Welcome to

Tendenser i sikkerhed

September 2015

Henrik Lund Kramshøj hlk@zencurity.dk

Slides are available as PDF, kramshoej@Github

Based on version from March, with stuff added

Goals of today

Update on trends in information security and internet security

Offer input to what things to look into

I will try to limit myself to things from 2014-2015

Hodge-podge of security related things - inspiration

Please give feedback and join me in discussions, dialogue ☺

Plan for today

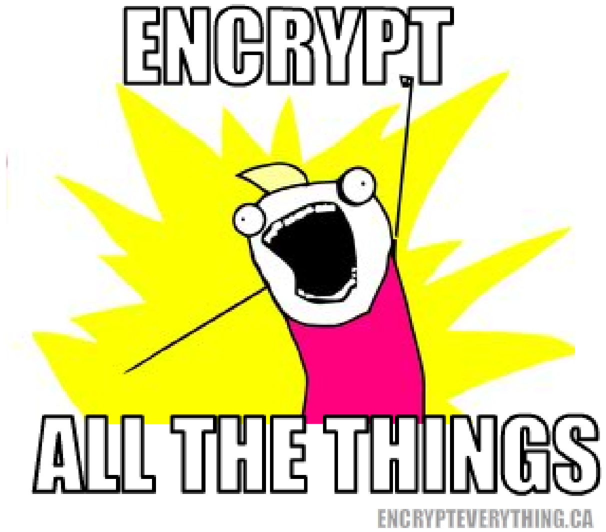
Kl 17:00-21:00 and some breaks

Less presentation, more talk

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

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 `https://torproject.org/`

Security Breaches: Ashley Madison

When hackers swiped an estimated 36 million accounts associated with Ashley-Madison.com, a site which helps married people cheat on their partners, there was a rush to find out what had been stolen.

- Ashley Madison, inkl password hacking
- Popular passwords 123456, ,password ,12345 ,qwerty ,12345678,football
- Also hacking kills? Suicides and family break-ups?
- accidental outing of gays/ Gay persecution, death?

Source:

`http://www.zdnet.com/article/these-are-the-worst-passwords-from-the-ashley-madison-hack/`

Security Breaches: Top 20 Ashley Madison Passwords

Previously thought to be impossible thanks to the slow pace and high stress it puts on a computer's CPU, the CynoSure Prime group managed to crack over 11 million passwords from the total of 36 million, mainly due to a programming error in how the passwords were hashed.

- Main passwords hashed with slow (good) bcrypt algoritm, but hackers found tokens hashed with MD5
  `http://cynosureprime.blogspot.dk/2015/09/how-we-cracked-millions-of-ashley.`
  `html`
- Also check out Twitter Mark Burnett @m8urnett and his 10 million password dump
  `http://wpengine.com/unmasked/`
- Systems exist which can try 135 billion MD5 hashes PER SECOND with 8 GPUs

Source: Catalin Cimpanu, Softpedia 15 September 2015

`http://news.softpedia.com/news/top-20-ashely-madison-passwords-491799.shtml`

Ransomware web ransomware

Tre Randomware familier rammer Danmark Ransomware, som rammer Danmark er groft fordelt i tre malware familier: Cryptowall, CTB-Locker og FileCoder. De spredes via to centrale metoder: spamkampagner med vedhæftede filer og ved brug af ”drive-by”angreb.

Source: https://www.csis.dk/da/csis/news/4676/

Andre kilder:

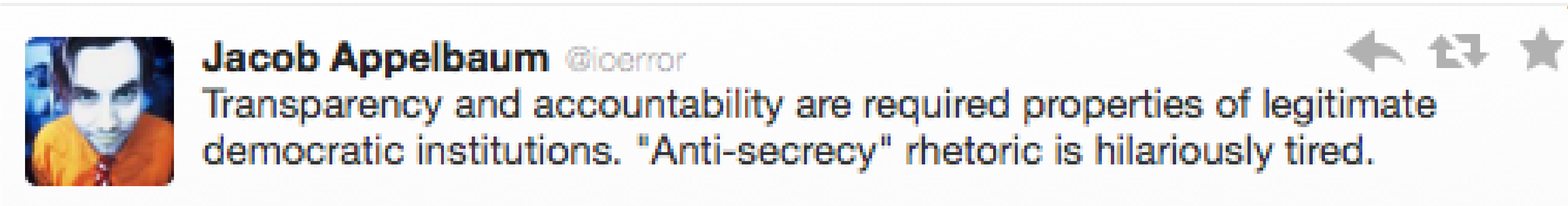
- The World Is Now Richer with 21 Million New Types of Malware, 230,000 Each Day
  `http://news.softpedia.com/news/the-world-is-now-richer-with-21-million-new-`
  `shtml`

Conclusion breaches og malware

- How to protect yourself in this hostile environment?
- How to protect your company?
- How to protect your family data?

First have a good backup, test it, rerun it

Democracy now: Why do we bother?



In a democracy we need the citizens with freedom that can act without constant surveillance

Democracy requires that we can actively select which personal data to give up and to whom

Cryptography is peaceful protest against blanket surveillance

PS Wrote this slide loooong before Copenhagen shooting in 2015, still stand by it!

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`

Snowden is on Twitter

Source: `https://twitter.com/twitter/status/648938950812274688`

Multiple browsers

- 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 others for generic browsing

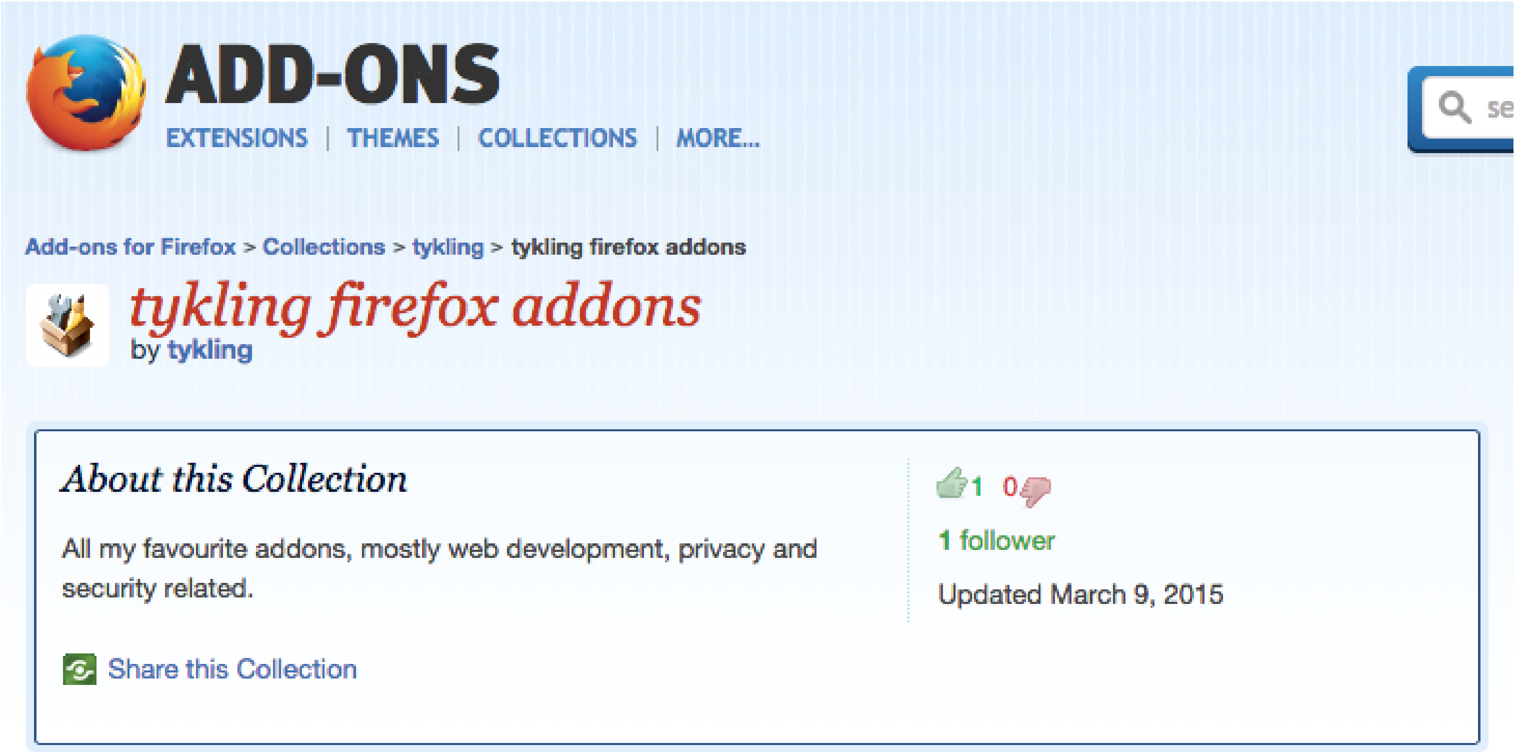
HTTPS Everywhere

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.

`https://www.eff.org/https-everywhere`

- Also check out their other projects
- Privacy Badger `https://www.eff.org/privacybadger`
- Surveillance Self-Defense is EFF's guide to defending yourself and your friends `https://ssd.eff.org/`

Add-ons Galore



You can find lots of privacy add-ons, above is a collection by @tykling from Twitter

`https://addons.mozilla.org/en-US/firefox/collections/tykling/tykling-firefox-addons/`

`https://www.denfri.dk/2015/03/5-firefox-tilfoejelser-der-kan-redde-dit-privatliv/`

Face reality

- 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 legals means, see *Rockerloven*

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

Overview of malware bypass today

Quote: The primary malware installation, sometimes referred as an infection, can be achieved using several attack vectors. The goal is always to run malicious code. Some of the most common attack vectors are:

- 1. Browser-based social engineering: where a user is tricked into clicking on a legitimate-looking URL which in turn triggers code execution using browser or browser-plugin vulnerabilities in Java and Flash. More advanced attacks can hide in legitimate traffic without requiring any user-interaction. These are commonly referred to as drive-by downloads.
- 2. Email-based social engineering and spear phishing: where a user receives an email that contains a hidden or visible binary, which executes when the user clicks on it.
- 3. Credential theft: when guessed or stolen credentials are used to access a remote machine and execute (malicious) code, such as installing a backdoor.

Source: Great summary article by Alon Nafta, senior security engineer at SentinelOne

How Malware Bypasses Our Most Advanced Security Measures, february 2015

`http://www.darkreading.com/perimeter/how-malware-bypasses-our-most-advanced-security-measures/a/d-id/1318974?_mc=RSS_DR_EDT`

Overview of malware bypass today, continued

Evasion techniques To evade detection, during and after installation, malware uses five primary techniques.

1. Wrapping. This process attaches the malicious payload (the installer or the malware itself) to a legitimate file. ... IceFog is a well-known malware commonly wrapped with a legitimate-looking CleanMyMac application and used to target OS X users. On the Windows platform, OnionDuke has been used with legitimate Adobe installers shared over Tor networks to infect machines.

2. Obfuscation. This involves modifying high level or binary code it in a way that does not affect its functionality, but completely changes its binary signature. ... Malware authors have adopted the technique to bypass antivirus engines and impair manual security research. ...

Source: How Malware Bypasses Our Most Advanced Security Measures

`http://www.darkreading.com/perimeter/how-malware-bypasses-our-most-advanced-security-measures/a/d-id/1318974?_mc=RSS_DR_EDT`

Overview of malware bypass today, continued

3. Packers. These software tools are used to compress and encode binary files, which is another form of obfuscation.... These techniques are extremely effective at circumventing static signature engines.

4. Anti-debugging. Like obfuscation, anti-bugging was originally created by software developers to protect commercial code from reverse-engineering. Anti-debugging can prevent a binary from being analyzed in an emulated environments such as virtual machines, security sandbox, and others. ...

5. Targeting. This technique is implemented when malware is designed to attack a specific type of system (e.g. Windows XP SP 3), application (e.g. Internet Explorer 10) and/or configuration (e.g. detecting a machine not running VMWare tools, which is often a telltale sign for usage of virtualization). ...

Source: How Malware Bypasses Our Most Advanced Security Measures

`http://www.darkreading.com/perimeter/how-malware-bypasses-our-most-advanced-security-measures/a/d-id/1318974?_mc=RSS_DR_EDT`

Most vulnerable operating systems in 2014

Operating system	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Apple Mac OS X	147	64	67	16
Apple iOS	127	32	72	23
Linux Kernel	119	24	74	21
Microsoft Windows Server 2008	38	26	12	0
Microsoft Windows 7	36	25	11	0
Microsoft Windows Server 2012	38	24	14	0
Microsoft Windows 8	36	24	12	0
Microsoft Windows 8.1	36	24	12	0
Microsoft Windows Vista	34	23	11	0
Microsoft Windows RT	30	22	8	0

An average of 19 vulnerabilities per day were reported in 2014, according to the data from the National Vulnerability Database (NVD).

Source:

`https://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/`

Most vulnerable applications in 2014

Application	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Microsoft Internet Explorer	242	220	22	0
Google Chrome	124	86	38	0
Mozilla Firefox	117	57	57	3
Adobe Flash Player	76	65	11	0
Oracle Java	104	50	46	8
Mozilla Thunderbird	66	36	29	1
Mozilla Firefox ESR	61	35	25	1
Adobe Air	45	38	7	0
Apple TV	86	29	49	8
Adobe Reader	44	37	7	0
Adobe Acrobat	43	35	8	0
Mozilla SeaMonkey	63	28	34	1

Not surprisingly at all, web browsers continue to have the most security vulnerabilities because they are a popular gateway to access a server and to spread malware on the clients.

Source:

`https://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/`

Release of vuln information without patch

Google project Zero

Follow a ”90-day disclosure deadline statement... which in this instance has passed.”

Released Zero-day information about Microsoft and Apple OS X vulnerabilities

MS patched some in *first Patch Tuesday of 2015, which came out on Jan. 13.*

Sources:

`http://googleonlinesecurity.blogspot.fr/2014/07/announcing-project-zero.html`

`http://searchsecurity.techtarget.com/news/2240238448/Googles-Project-Zero-reveals-another-Windows-zero-day-vulner`

`http://www.engadget.com/2015/01/02/google-posts-unpatched-microsoft-bug/`

`http://www.eweek.com/security/google-project-zero-continues-its-microsoft-zero-day-assault.html`

`http://www.zdnet.com/article/googles-project-zero-reveals-three-apple-os-x-zero-day-vulnerabilities/`

Trend with more vulnerabilities per day, and
even big vendors cannot react quickly enough

Samba remote code execution

```
===========================================================
== Subject:     Unexpected code execution in smbd.
==
== CVE ID#:     CVE-2015-0240
==
== Versions:    Samba 3.5.0 to 4.2.0rc4
==
== Summary:     Unauthenticated code execution attack on
== smbd file services.
==
===========================================================
```

Great, even our old tools still has multiple bugs

Source:
`https://www.samba.org/samba/security/CVE-2015-0240`

DNS attacks, February 2015 - ongoing for +10 years!

26 FEB 15

Webnic Registrar Blamed for Hijack of Lenovo, Google Domains

Two days ago, attackers allegedly associated with the fame-seeking group **Lizard Squad** briefly hijacked Google's Vietnam domain (google.com.vn). On Wednesday, **Lenovo.com** was similarly attacked. Sources now tell KrebsOnSecurity that both hijacks were possible because the attackers seized control over **Webnic.cc**, the Malaysian registrar that serves both domains and 600,000 others.

DNS insecurity has huge impact on your security!

Most are denial of service, by may create Mitm or confidentiality concerns

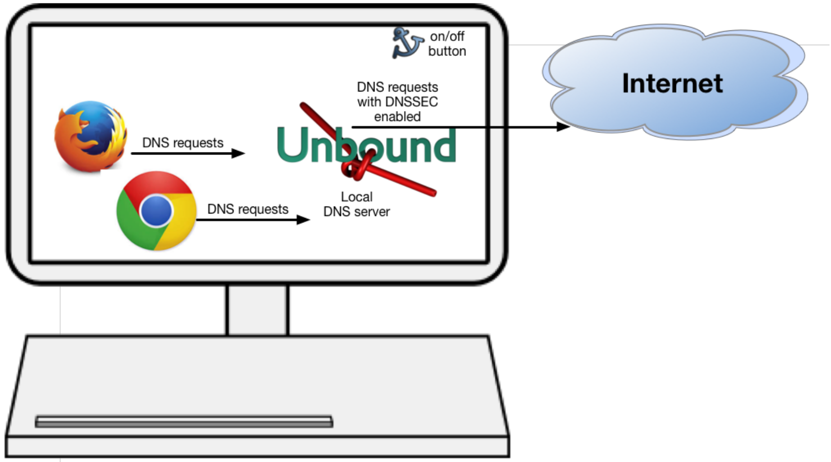
Select DNS providers with care

Sources:

`https://krebsonsecurity.com/2015/02/webnic-registrar-blamed-for-hijack-of-lenovo-google-domains/`

`http://www.version2.dk/artikel/google-og-lenovo-defaced-som-foelge-af-overset-sikkerhedsproblemstilling-91295`

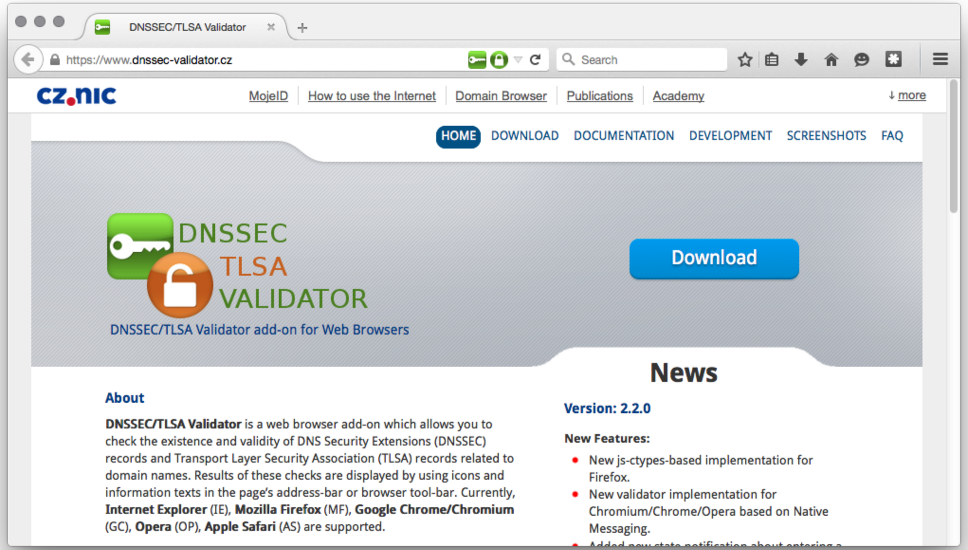
DNSSEC trigger



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`
- `https://www.nlnetlabs.nl/projects/dnssec-trigger/`

DNSSEC get started now



”TLSA records store hashes of remote server TLS/SSL certificates. The authenticity of a TLS/SSL certificate for a domain name is verified by DANE protocol (RFC 6698). DNSSEC and TLSA validation results are displayer by using several icons.”

DNSSEC and DANE

> ”Objective:
>
> Specify mechanisms and techniques that allow Internet applications to establish cryptographically secured communications by using information distributed through DNSSEC for discovering and authenticating public keys which are associated with a service located at a domain name.”

DNS-based Authentication of Named Entities (dane)

Old news - we have been talking about DANE for years! `https://datatracker.ietf.org/wg/dane/charter/`

`http://googleonlinesecurity.blogspot.dk/2011/04/improving-ssl-certificate-security.html`

Trend, we have HUGE populations of older servers, systems, people, that are just not taking to new technologies - even if it would solve a lot of problems

Case in point: IPv6

But DNSSEC is bad! DNS Amplification?!

Yes, DNSSEC has larger responses, used for amplification DDoS attacks.

> ”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

Trend, any problem has a Github repo with parts of the solution ☺

Example, Using tools similar to PacketQ

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
```

Are you using your brain and existing tools? Building own specialised tools?
Discussion: bridging the gaps between Devops and Security? Good thing, easy?

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

http://jpmens.net/2013/05/27/server-agnostic-logging-of-dns-queries-responses/

Storing query logs, old school or needed?

- policy/protocols/ssl/expiring-certs.bro
- policy/protocols/ssl/extract-certs-pem.bro
- policy/protocols/ssl/heartbleed.bro
- policy/protocols/ssl/known-certs.bro
- policy/protocols/ssl/log-hostcerts-only.bro
- policy/protocols/ssl/validate-certs.bro
- policy/protocols/ssl/validate-ocsp.bro
- policy/protocols/ssl/weak-keys.bro

Looking at DNS PacketQ it was an Older link, but thinking the time is now for doing:

- DNS query logs, keep it for at least a week? - with DSC and PacketQ
- SSL/TLS full logs over sessions, certs, keys - with Bro/Suricata
  `https://www.bro.org/sphinx-git/script-reference/scripts.html`
- Log and search with Elasticsearch?
  `https://www.elastic.co/guide/en/elasticsearch/guide/current/index.html`
- Even netflow session logging, full 1:1 - NFSen, Suricata Flow mode?

February 2015: Finding infected sources

”We were contacted by a client to help with their incident response in tracking down an infection on a clients machine with the new CTB-Locker ransomware (Curve-Tor-Bitcoin Locker) aka Critroni which had no signatures available at the time of infection for this variant.

LANGuardian includes a file share activity monitoring module which provided a very detailed forensic analysis of the ransomware and the paths it had taken in order to encrypt the clients system and also the fileserver in which it was connected to, the initial infection came from the opening of an attachment in an e-mail.”

It has become critical to identify vulnerable or infected ASAP!

Source: `https://www.netfort.com/support-team-stories-detecting-the-source-of-ransomware/`

Dont forget Suricata and Security Onion, mentioned later

Why?, because things like Superfish February 2015

Yet another SSL/TLS related problem

Thursday, February 19, 2015

Extracting the SuperFish certificate

By Robert Graham

I extracted the certificate from the SuperFish adware and cracked the password ("*komodia*") that encrypted it. I discuss how down below. The consequence is that I can intercept the encrypted communications of SuperFish's victims (people with Lenovo laptops) while hanging out near them at a cafe wifi hotspot. Note: this is probably trafficking in illegal access devices under the proposed revisions to the CFAA, so get it now before they change the law.

Lenovo laptops included Adware, which did SSL/TLS Man in the Middle on connections. They had a root certificate installed on the Windows operating system, WTF!

Sources:

`https://en.wikipedia.org/wiki/Superfish`

`http://blog.erratasec.com/2015/02/extracting-superfish-certificate.html`

`http://www.version2.dk/blog/kibana4-superfish-og-emergingthreats-81610`

`https://www.eff.org/deeplinks/2015/02/further-evidence-lenovo-breaking-https-security-its-laptops`

FREAK March 2015

> ”A group of cryptographers at INRIA, Microsoft Research and IMDEA have discovered some serious vulnerabilities in OpenSSL (e.g., Android) clients and Apple TLS/SSL clients (e.g., Safari) that allow a ’man in the middle attacker’ to downgrade connections from ’strong’ RSA to ’export-grade’ RSA. These attacks are real and exploitable against a shocking number of websites – including government websites. Patch soon and be careful.”

Source: Matthew Green, cryptographer and research professor at Johns Hopkins Univ

`http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html`

`https://www.smacktls.com/` `https://freakattack.com/`

OpenSSL, LibreSSL, Apple SSL flaw exit exit exit!, Android SSL, certs certs!!!111, SSLv3, Heartbleed, MS TLS

F this I’m going out drinking beer *drops mic*

PS From now on its TLS! Not SSL anymore, any SSLv2, SSLv3 is old and vulnerable

Bettercrypto.org pretty good advise

SSL settings for nginx

```
ssl_prefer_server_ciphers on;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2; # not possible to do exclusive
ssl_ciphers 'EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA384:EECDH+\
  \aRSA+SHA256:EECDH:+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:!aNULL:!\
  \eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ECDSA:CAMELLIA256-SHA:AES256\
  \-SHA:CAMELLIA128-SHA:AES128-SHA';
add_header Strict-Transport-Security max-age=15768000; # six months
# use this only if all subdomains support HTTPS!
# add_header Strict-Transport-Security "max-age=15768000; includeSubDomains";
```

Listing 2.6: *SSL settings for nginx*
[configuration/Webservers/nginx/default]

Overview

> ”This whitepaper arose out of the need for system administrators to have an updated, solid, well researched and thought-through guide for configuring SSL, PGP, SSH and other cryptographic tools in the post-Snowden age. ... This guide is specifically written for these system administrators.”

`https://bettercrypto.org/`

New tools - learn a lot - try new tools!

Kali 2.0

Kibana 4 everyone can start creating dashboards

Burp Suite Professional - efficient web scanner

Security Onion and Suricata updates - learn some NSM

Tor Browser 4.0.4 anonymous browsing

Tails 1.3 - anonymous computing from USB sticks

Wordlists −> change your passwords frequently!

Decrypt SSL sessions while debugging - nifty tricks

Kali 2.0 August 2015

Highly recommended! Used by everybody

Source:
`https://www.kali.org/`

Kibana 4 february 2015

Highly recommended for a lot of data visualisation

Non-programmers can create, save, and share dashboards

Source: `https://www.elastic.co/products/kibana`

Hacker tools Burp

Tuesday, February 17, 2015

v1.6.11

This release adds a new Scanner check for path-relative style sheet import (PRSSI) vulnerabilities.

PRSSI vulnerabilities (sometimes termed "relative path overwrite") are not widely understood by security testers or application developers. The key prerequisite for the vulnerability (a CSS import directive that uses a path-relative URL) is both seemingly innocuous and very common. There are some other conditions that are needed for exploitability, but real vulnerabilities are quite prevalent in the wild. The impact of the vulnerability is in many cases serious, and equivalent to cross-site scripting (XSS).

New attack types and updates `http://blog.portswigger.net/`

Do it in your own network - your systems, keep it legal

Burp is a highly recommended commercial Web proxy EUR 275/user/year 2.000DKK

Pro version includes scanner and spidering functionality

2015, Suricata and Security Onion updates

- Security Onion 12.04.5.1 ISO image now available
- Suricata IDS engine 2.0.7 updated packages for SO released
- Learn NSM with Security Onion today - its free

```
http://blog.securityonion.net/2015/03/suricata-207.html
http://blog.securityonion.net/2015/02/security-onion-120451-iso-image-now.html
```

September 22nd 2015: Tor Browser 5.5a3 Released

> ”Tor - a privacy oriented encrypted anonymizing service, has announced the launch of its next version of Tor Browser Bundle, i.e. Tor version 4.0.4, mostly supposed to improve the built-in utilities, privacy and security of online users on the Internet.”

Source: `http://thehackernews.com/2015/02/tor-browser-download.html`
`https://www.torproject.org/`

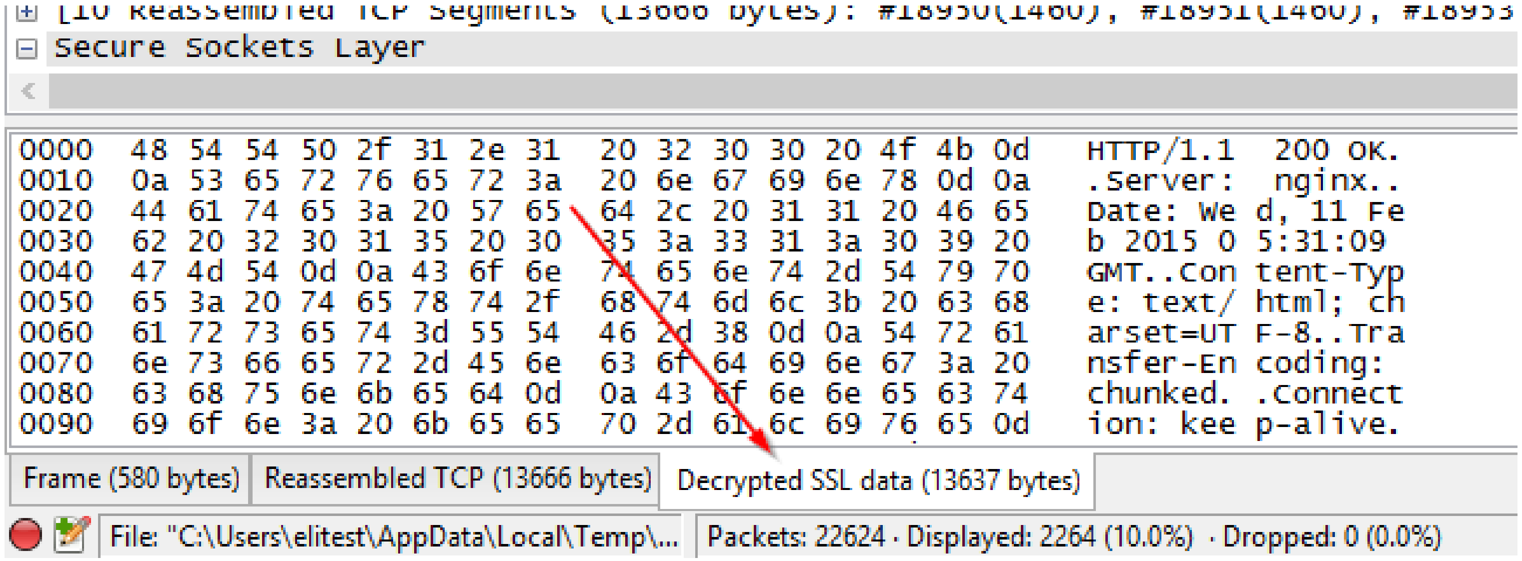
also new Tails Tails 1.6 September 22, 2015
`http://thehackernews.com/2015/02/tails-tor-privacy-tools.html`
`https://tails.boum.org/download/index.en.html`

Feb 2015 Today I Am Releasing Ten Million Passwords

”Why the FBI Shouldn’t Arrest Me
Although researchers typically only release passwords, I am releasing usernames with the passwords. Analysis of usernames with passwords is an area that has been greatly neglected and can provide as much insight as studying passwords alone. Most researchers are afraid to publish usernames and passwords together because combined they become an authentication feature. If simply linking to already released authentication features in a private IRC channel was considered trafficking, surely the FBI would consider releasing the actual data to the public a crime.”

Source: Mark Burnett’s Blog
`https://xato.net/passwords/ten-million-passwords/`

Feb 2015 Decrypting TLS Browser Traffic With Wireshark



Firefox and Chrome both support logging the symmetric session key used to encrypt TLS traffic to a file

Wireshark can read this file - and decrypt sessions - Nifty trick

Source: great blog article about the features used

`https://jimshaver.net/2015/02/11/decrypting-tls-browser-traffic-with-wireshark-the-easy-way/`

DDoS in 2015

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.

Please think about DDoS and plan organizational responses

Both technical preparedness and organizational awareness important

DDoS in 2015

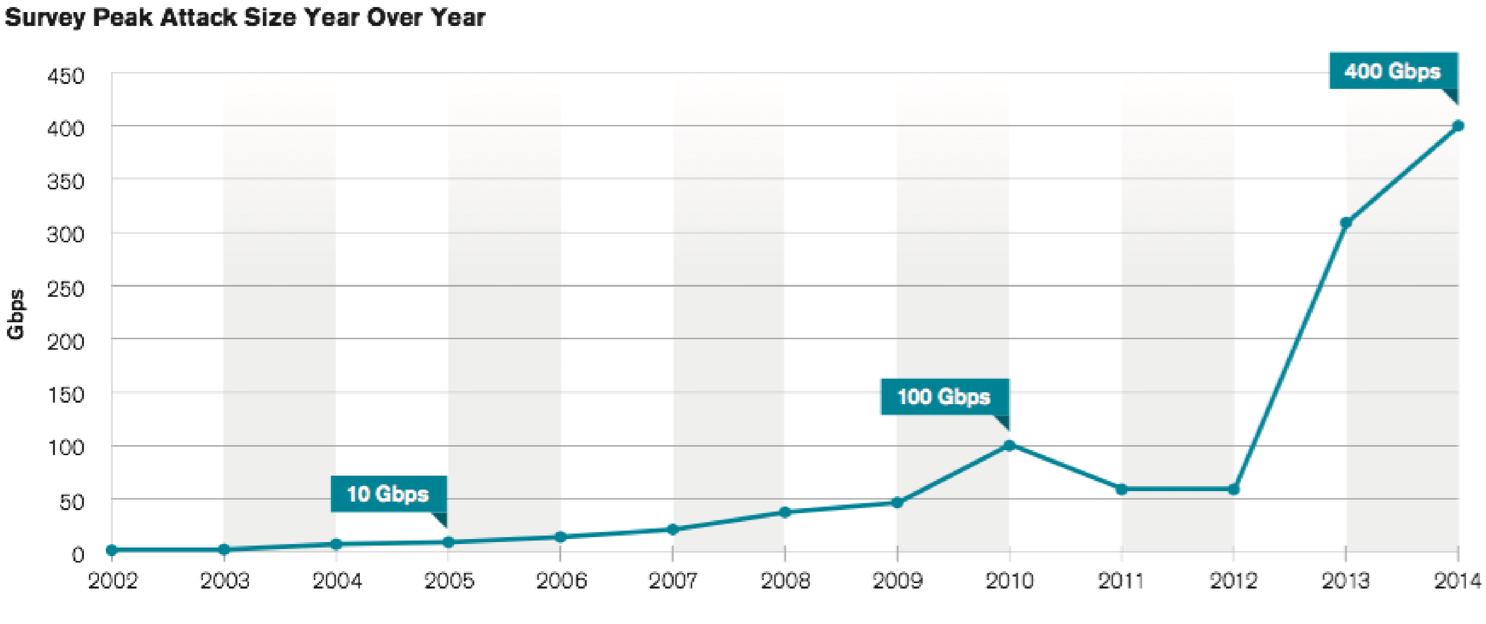
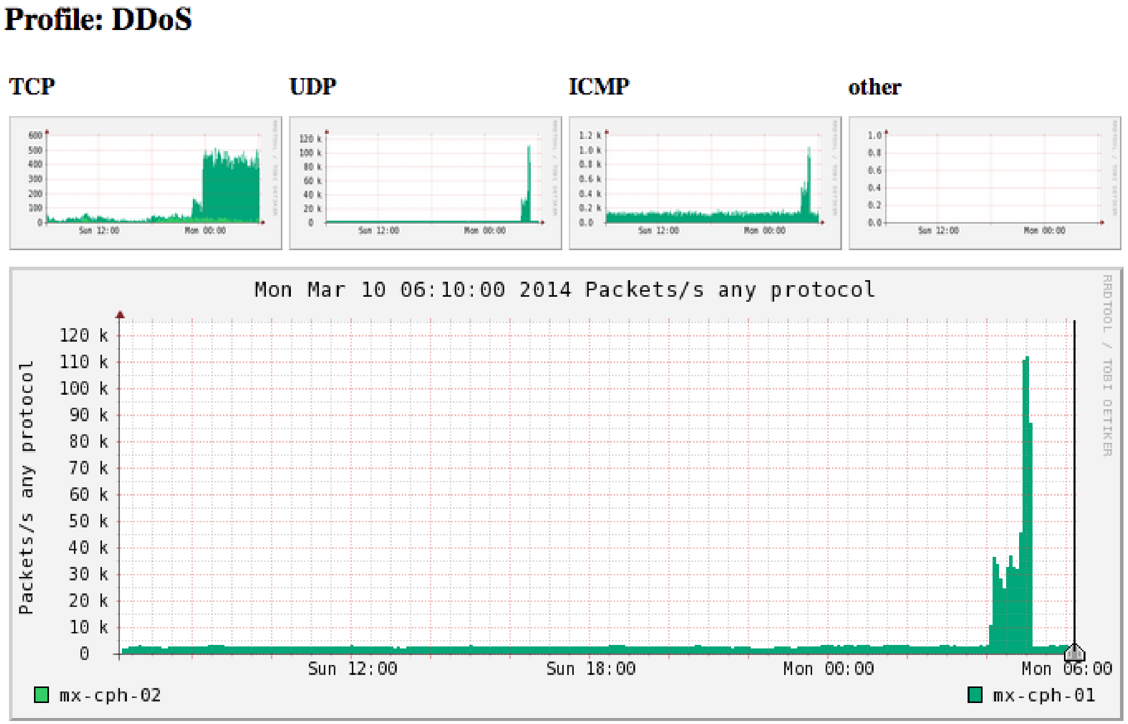


Figure 12 Source: Arbor Networks, Inc.

Expect amplification attacks and 3-digit attacks for some years

Source:
Arbor Networks: Worldwide Infrastructure Security Report, Volume X January 2015

Detecting DDoS example tool Nfsen

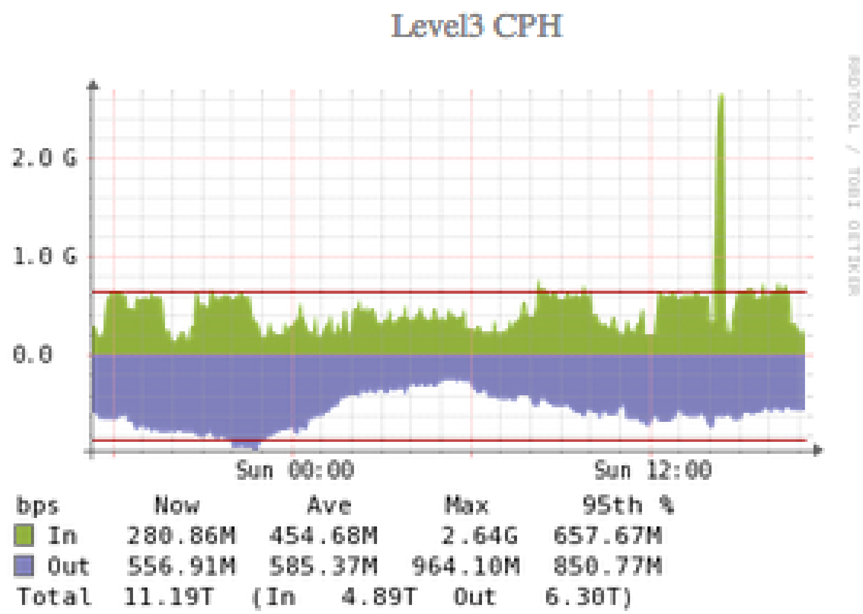


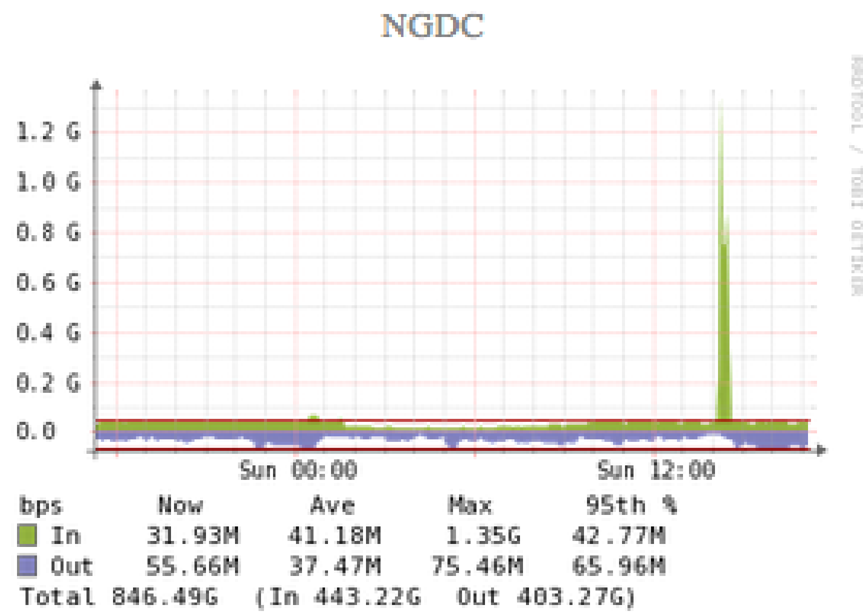
We created a DDoS profile with the common types.

We can ask RRDtools 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
```

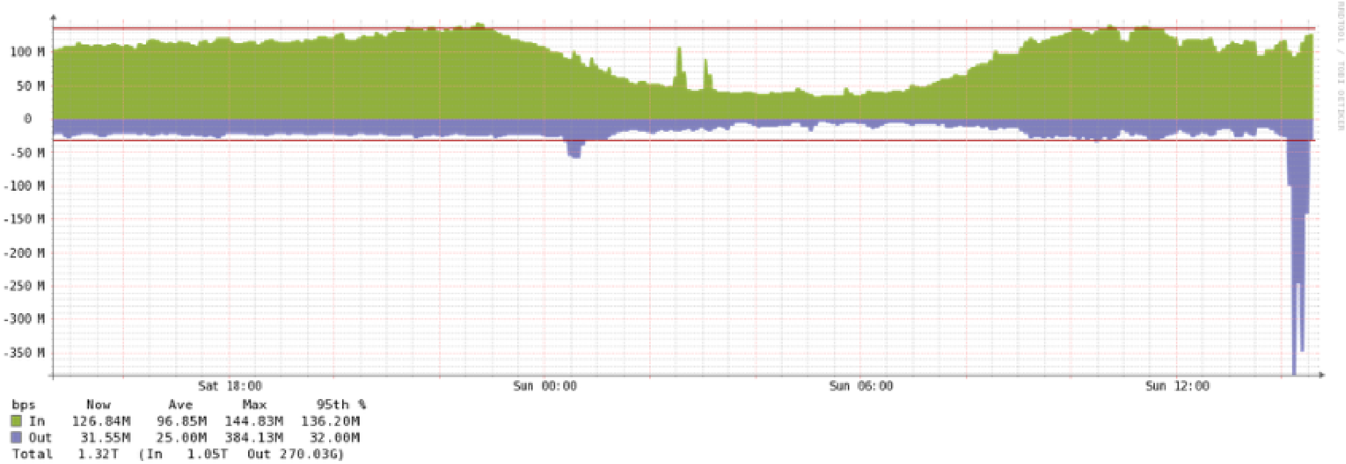
DDoS traffic before filtering





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

DDoS traffic after filtering



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

Problem: We receive unauthenticated chaotic traffic

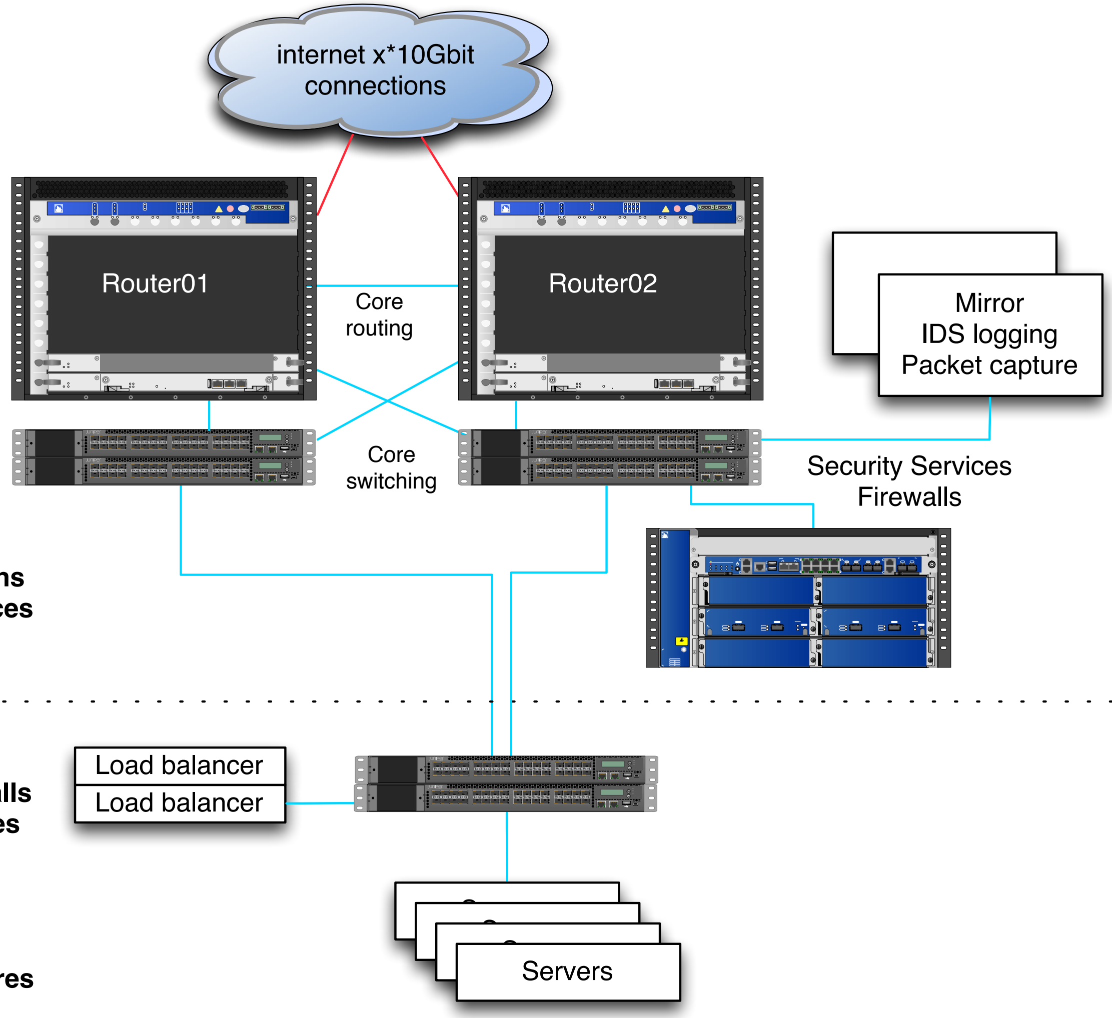
Solution: Discard early, discard on edge, reduce noise

Only use CPU resources for potentially real traffic

Single firewall layer typically cannot cope!

Defense in depth - multiple layers of security

Knowledge about traffic	Proposed actions to be done
	Get more bandwidth
Individual packets	Stateless filtering
Valid source IP ?	Null-routing RTBH Blackholing
Identify traffic by Ports/Protocols	Shaping and fair distribution
Sessions #sessions/IP	Stateful filtering screens IDS/IDP security services
Full request with parameters and cookies	Application tuning Next generation firewalls Load balancer features
Logged in user authenticated?	Server security Input validation
	Stack protection features



Proxy servers - protection services

Several big players you need to research before needing them!

Arbor Networks sells software solutions for carriers
https://www.arbornetworks.com/

Prolexic sells DDoS services, DNS and BGP based
https://www.prolexic.com/

CloudFlare proxy based
https://www.cloudflare.com/

Juniper DDoS solutions

Multiple Major Danish ISPs have bought services from the above companies

Focus for the near future

- Walk through your infrastructure
  get a detailed view of data, flows, protocols, bandwidth, ports and services
- Create a list of critical phone numbers and contacts, enter it in your phone
- Automate updates for both clients and servers, goal update everything in hours
- Learn to run Nmap and Metasploit scripts - identify vulnerable servers

consider the fact we have multiple overlapping critical security incidents now!

How many incidents can your organisation handle in parallel?

Can multiple people in your organisation initate updates?

Future actions- fall 2015

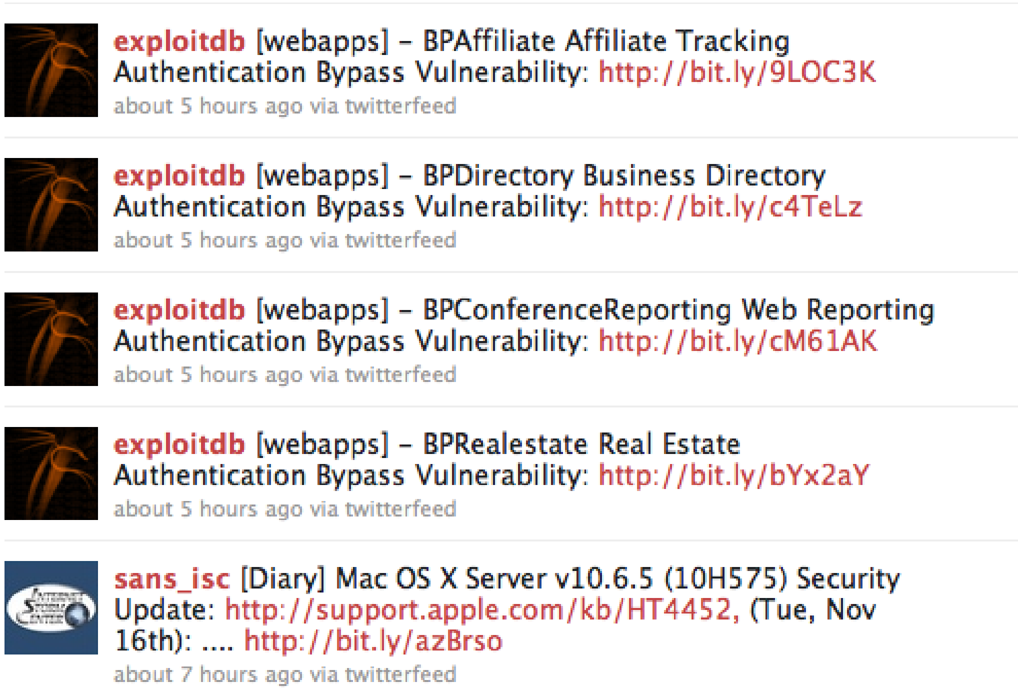
- Document your processes, systems, applications, databases, backup and restore procedures
  Finish before summer - so you can have vacation, will be needed!
- Share information within your organisation, and outside
  Make friends!
- Crypto Parties - get them started, keep them going!
- My Conferences: catch up after CCC Summercamp
- Next up? Congress? `https://en.wikipedia.org/wiki/Chaos_Communication_Congress`

Keep learning, keep coorporating, help others = help yourself

Chaos Communication Camp 2015

It was Awesome!

Sources for information



Twitter has replaced RSS for me

Email lists are still a good source of data

Open Mike night ...

what did I forget? tells us about your favourites ☺

Things I forgot, didn't include: february Gemalto hack,
Citizenfour won an oscar in February!

December Thunderbolt hack - thunderstrike

March, Rowhammer

`http://www.wired.com/2015/03/google-hack-dram-memory-electric-leaks/`

Samsung TVs listening and watching

DNS censorship, NemID bashing, Apple malware, Android malware, iPhone malware?

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

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

