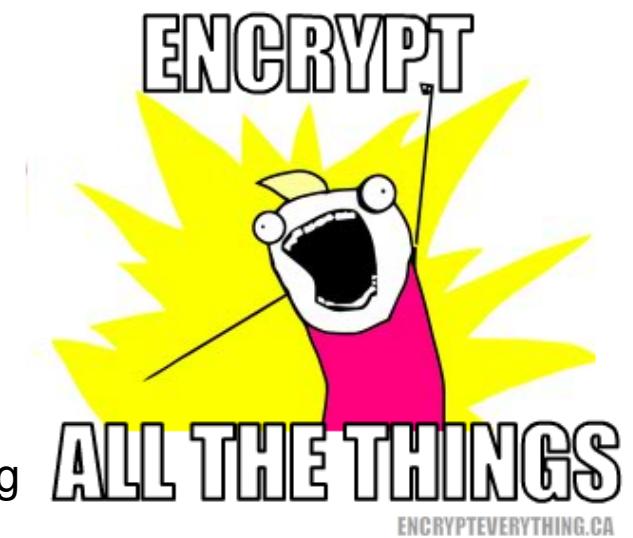
PROSA Superhelteseminar

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

<http://www.solidonetworks.com>

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, and separate for home banking apps?
- Multiple laptops? One for private data, one for work?
- Think of the data you produce, why do people take naked pictures and SnapChat them?
- Use pseudonyms and aliases, do not use your real name everywhere
- Enable encryption: **IMAPS POP3S HTTPS TOR OpenPGP VPN SSL/TLS**





Don't Panic!

KI 17:30-19:30 - med pause

Mindre enetale, mere foredrag 2.0 med sociale medier, informationsdeling og interaktion

Send gerne spørgsmål senere

PS er her nogle timer efter foredraget til spørgsmål og snak

The current situation



Internet security sucks

Personal computers like laptops suck at security

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

We depend on cloud services and underfunded infrastructure - OpenSSL

We depend on others and the whole internet - DDoS

Goals: Internet Ninjas



Superhelte er ninajer

Kender internet, teknologierne og mulighederne

Rettidig omhu og defense in depth

Konsekvenserne ved dårlig sikkerhed

The 5th Wave By Rich Tennant



"Don't be silly – of course my passwords are safe. I keep them written on my window, but then I pull the shade if anyone walks in the room."

Opbevaring af passwords



Think security always appropriate paranoia

Follow news about software security

Support communities, join and learn



Hackerværktøjer er også til dig!



- Hackers work all the time to break stuff, Use hackertools:
- Nmap, Nping <http://nmap.org>
- Wireshark - <http://www.wireshark.org/>
- Aircrack-ng <http://www.aircrack-ng.org/>
- Metasploit Framework <http://www.metasploit.com/>
- Burpsuite <http://portswigger.net/burp/>
- Skipfish <http://code.google.com/p/skipfish/>
- Kali Linux <http://www.kali.org>

Most popular hacker tools <http://sectools.org/>

Kali Linux the new backtrack

The most advanced penetration testing distribution, ever.

From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system. With all this buzz, you might be asking yourself: - [What's new?](#)



KALI LINUX
"the quieter you become, the more you are able to hear"

**PENETRATION TESTING,
REDEFINED.**

A Project By Offensive Security

BackTrack <http://www.backtrack-linux.org>

Kali <http://www.kali.org/>

100.000s of videos on youtube: "kali hack" 60.000, "backtrack hack" 125.000



frednecksec Matt Franz  by kramse

Painful interview with a junior candidate today "wanting to get into security" yet who didn't build their own network @ home or run Linux!!

1 Mar

Skal du igang med sikkerhed?

Installer et netværk, evt. bare en VMware, Virtualbox, Parallels, Xen, GNS3, ...

Brug BackTrack, se evt. youtube videoer om programmerne

Quote fra Jurassic Park <http://www.youtube.com/watch?v=dFULAQZB9Ng>

What is it?

The Metasploit Framework is a development platform for creating security tools and exploits. The framework is used by network security professionals to perform penetration tests, system administrators to verify patch installations, product vendors to perform regression testing, and security researchers world-wide. The framework is written in the Ruby programming language and includes components written in C and assembler.

<http://www.metasploit.com/>

Armitage GUI fast and easy hacking for Metasploit

<http://www.fastandeasyhacking.com/>

Kursus Metasploit Unleashed

http://www.offensive-security.com/metasploit-unleashed/Main_Page

Bog: Metasploit: The Penetration Tester's Guide, No Starch Press

ISBN-10: 159327288X

I 1993 skrev Dan Farmer og Wietse Venema artiklen
Improving the Security of Your Site by Breaking Into it

I 1995 udgav de softwarepakken SATAN
Security Administrator Tool for Analyzing Networks

We realize that SATAN is a two-edged sword - like many tools, it can be used for good and for evil purposes. We also realize that intruders (including wannabees) have much more capable (read intrusive) tools than offered with SATAN.

Se <http://sectools.org> og <http://www.packetstormsecurity.org/>

Kilde: <http://www.fish2.com/security/admin-guide-to-cracking.html>

Heartbleed hacking

```
06b0: 2D 63 61 63 68 65 0D 0A 43 61 63 68 65 2D 43 6F -cache..Cache-Co
06c0: 6E 74 72 6F 6C 3A 20 6E 6F 2D 63 61 63 68 65 0D ntrol: no-cache.
06d0: 0A 0D 0A 61 63 74 69 6F 6E 3D 67 63 5F 69 6E 73 ...action=gc_ins
06e0: 65 72 74 5F 6F 72 64 65 72 26 62 69 6C 6C 6E 6F ert_order&billno
06f0: 3D 50 5A 4B 31 31 30 31 26 70 61 79 6D 65 6E 74 =PZK1101&payment
0700: 5F 69 64 3D 31 26 63 61 72 64 5F 6E 75 6D 62 65 _id=1&card_numbe
0710: XX r=4060xxxx413xxx
0720: 39 36 26 63 61 72 64 5F 65 78 70 5F 6D 6F 6E 74 96&card_exp_mont
0730: 68 3D 30 32 26 63 61 72 64 5F 65 78 70 5F 79 65 h=02&card_exp_ye
0740: 61 72 3D 31 37 26 63 61 72 64 5F 63 76 6E 3D 31 ar=17&card_cvn=1
0750: 30 39 F8 6C 1B E5 72 CA 61 4D 06 4E B3 54 BC DA 09.l...r.aM.N.T..
```

- Obtained using Heartbleed proof of concepts - Gave full credit card details
- "can XXX be exploited" - yes, clearly! PoCs ARE needed without PoCs even Akamai wouldn't have repaired completely!
- The internet was ALMOST fooled into thinking getting private keys from Heartbleed was not possible - scary indeed.

Nothing more about HB in this presentation - we have better things to discuss

Attack overview

 LIFE IS FOR SHARING.

OVERVIEW INFO IMPRINT

Allianz für Cyber-Sicherheit 

English German

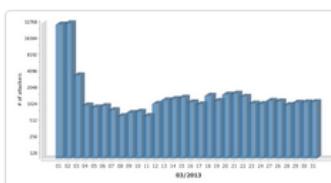
Overview of current cyber attacks (logged by 97 Sensors)



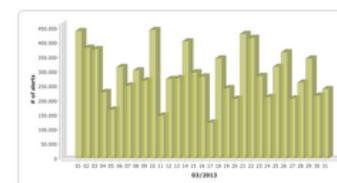
Live-Ticker

Date	Source	Attack on	Parameter
2013-04-09 09:29:38	unbekannt		Kippo.SSH_Connect.Fail
2013-04-09 09:29:40	unbekannt		Kippo.SSH_Connect.Fail
2013-04-09 09:29:40	USA	Web site	/administra%20%3Cbr%20%3E%sa=U&a
2013-04-09 09:29:40	China	Console/Shell	Kippo.SSH_Connect.Fail
2013-04-09 09:29:20	unbekannt		Kippo.SSH_Connect.Fail

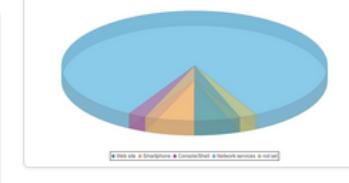
Overall sum of attackers per Day (Last Month)



Overall sum of attacks per Day (Last Month)



Distribution of Attack Targets (Last Month)



Top 15 of Source Countries (Last month)

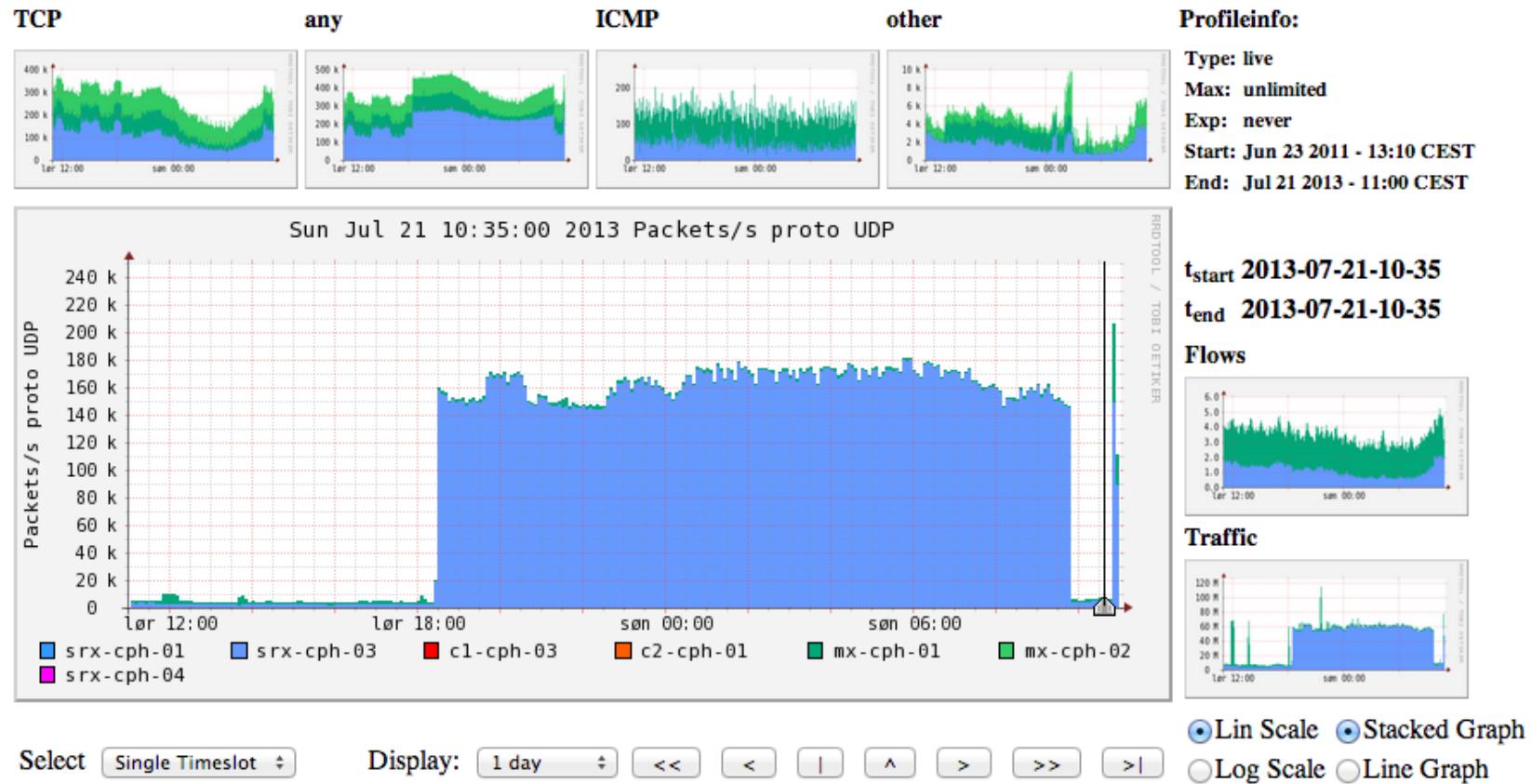
Source of Attack	Number of Attacks
Russian Federation	2,446,168
Germany	1,308,617
Taiwan, Province of China	536,034
United States	449,853
Australia	378,792
India	358,114
Ukraine	250,213
Hungary	237,607
Brazil	218,265
China	197,152
Italy	194,102
France	184,073
Argentina	182,166
Japan	151,861
Venezuela, Bolivarian Republic of	127,862

Top 5 of Attack Types (Last month)

Description	Number of Attacks
Attack on SMB protocol	31,077,005
Attack on Netbios protocol	1,108,033
Attack on Port 5353	921,115
Attack on SSH protocol	919,145
Attack on Port 33434	687,446

<http://www.sicherheitstacho.eu/?lang=en>

Profile: live



An extra 100k packets per second from this netflow source (source is a router)

Alert (TA14-017A) UDP-based Amplification Attacks



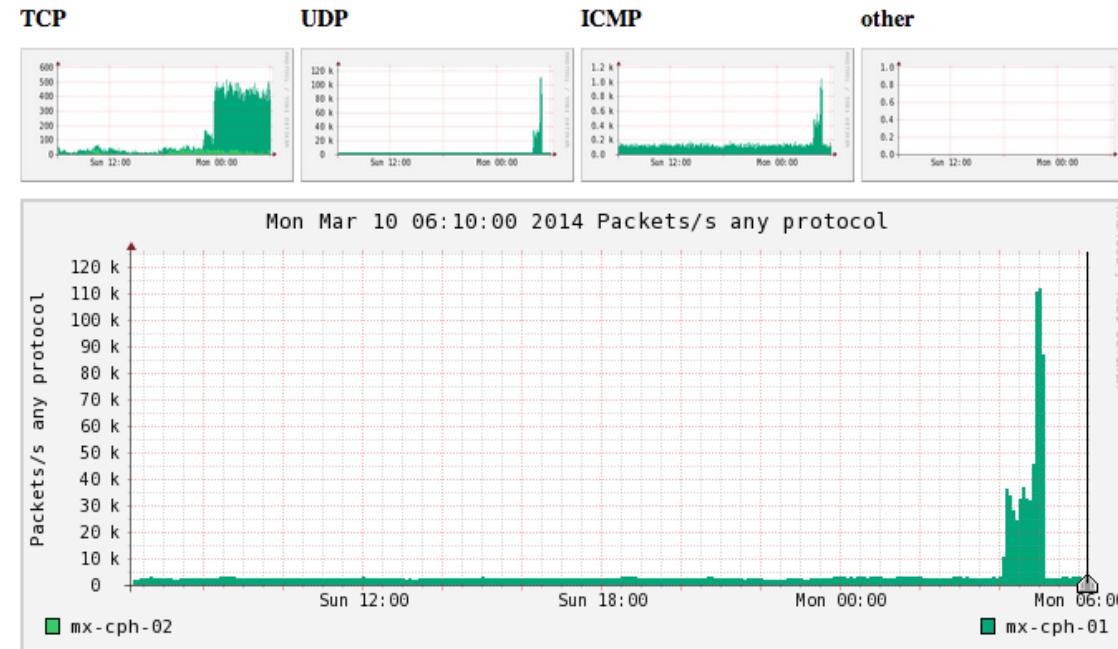
Protocol	Bandwidth	Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [1]	
NTP	556.9	see: TA14-013A [2]	
SNMPv2	6.3	GetBulk request	
NetBIOS	3.8	Name resolution	
SSDP	30.8	SEARCH request	
CharGEN	358.8	Character generation request	
QOTD	140.3	Quote request	
BitTorrent	3.8	File search	
Kad	16.3	Peer list exchange	
Quake Network Protocol	63.9	Server info exchange	
Steam Protocol	5.5	Server info exchange	

Source: US-CERT

<http://www.us-cert.gov/ncas/alerts/TA14-017A>

Detecting DDoS

Profile: DDoS



We created a DDoS profile with the common types.

We can ask RDDtools about max, average etc.

```
rrdtool graph x -s -24h DEF:v=DDoS/mx-cph-01.rrd:packets:MAX VDEF:vm=v,MAXIMUM PRINT:vm:%.lf
```

But DNS is bad! DNS Amplification?!

This is the official homepage for PacketQ, a simple tool to make SQL-queries against PCAP-files, making packet analysis and building statistics simple and quick. PacketQ was previously known as DNS2db but was renamed in 2011 when it was rebuilt and could handle protocols other than DNS among other things.

Look how easy it's to count DNS-packets in a PCAP-file.

```
# packetq -s "select count(*) as count_dns from dns" packets.pcap
[ { "table_name": "result",
    "head": [
      { "name": "count_dns", "type": "int" } ],
      "data": [ [95501] ] }
```

<https://github.com/dotse/packetq/wiki>

Using PacketQ

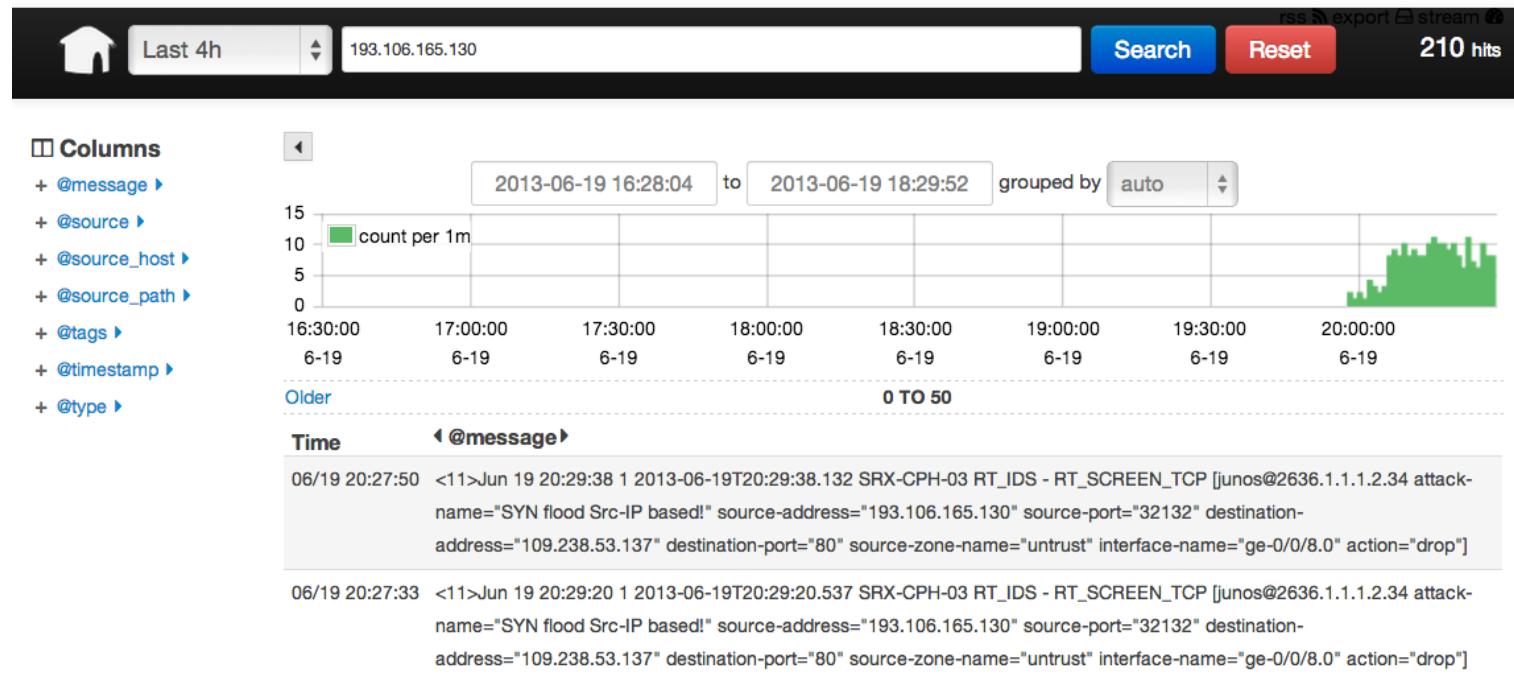
Let's have a practical look at how PacketQ works by trying to figure out what kind of DNS ANY queries are being sent towards our name-server.

DNS ANY traffic is currently commonly abused for DNS amplification attacks (See Blog post "[DDoS-Angriffe durch Reflektierende DNS-Amplifikation vermeiden](#)" in German). The first thing I want to know is what are the IP addresses of the victims of this potential DNS amplification attack:

```
packetq -t -s "select src_addr,count(*) as count from dns where qtype=255 group  
by src_addr order by count desc limit 3" lolo.20130118.070000.000179  
"src_addr" , "count"  
"216.245.221.243" , 933825  
"85.126.233.70" , 16802  
"80.74.130.55" , 91
```

Discussion: bridging the gaps between Devops and Security? Good thing, easy?

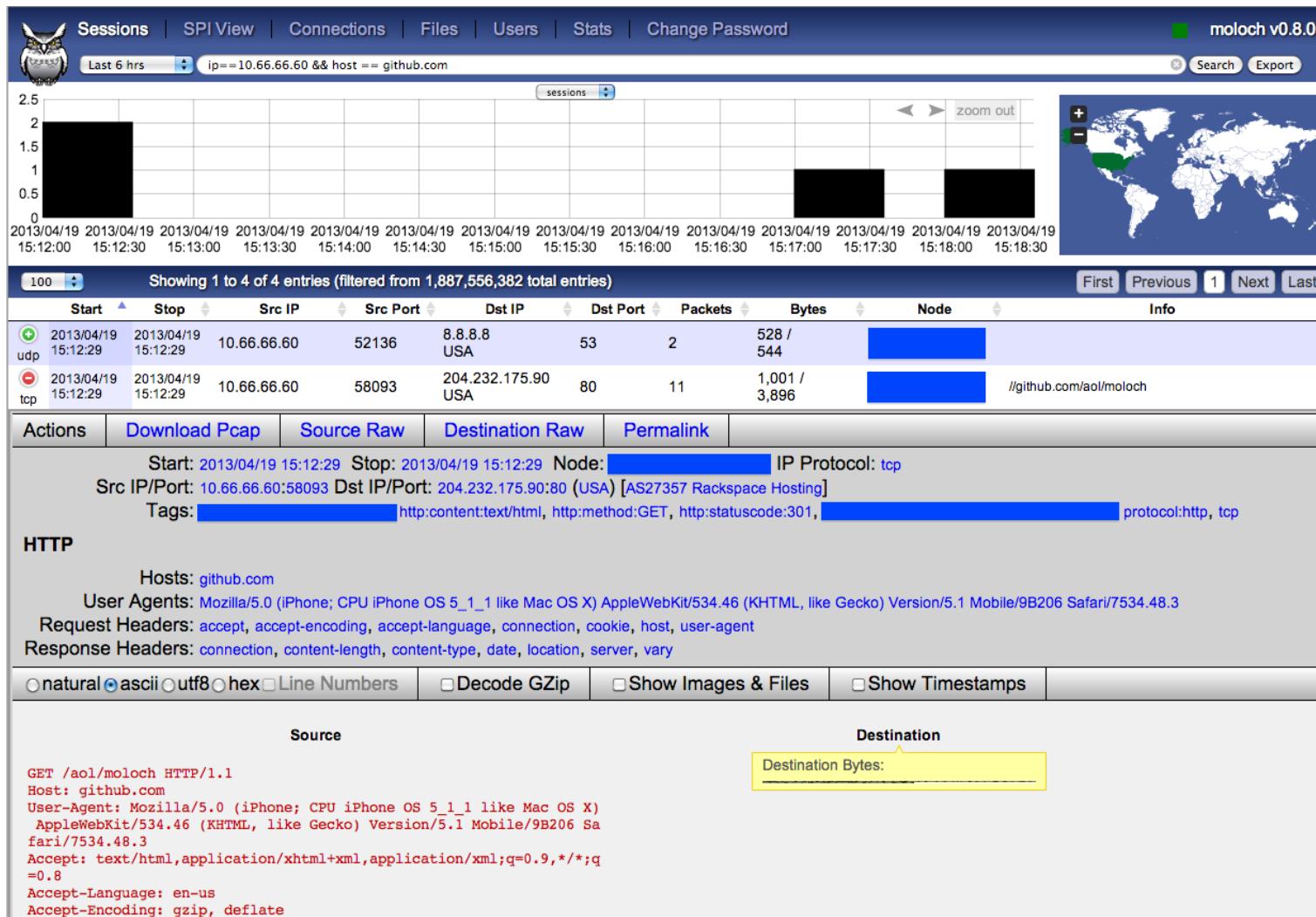
<http://securityblog.switch.ch/2013/01/22/using-packetq/>



Moloch <https://github.com/aol/moloch>

DSC and PacketQ <https://github.com/dotse/packetq/wiki>

Logstash, Elasticsearch and Kibana



Picture from <https://github.com/aol/moloch>

Suricata with Dashboards



Picture from Twitter

<https://twitter.com/nullthreat/status/445969209840128000>

New link March 2014: 10Gbits

<http://pevma.blogspot.se/2014/03/suricata-prepearing-10gbps-network.html>

<http://suricata-ids.org/2014/03/25/suricata-2-0-available/>

We need devops skillz in security

automate, security is also big data

integrate tools, transfer, sort, search, pattern matching, statistics, ...

tools, languages, databases, protocols, data formats

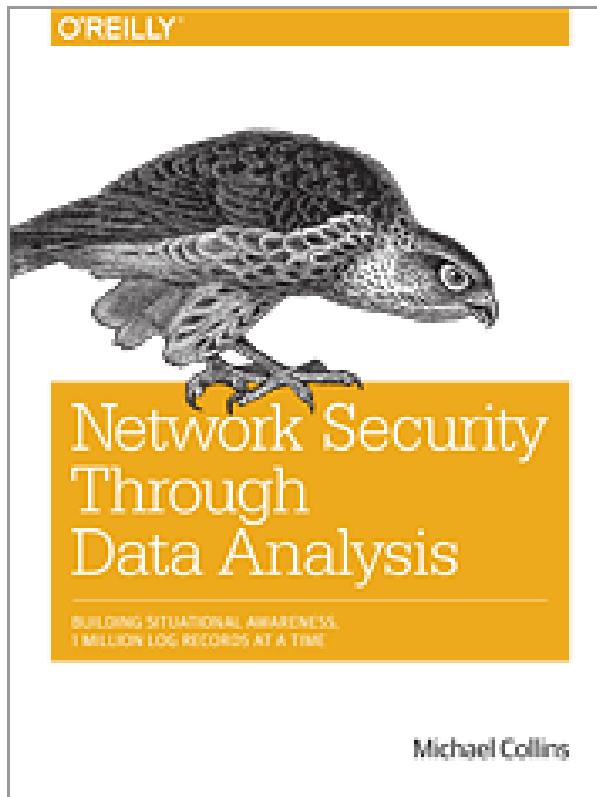
Example introductions:

- Seven languages/database/web frameworks in Seven Weeks
- Elasticsearch the definitive guide

<http://www.elasticsearch.org/guide/en/elasticsearch/guide/current/index.html>

- <http://www.elasticsearch.org/overview/kibana/>
- <http://www.elasticsearch.org/overview/logstash/>

We are all Devops now, even security people!



Low page count, but high value! Recommended.

Network Security Through Data Analysis: Building Situational Awareness
By Michael Collins
Publisher: O'Reilly Media Released: February 2014 Pages: 348



The Bro Network Security Monitor

Bro is a powerful network analysis framework that is much different from the typical IDS you may know.

While focusing on network security monitoring, Bro provides a comprehensive platform for more general network traffic analysis as well. Well grounded in more than 15 years of research, Bro has successfully bridged the traditional gap between academia and operations since its inception.

<http://www.bro.org/>

The key point that helped me understand was the explanation that Bro is a domain-specific language for networking applications and that Bro-IDS (<http://bro-ids.org/>) is an application written with Bro.

Why I think you should try Bro

<https://isc.sans.edu/diary.html?storyid=15259>

```
global dns_A_reply_count=0;
global dns_AAAA_reply_count=0;

...
event dns_A_reply(c: connection, msg: dns_msg, ans: dns_answer, a: addr)
{
++dns_A_reply_count;
}

event dns_AAAA_reply(c: connection, msg: dns_msg, ans: dns_answer, a: addr)
{
++dns_AAAA_reply_count;
}
```

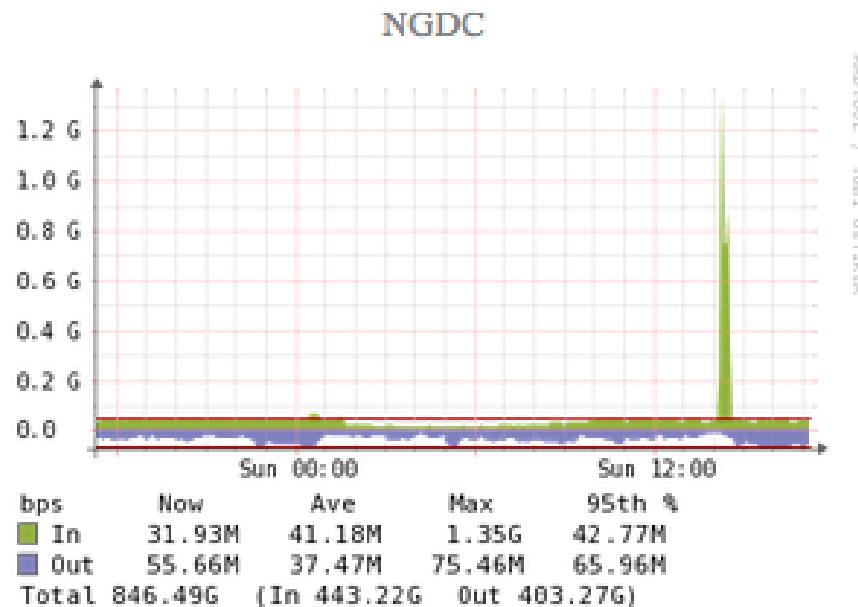
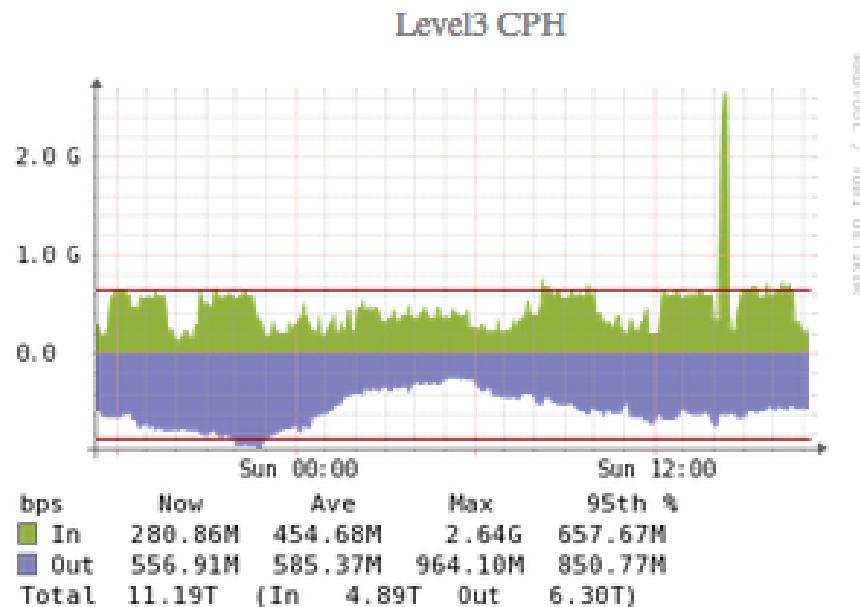
source: dns-fire-count.bro from

<https://github.com/LiamRandall/bro-scripts/tree/master/fire-scripts>



- Security Onion is a Linux distro for IDS, NSM, and log management
- securityonion.blogspot.dk
- <http://blog.securityonion.net/p/securityonion.html>

Problem: DDoS traffic before filtering



Problem: We receive unauthenticated chaotic traffic

Only two links shown, at least 3Gbit incoming for this single IP

Goal: DDoS traffic after filtering



Solution: Discard early, discard on edge, reduce noise

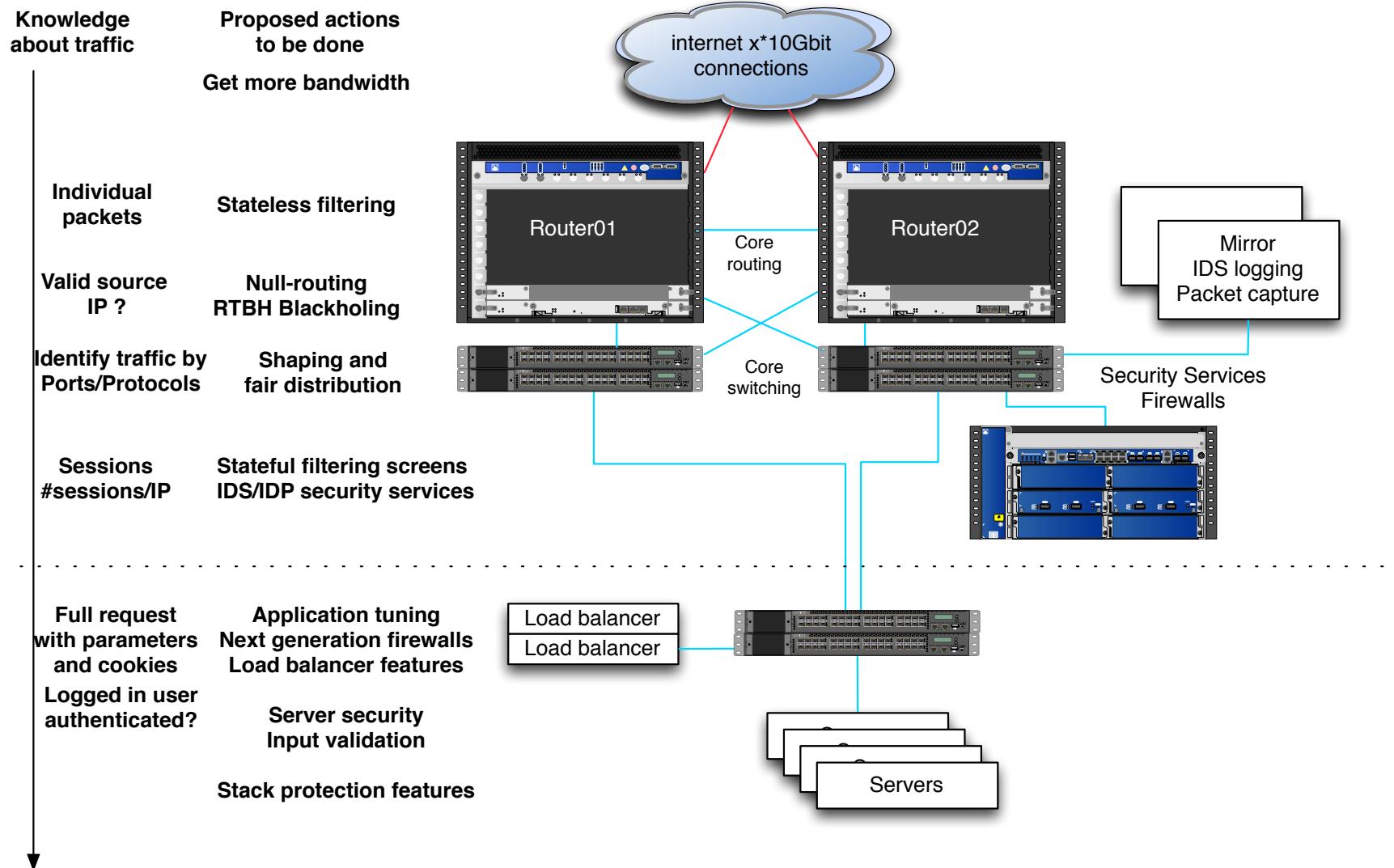
Only use CPU resources for potentially real traffic

Link toward server (next level firewall actually) about 350Mbit outgoing

Drinking from a water hose, eating an elephant

Reduce problems until manageable, divide and conquer

Defense in depth - multiple layers of security



Stateless firewall filter limit protocols

```
term limit-icmp {  
    from {  
        protocol icmp;  
    }  
    then {  
        policer ICMP-100M;  
        accept;  
    }  
}  
term limit-udp {  
    from {  
        protocol udp;  
    }  
    then {  
        policer UDP-1000M;  
        accept;  
    }  
}
```

Routers also have extensive Class-of-Service (CoS) tools today

Strict filtering for some servers, still stateless!

```
term some-server-allow {  
    from {  
        destination-address {  
            109.238.xx.0/xx;  
        }  
        protocol tcp;  
        destination-port [ 80 443 ];  
    }  
    then accept;  
}  
term some-server-block-unneeded {  
    from {  
        destination-address {  
            109.238.xx.0/xx;  
        }  
        protocol-except icmp;  
    }  
    then {  
        count some-server-block;  
        discard;  
    }  
}
```

Wut - no UDP, yes UDP service is not used on these servers

Summary: Goal of protection mechanisms



DDoS attacks increase in size

+100Gb happens regularly

Even 200Gb is becoming more common

No vendor can deliver a single device with 100%

Slice the attacks - Divide and conquer

Use the available features and resources in combination - optimize your infrastructure

Allowed traffic to next layer

Basic filtering and routers can eliminate a lot

Characteristics after employing the techniques:

Known bad sources removed

Maximum 100Mbit ICMP

Maximum 1000Mbit UDP

Only port 80/tcp and 443/tcp to some range

LESS traffic to consider on firewall/next device

SC Magazine > News > Arbor Networks observes several large NTP-based DDoS attacks



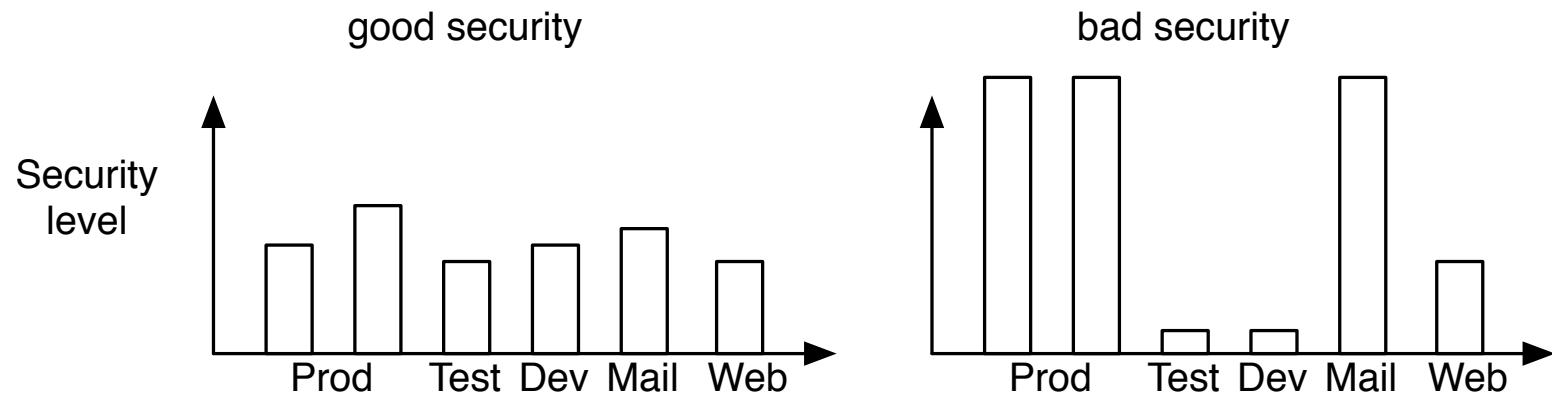
Adam Greenberg, Reporter

February 14, 2014

Arbor Networks observes several large NTP-based DDoS attacks

Arbor Networks [announced on Friday](#) that it observed several large NTP-based distributed denial-of-service (DDoS) attacks this week, including one on [Monday](#) that peaked at 325 gigabytes per second.

- Several big players you need to research before needing them!
- Arbor Networks sells software solutions for carriers
<http://www.arbornetworks.com/>
- Prolexic sells DDoS services, DNS and BGP based
<http://www.prolexic.com/>
- CloudFlare proxy based
<http://www.cloudflare.com/>



Det er bedre at have et ensartet niveau

Hvor rammer angreb hvis du har Fort Knox et sted og kaos andre steder

Hackere vælger ikke med vilje den sværreste vej ind

Part II

Hvad gør I for at undgå problemer som de her nævnte? - kan man gøre mere?

Man bør være klar over hvilke teknologier man bruger

Standardiser på et mindre antal produkter, biblioteker, sprog

Regler og procedurer skal hele tiden opdateres:

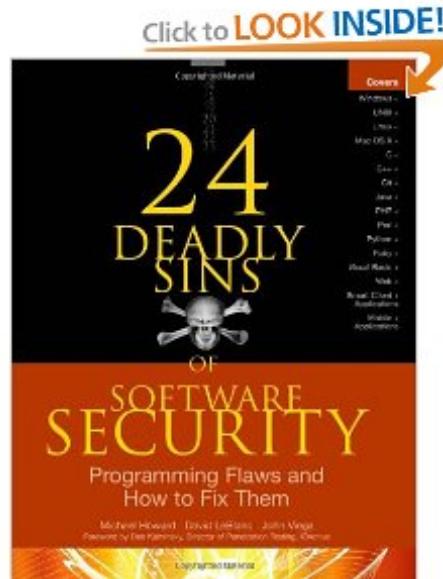
- Kvalitetssikring
- Retningslinier for tilladte tags
- Retningslinier for brug af SQL

Ved at fokusere på antallet af produkter kan man måske indskrænke mulighederne for fejl, høj kvalitet er ofte mere sikkert

nye produkter kan være farlige til man lærer dem at kende!

- Hvis der ikke findes retningslinier for udvikling så etabler disse
- eksempel:
javascript må gerne benyttes til at validere forms for at give hurtig feedback til brugeren
- serveren der modtager input fra brugeren validerer alle data sikkerhedsmæssigt
- Retningslinierne er medvirkende til at foretage en afbalanceret investering i sikkerheden
- undgå dyre hovsa løsninger
- undgå huller i sikkerheden, ens niveau
- Der findes vejledninger til både gamle og nye sprog/systemer,
eks Ruby On Rails Security Guide <http://guides.rubyonrails.org/security.html>

Deadly sins bogen



24 Deadly Sins of Software Security Michael Howard, David LeBlanc, John Viega 2. udgave, første hed 19 Deadly Sins



The OWASP Top Ten provides a minimum standard for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are.

The Open Web Application Security Project (OWASP)

OWASP har gennem flere år udgivet en liste over de 10 vigtigste sikkerhedsproblemer for webapplikationer

<http://www.owasp.org>

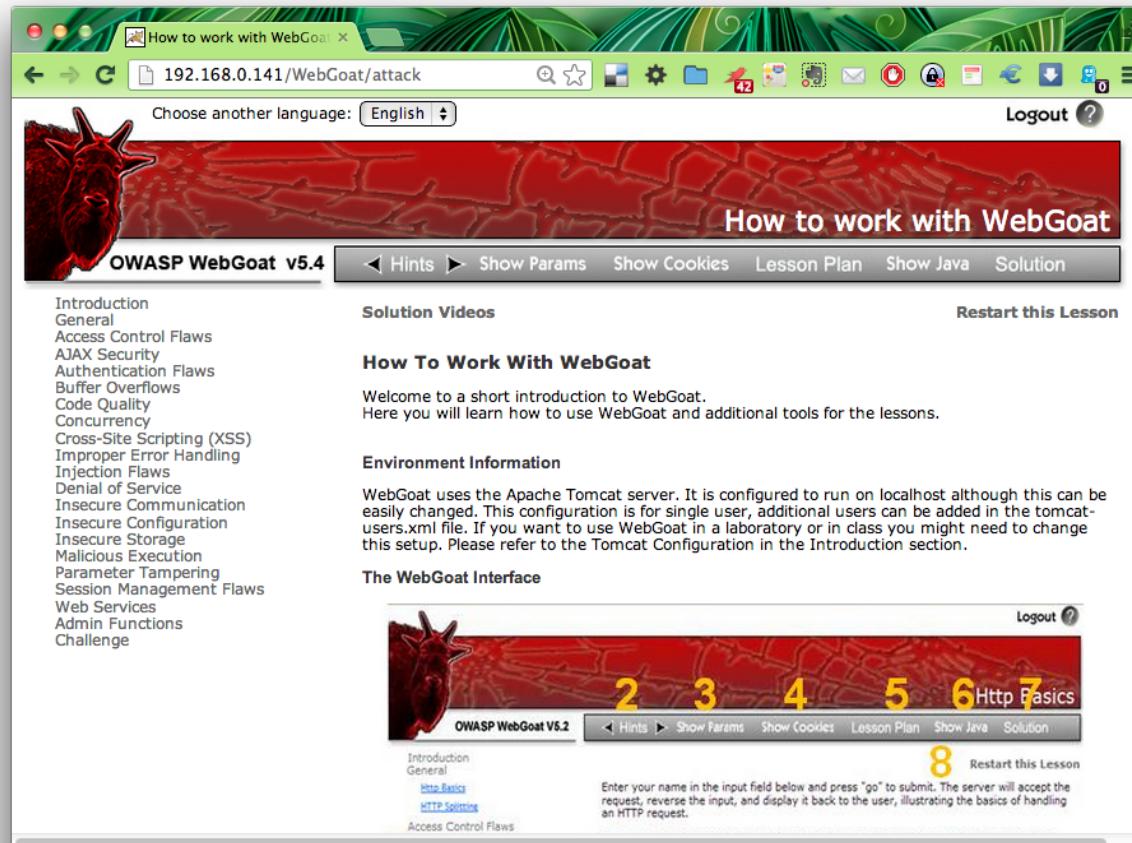


WebGoat fra OWASP, <http://www.owasp.org>

Træningsmiljø til webhacking

Downloads som Zipfil og kan afvikles direkte på en Windows laptop

<https://www.owasp.org>



Perfect for learning web hacking/protection

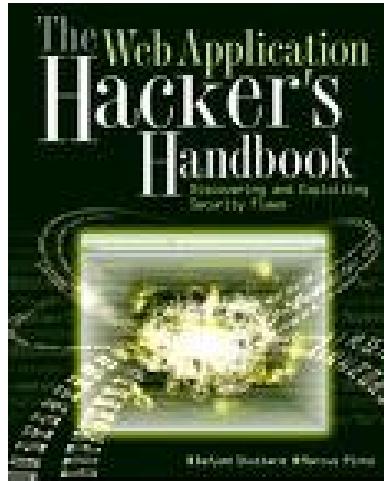
Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.

Burp suite indeholder både proxy, spider, scanner og andre værktøjer i samme pakke -
NB: EUR 249 per user per year.

<http://portswigger.net/burp/>

More Web application hacking



The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws
Dafydd Stuttard, Marcus Pinto, Wiley 2007 ISBN: 978-0470170779

Protect yourself: Why think of security?



Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world. A Cypherpunk's Manifesto by Eric Hughes, 1993

Copied from <https://cryptoparty.org/wiki/CryptoParty>

- Criminals sell your credit card information and identity theft
- Trade infected computers like a commodity
- Governments write laws that allows them to introduce back-doors - and use these
- Governments do blanket surveillance of their population
- Governments implement censorship, threaten citizens and journalist
- Governments will introduce back-doors in products we use
- Danish police and TAX authorities have the legal means, see *Rockerloven*

You are not paranoid when there are people actively attacking you!



Turkey: Erdogan bans Twitter

 **Mashable** 
@mashable

Whoa: 1.2 million tweets sent in Turkey,
despite ban on.mash.to/1kQ7ijw
#OccupyTwitter #direntwitter
pic.twitter.com/opvuEeEh7f

 View translation

 Reply  Retweet  Favorite  More



RETWEETS 1,311 FAVORITES 379



The Net interprets censorship as damage and routes around it.

John Gilmore

John Gilmore is an American computer science innovator, Libertarian, Internet activist, and one of the founders of [Electronic Frontier Foundation](#). He created the alt.* hierarchy in [Usenet](#) and is a major contributor to the [GNU](#) project.



This [scientist](#) article is a [stub](#). You can help Wikiquote by [expanding it](#).

Sourced [\[edit\]](#)

- **The Net interprets censorship as damage and routes around it.**
 - As quoted in [TIME magazine \(6 December 1993\)](#)
 - Unsourced variant:
The Net treats censorship as a defect and routes around it.
- How many of you have broken no laws this month?
 - As quoted in a [speech](#) to the First Conference on Computers, Freedom, and Privacy in 1991
- If you're watching everybody, you're watching nobody.
 - As quoted in [Subject: \[IP\] John Gilmore on government trustworthiness and spy gear](#)
- **When the X500 revolution comes, your name will be lined against the wall and shot.**
 - As quoted in Peter Gutmann's [X509 style guide](#)



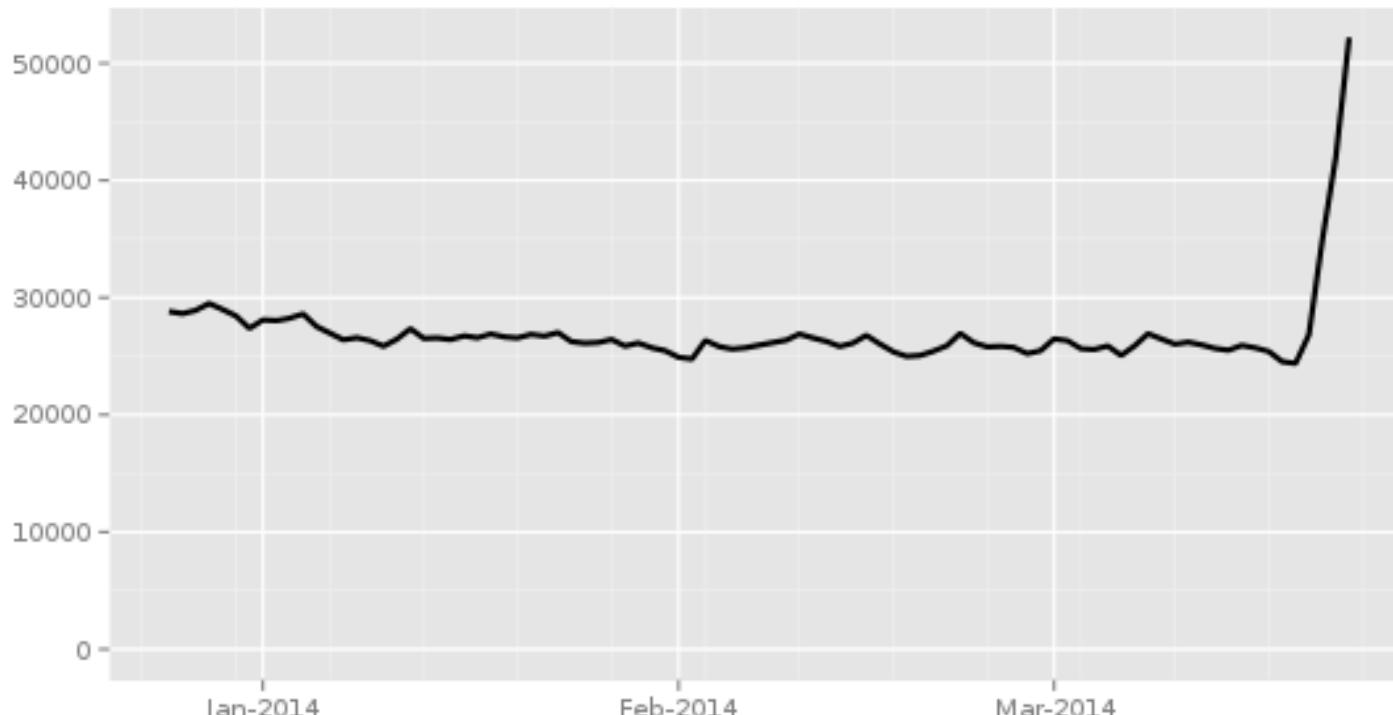
The Net interprets censorship as
damage and routes around it. 

http://en.wikiquote.org/wiki/John_Gilmore

[http://en.wikipedia.org/wiki/John_Gilmore_\(activist\)](http://en.wikipedia.org/wiki/John_Gilmore_(activist))

Directly connection Tor Users from Turkey

Directly connecting users from Turkey

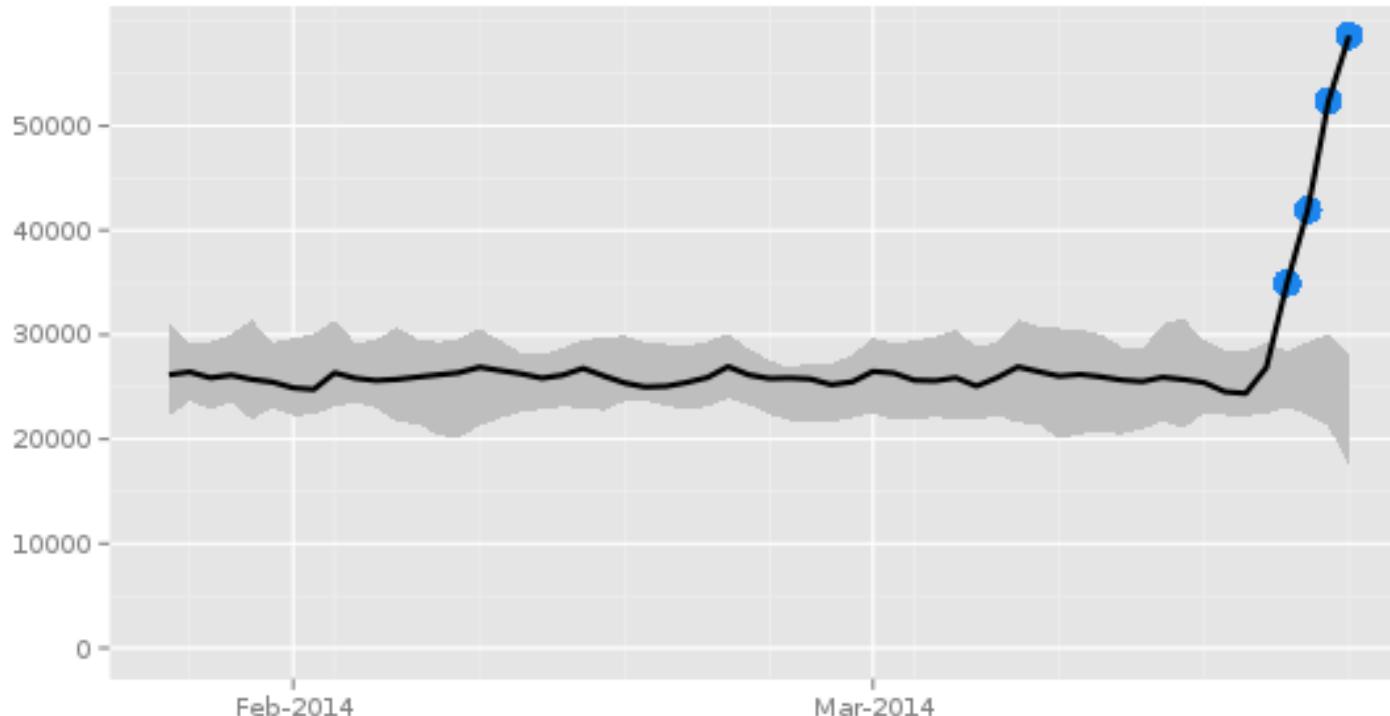


The Tor Project - <https://metrics.torproject.org/>

Image from https://metrics.torproject.org
via <https://twitter.com/runasand>

Directly connection Tor Users from Turkey +10.000

Directly connecting users from Turkey



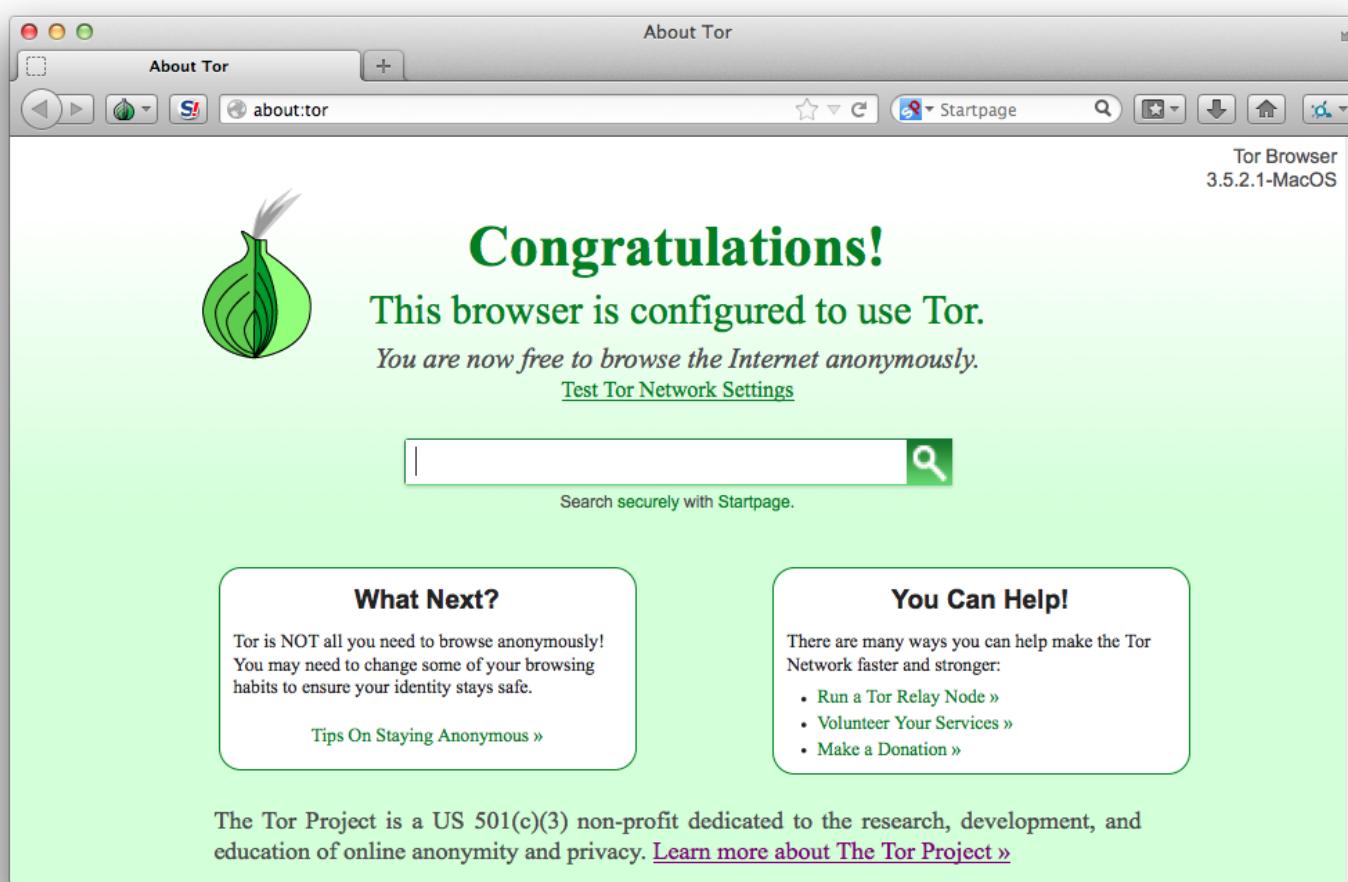
The Tor Project - <https://metrics.torproject.org/>

Image from <https://metrics.torproject.org> via <https://twitter.com/ioc32/status/448791582423408640>



Der findes diverse tools til Tor, Torbutton on/off knap til Firefox osv.

Det anbefales at bruge Torbrowser bundles fra <https://www.torproject.org/>



Mere anonym browser - Firefox in disguise

Whonix Anonymous Operating System



The red arrows → indicate that malicious or misbehaving applications can't break out of the Whonix-Workstation.

All network connections → are forced to go through Whonix-Gateway, where they are torified and routed to the Internet.

Whonix is an operating system focused on anonymity, privacy and security. It's based on the Tor anonymity network[5], Debian GNU/Linux[6] and security by isolation. DNS leaks are impossible, and not even malware with root privileges can find out the user's real IP. <https://www.whonix.org/>

Torbrowser er godt, Whonix giver lidt ekstra sikkerhed

Multiple browsers



Firefox



Allow active content to run
only from sites you trust



chrome



noscripts

Take control of the javascript, iframes, and plugins



TorProject.org



- Strict Security settings in the general browser, Firefox or Chrome?
- More lax security settings for "trusted sites" - like home banking
- Security plugins like HTTPS Everywhere and NoScripts for generic browsing



HTTPS Everywhere is a Firefox extension produced as a collaboration between The Tor Project and the Electronic Frontier Foundation. It encrypts your communications with a number of major websites.

<http://www.eff.org/https-everywhere>

Secure your mobile



Orbot:
Proxy With Tor



Orweb:
Private Web Browser



ChatSecure:
Private and Secure Messaging



ObscuraCam:
The Privacy Camera



Ostel:
Encrypted Phone Calls



CSipSimple:
Encrypted Voice Over IP (VOIP)



K-9 and APG:
Encrypted E-mail



KeySync:
Syncing Trusted Identities



TextSecure:
Short Messaging Service (SMS)



Pixelknot:
Hidden Messages

Dont forget your mobile platforms <https://guardianproject.info/>





Lots of DNSSEC tools, I recommend DNSSEC-trigger a local name server for your laptop

- DNSSEC Validator for firefox
<https://addons.mozilla.org/en-us/firefox/addon/dnssec-validator/>
- OARC tools <https://www.dns-oarc.net/oarc/services/odvr>
- <http://www.nlnetlabs.nl/projects/dnssec-trigger/>

Følg med Twitter news



The screenshot shows the Twitter profile for the account @safety, which is verified. The profile bio reads: "Twitter's Trust and Safety Updates! http://help.twitter.com/forums/10711/entries/76036". Below the bio, there is a green "Following" button, a reply icon, and a direct message icon. A text input field says "Tweet to @safety". Below these are tabs for "Tweets", "Favorites", "Following", "Followers", and "Lists". Three tweets from the account are listed:

- safety Safety** Also, we will never send you an email saying that you've been suspended for "tweeting too much." Those emails are fake & not from us.
26 Sep
- safety Safety** We will never send you emails requiring you to "complete offers" in order to unsuspend your account. That's spam, not us.
26 Sep
- safety Safety** Warn your friends if they sent you a DM saying "When I found this about you" with a link - they've been phished. bit.ly/accountamiss
21 Sep

Twitter has become an important new resource for lots of stuff

Twitter has replaced RSS for me

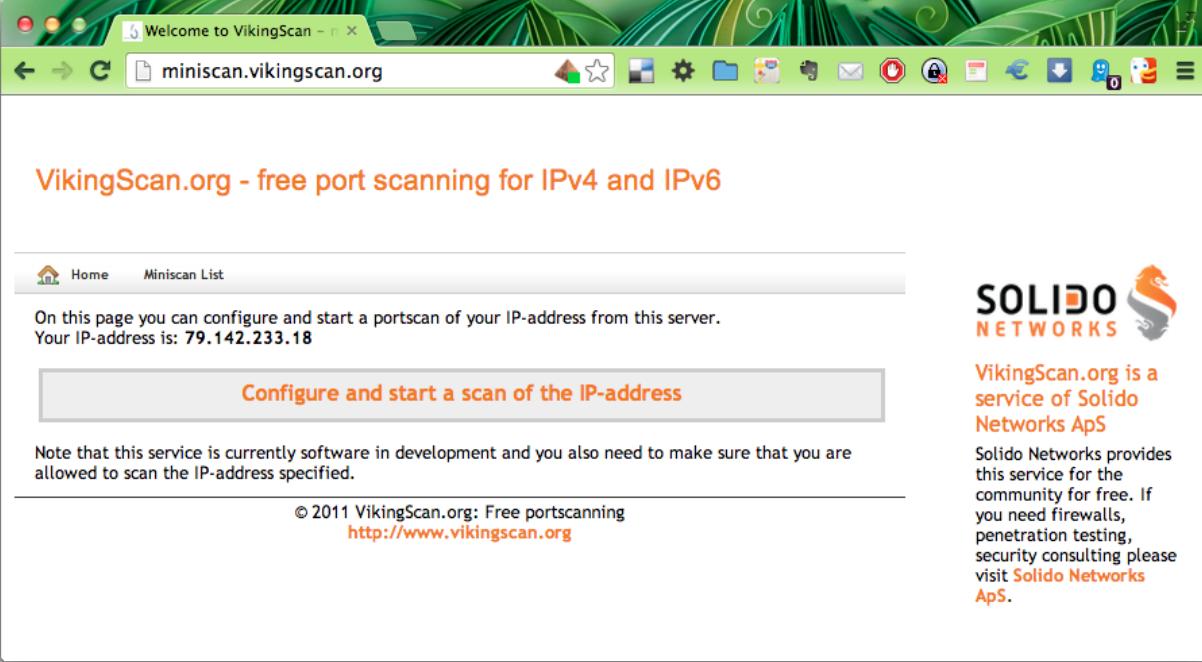
Be careful - spørgsmål?



Hey, Lets be careful out there!

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

Billede: Michael Conrad <http://www.hillstreetblues.tv/>



The screenshot shows a web browser window titled "Welcome to VikingScan". The address bar displays "miniscan.vikingscan.org". The main content area is titled "VikingScan.org - free port scanning for IPv4 and IPv6". It features a navigation bar with "Home" and "Miniscan List" links. Below the navigation, a message states: "On this page you can configure and start a portscan of your IP-address from this server. Your IP-address is: 79.142.233.18". A prominent button labeled "Configure and start a scan of the IP-address" is centered. A note below the button says: "Note that this service is currently software in development and you also need to make sure that you are allowed to scan the IP-address specified." At the bottom, copyright information reads: "© 2011 VikingScan.org: Free portscanning <http://www.vikingscan.org>". To the right of the main content, there is a sidebar with the Solido Networks logo and text: "VikingScan.org is a service of Solido Networks ApS. Solido Networks provides this service for the community for free. If you need firewalls, penetration testing, security consulting please visit [Solido Networks ApS](#)".