Welcome to

Tendenser i sikkerhed

Marts 2014

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

Slides are available as PDF, kramshoej@Github

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

Hodge-podge of security related things - inspiration

Please give feedback and join me in discussions, dialogue ☺

Plan for today

Kl 17:30-21 and some breaks

Less presentation, more talk

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

Generic advice

SOLIDO NETWORKS

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

Democracy now: Why do we bother?

Jacob Appelbaum @ioerror

Transparency and accountability are required properties of legitimate democratic institutions. "Anti-secrecy" rhetoric is hilariously tired.

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

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`

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 NoScripts 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.

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

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!

Use protection - always

Turkey: Erdogan bans Twitter

Censorship on the internet - lol

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)

Directly connection Tor Users from Turkey

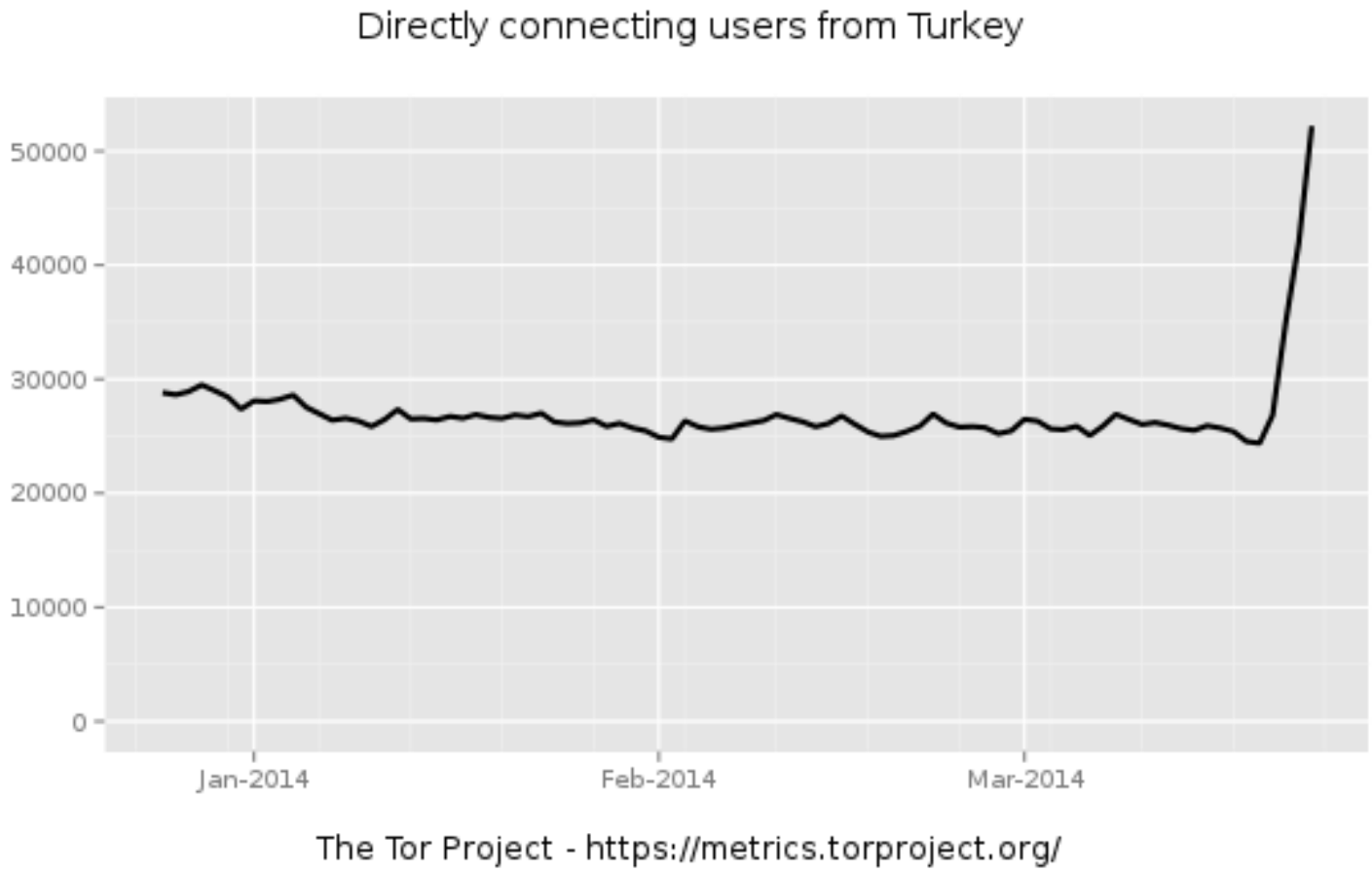


Image from `https://metrics.torproject.org`
via `https://twitter.com/runasand`

Directly connection Tor Users from Turkey +10.000

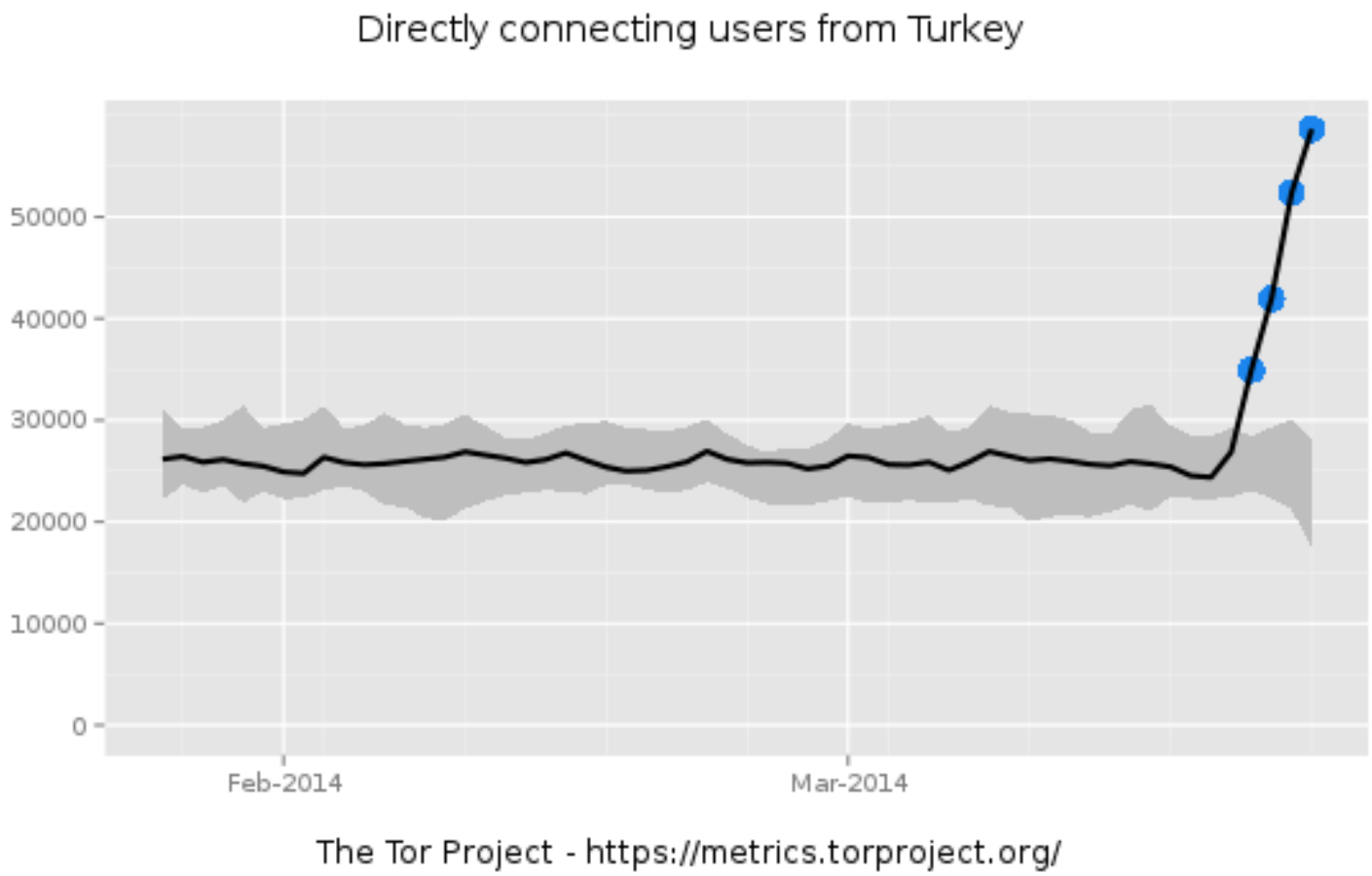


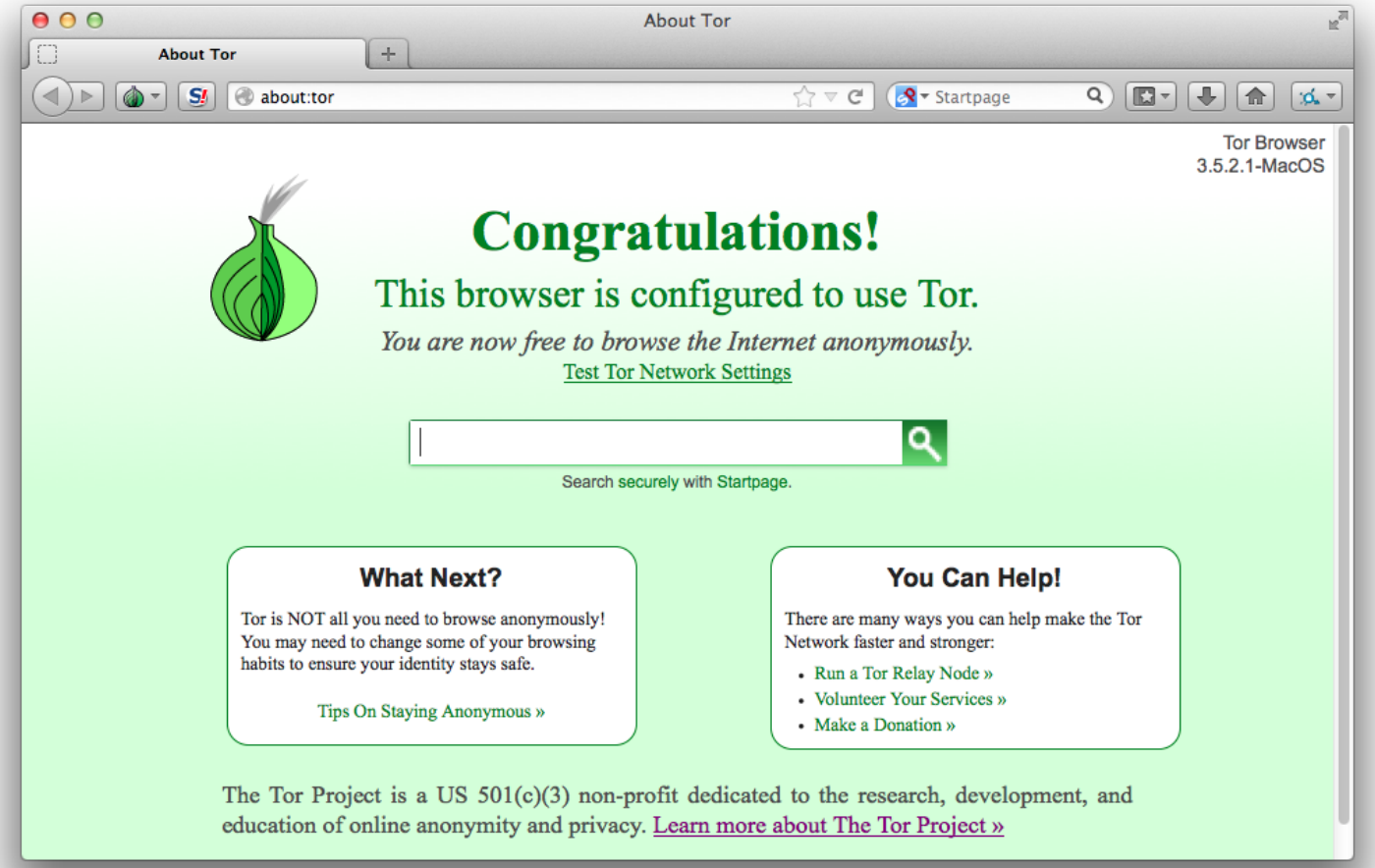
Image from `https://metrics.torproject.org` via `https://twitter.com/ioc32/status/448791582423408640`

Tor project install

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

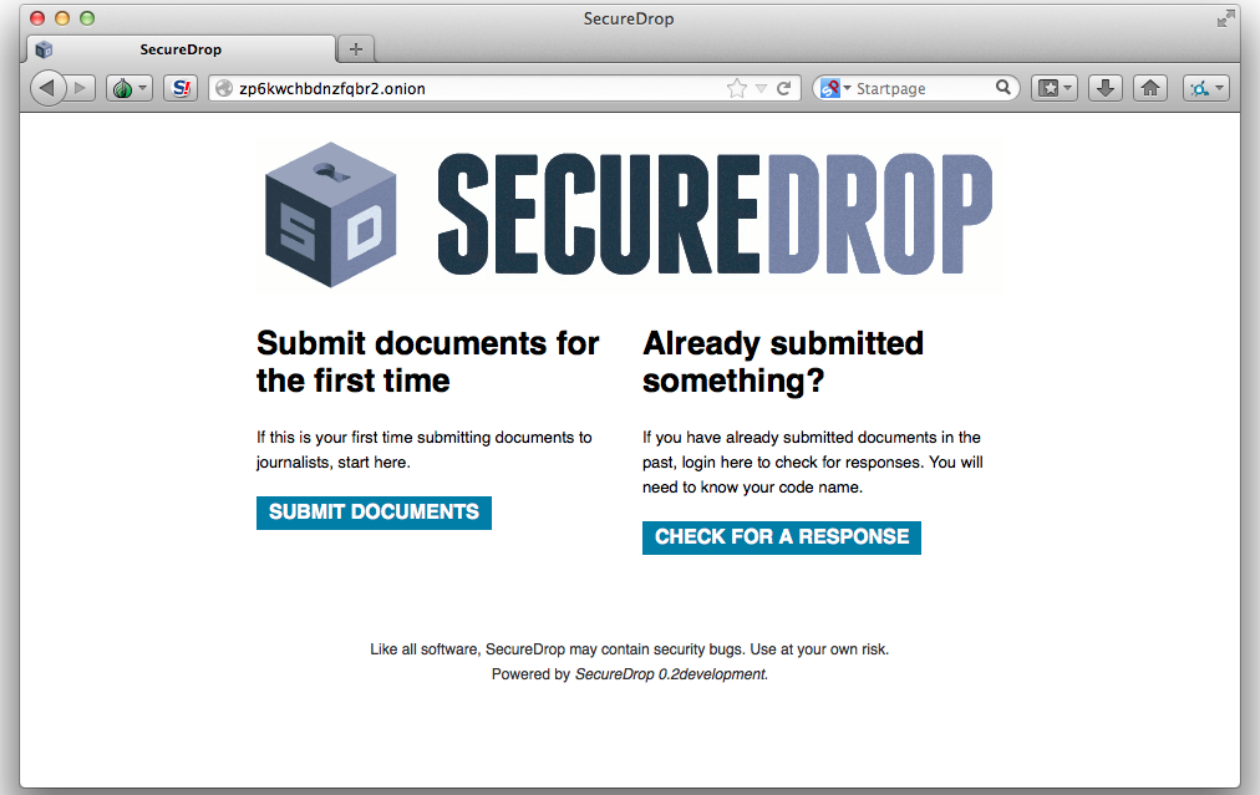
Det anbefales at bruge Torbrowser bundles fra `https://www.torproject.org/`

Torbrowser - anonym browser



Mere anonym browser - Firefox in disguise

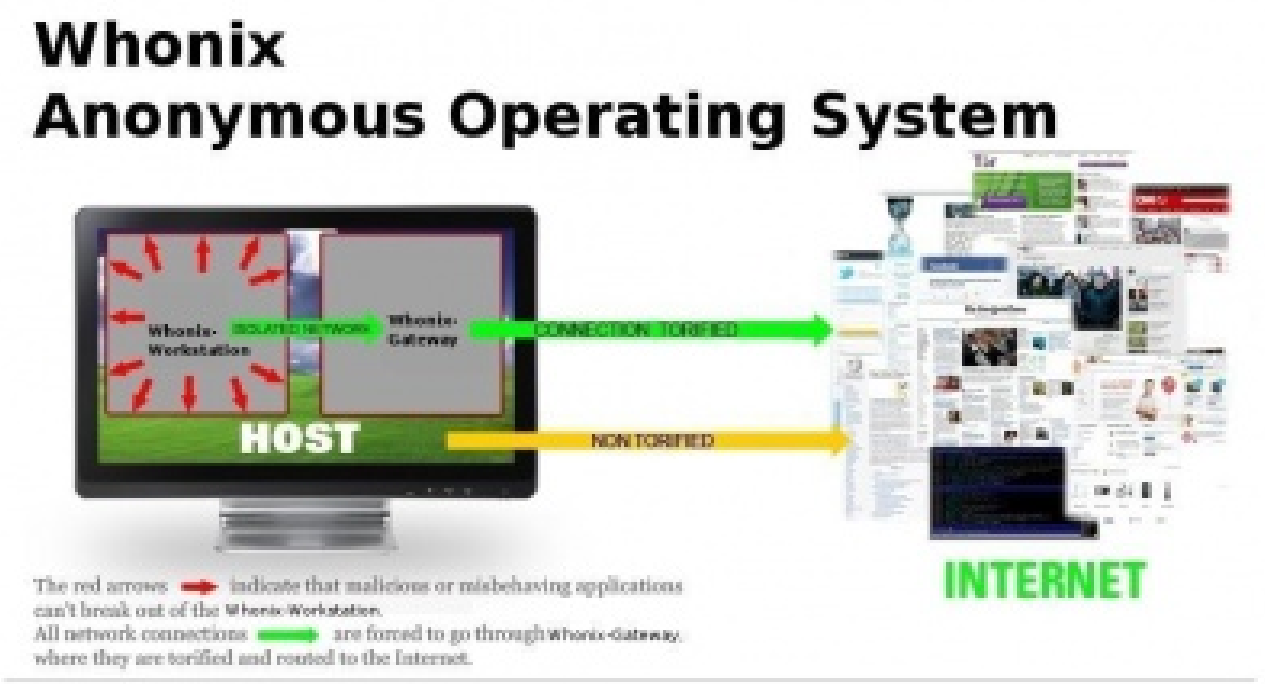
Torbrowser - sample site



.onion er Tor adresser - hidden sites

Den viste side er SecureDrop hos Radio24syv `http://www.radio24syv.dk/dig-og-radio24syv/securedrop/`

Whonix - Tor to the max!



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

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/`

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

But DNS is bad! DNS Amplification?!

SOLIDO NETWORKS

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

SOLIDO NETWORKS

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.

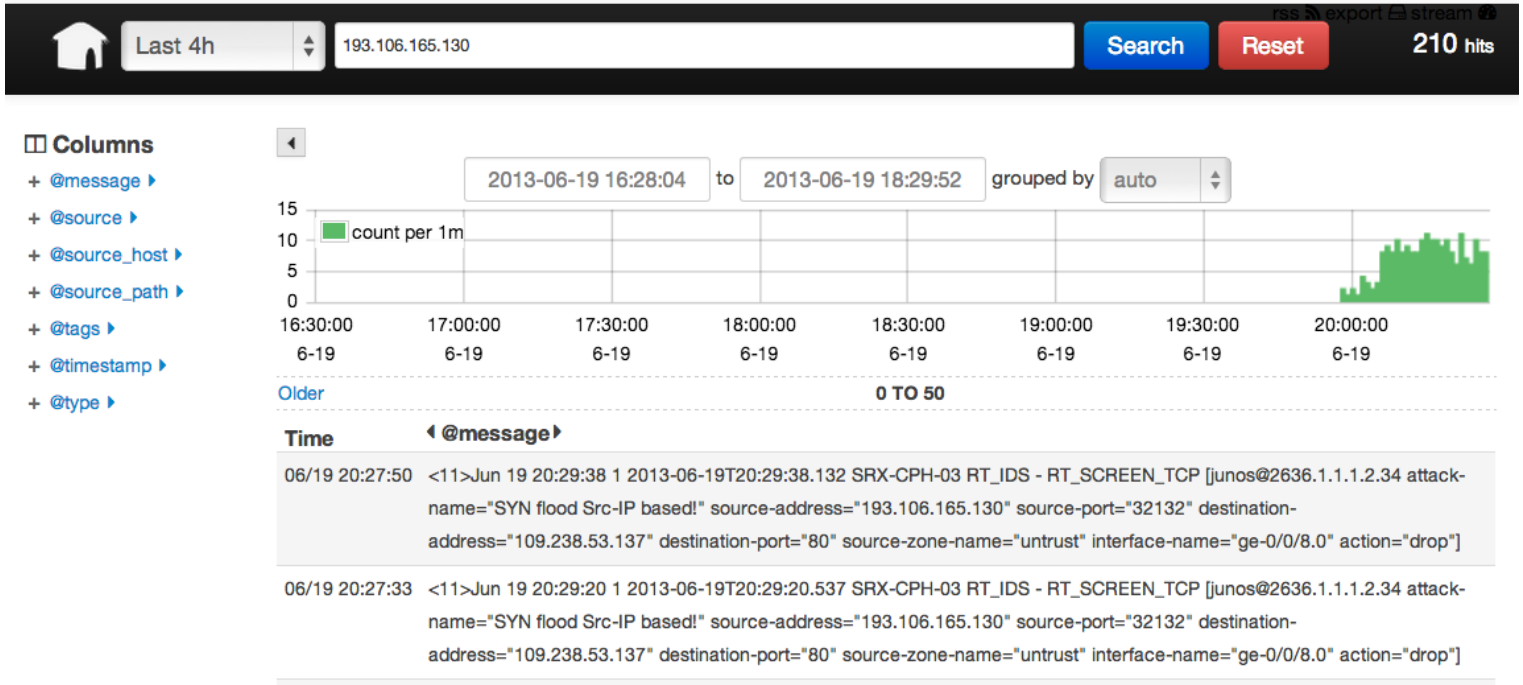
DNS ANY traffic is currently commonly abused for DNS amplification attacks (See Blog post "DDoS-Angriffe durch Reflektierende DNS-Amplifikation vermeiden" in German). The first thing I want to know is what are the IP addresses of the victims of this potential DNS amplification attack:

```
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/

Big data tools

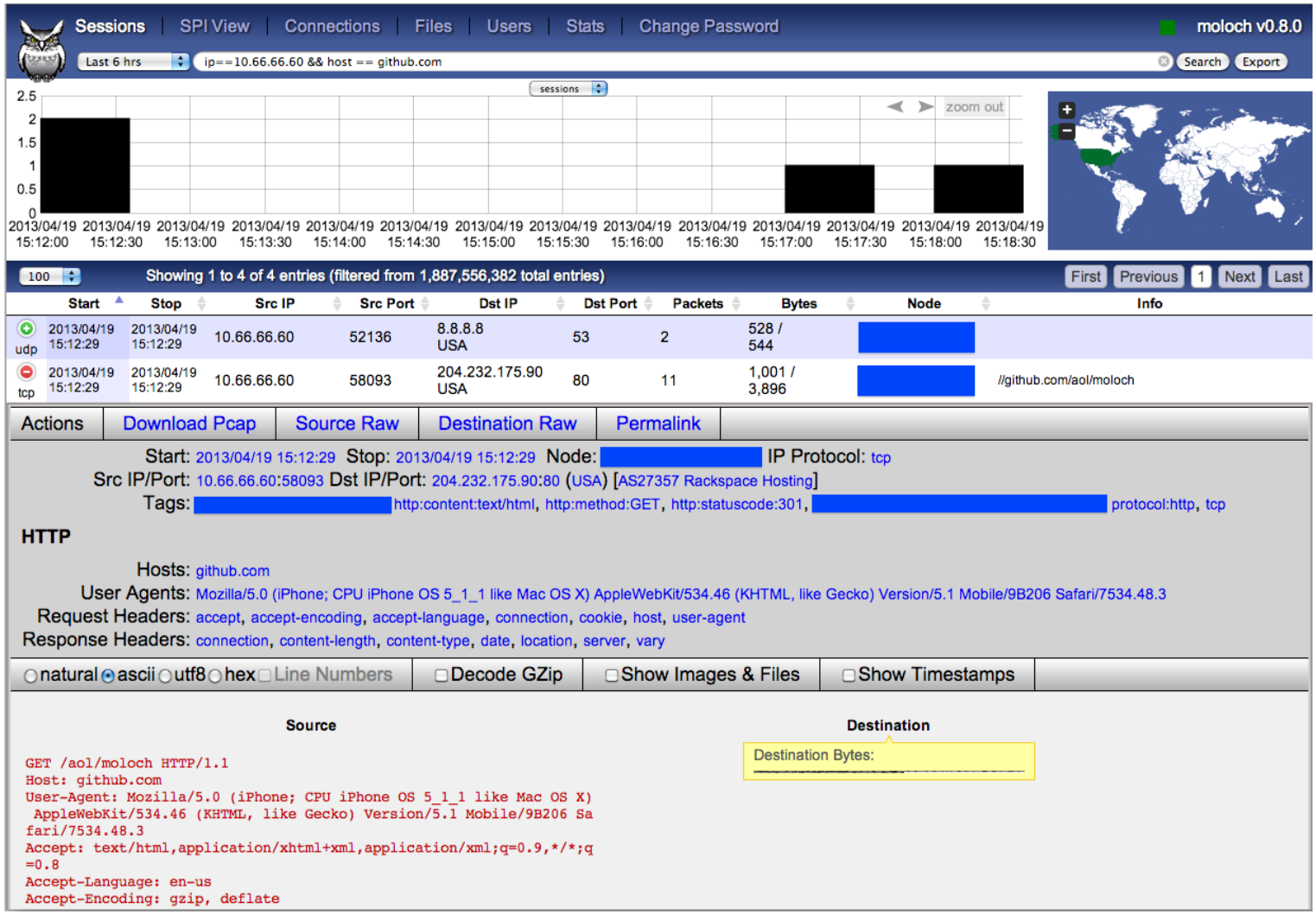


Moloch `https://github.com/aol/moloch`

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

Logstash, Elasticsearch and Kibana

Moloch



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/

SOLIDO NETWORKS

elasticsearch

the definitive guide

clinton gormley zachary tong Copyright Â© 2014 Elasticsearch

`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!

Nye tools

`http://www.kali.org/` Kali Linux Rebirth of BackTrack

`http://www.arachni-scanner.com/`
- been on my todolist for too long, try it maybe?

Hacker tools BackTrack and Kali

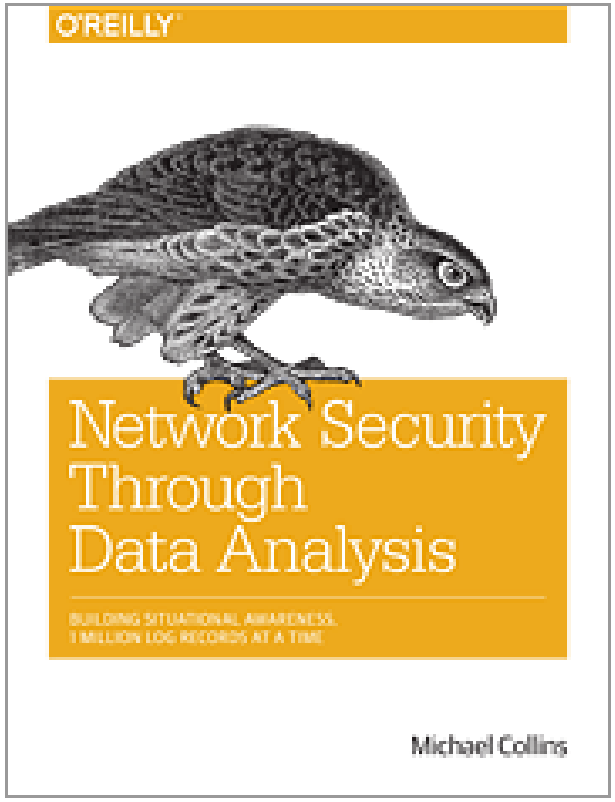
Hacking is fun - learn a lot

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

Run Kali Linux in a virtual machine

Kali Linux `http://www.kali.org/` denne version anbefales

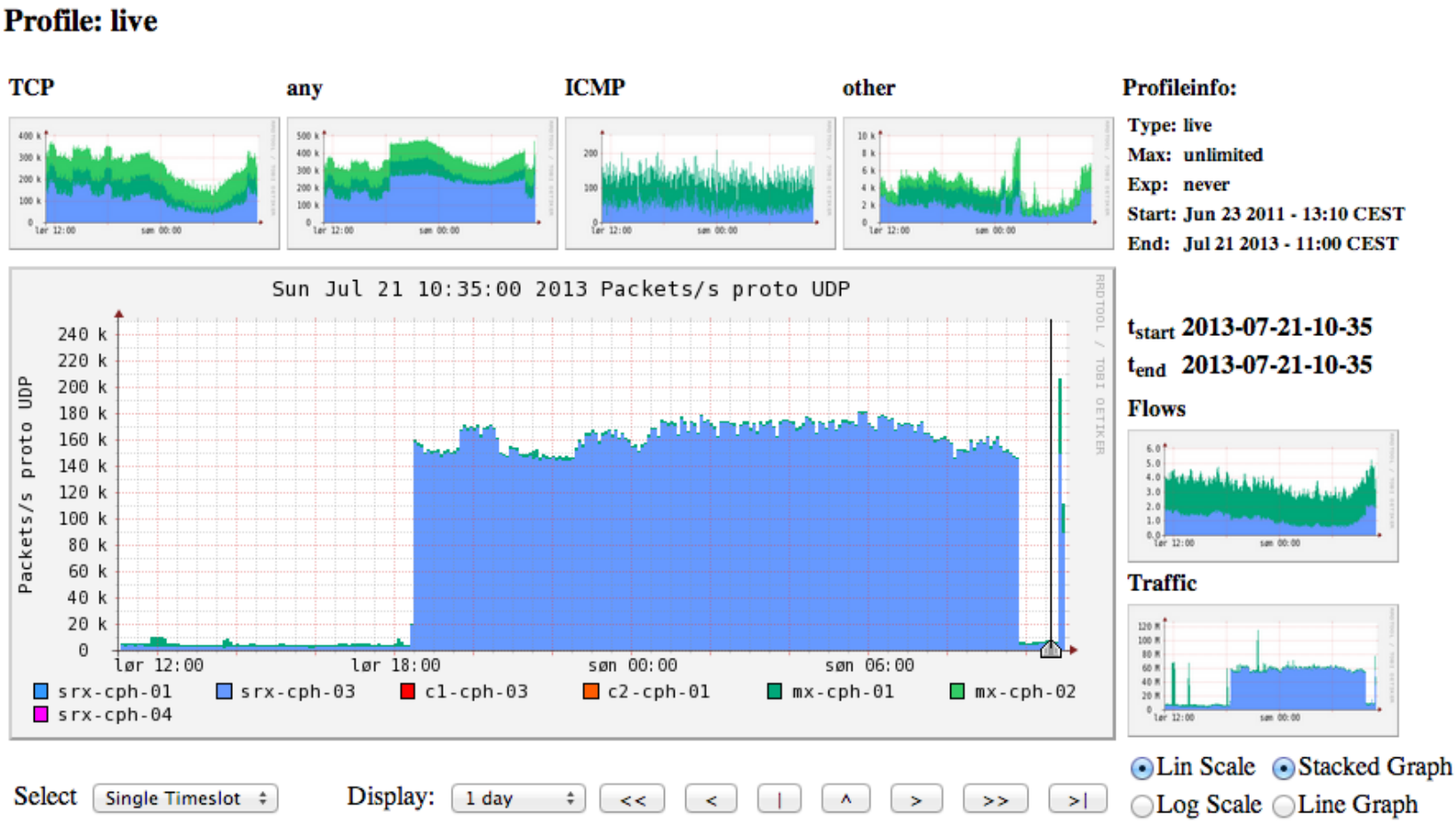
Network Security Through Data Analysis



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

Netflow NFSen



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

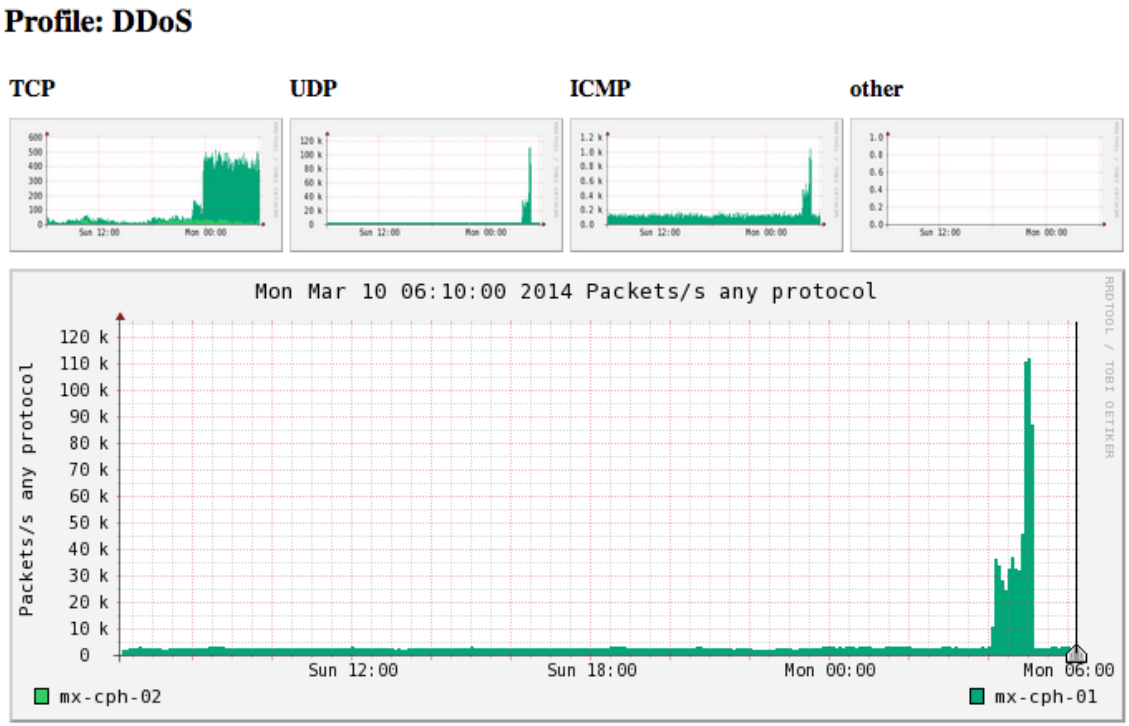
Alert (TA14-017A) UDP-based Amplification Attacks

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

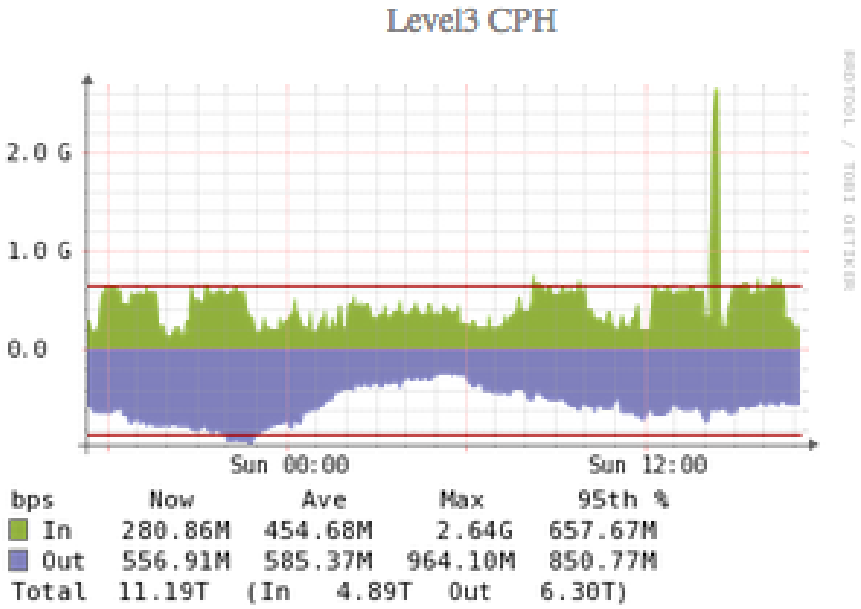


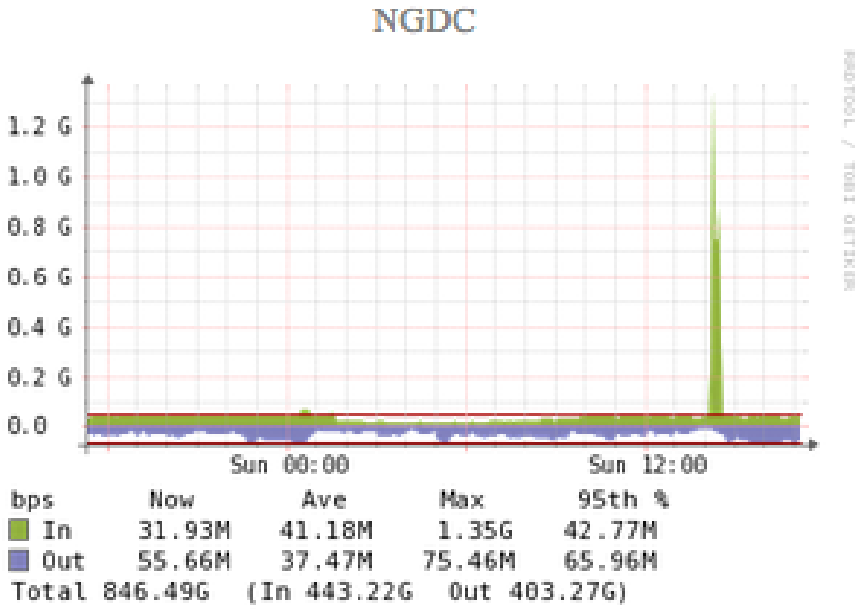
We created a DDoS profile with the common types.

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
```

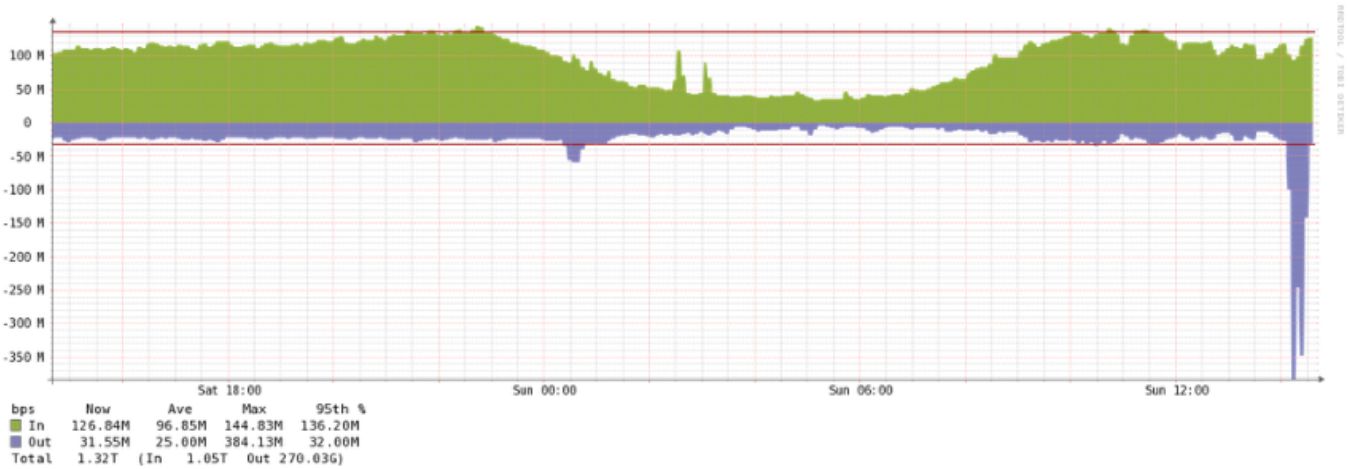
DDoS traffic before filtering





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

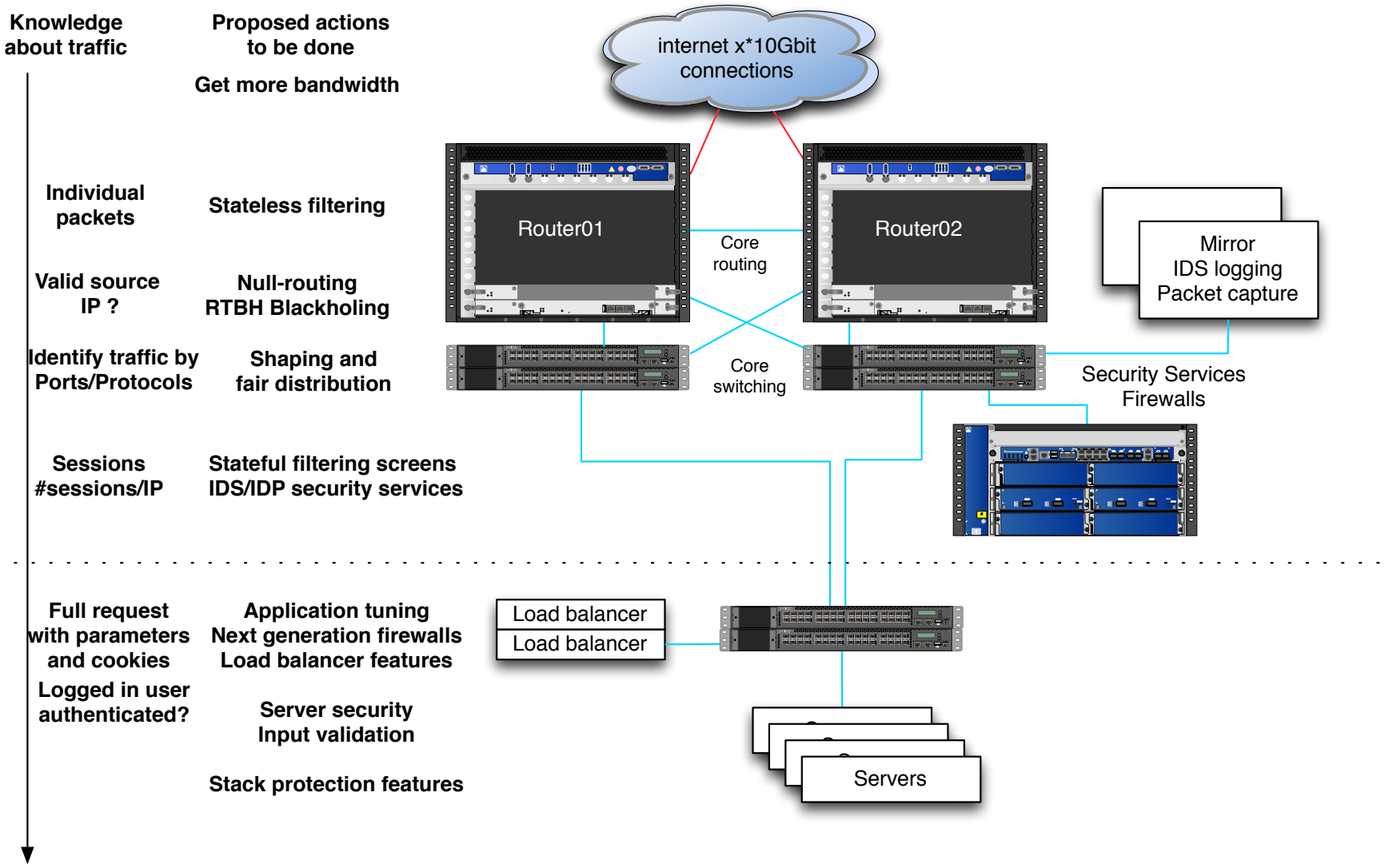
Strategy planning

Problem: We receive unauthenticated chaotic traffic

Solution: Discard early, discard on edge, reduce noise

Only use CPU resources for potentially real traffic

Defense in depth - multiple layers of security



Stateless firewall filter throw stuff away

```
hlk@MX-CPH-02> show configuration firewall filter all | no-more
/* This is a sample, better to use BGP flowspec and RTBH */
inactive: term edgeblocker {
    from {
        source-address {
            84.180.xxx.173/32;
...
            87.245.xxx.171/32;
        }
        destination-address {
            91.102.91.16/28;
        }
        protocol [ tcp udp icmp ];
    }
    then {
        count edge-block;
        discard;
    }
}
```

Hint: can also leave out protocol and then it will match all protocols

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

Firewalls - screens, IDS like features

When you know regular traffic you can decide:

```
hlk@srx-kas-05# show security screen ids-option untrust-screen
icmp {    ping-death; }
ip {    source-route-option;  tear-drop; }
tcp {    Note: UDP flood setting also exist
    syn-flood {
        alarm-threshold 1024;
        attack-threshold 200;
        source-threshold 1024;
        destination-threshold 2048;
        timeout 20;    }
    land;
} Always select your own settings YMMV
```

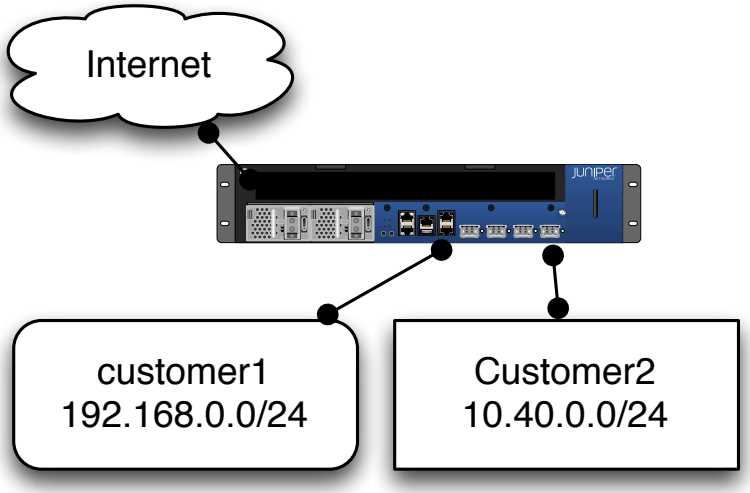
- Firewalls and security devices have lots of settings
- How many sessions does a single IP need?
- This can be done with reduced incoming traffic

Solving DDoS problems uRPF

Reverse path forwarding (RPF) is a technique used in modern routers for the purposes of ensuring loop-free forwarding of multicast packets in multicast routing and to help prevent IP address spoofing in unicast routing.

Source: `http://en.wikipedia.org/wiki/Reverse_path_forwarding`

Strict vs loose mode RPF

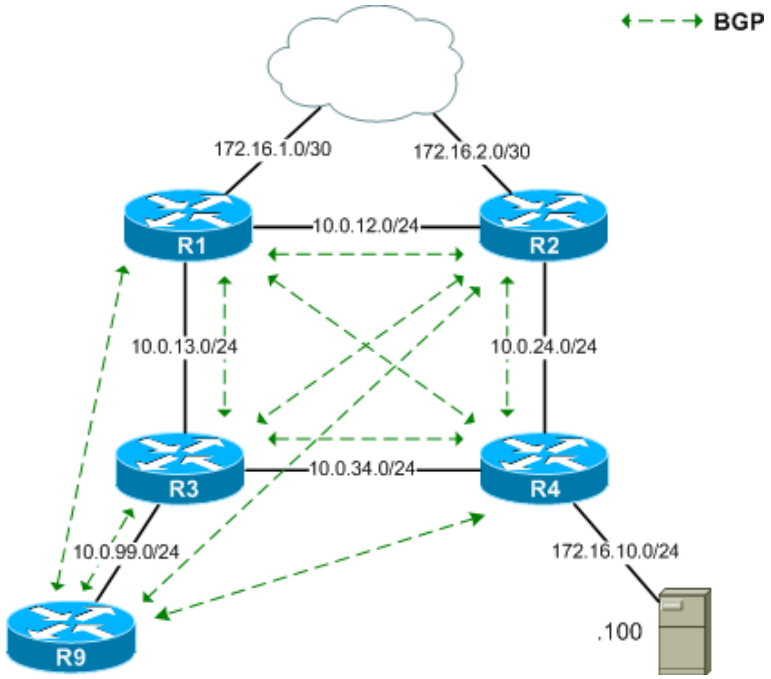



```
user@router# show interfaces
ge-0/0/0 {
        unit 2 {
                family inet {
                        rpf-check fail-filter rpf-special-case-dhcp;
                        address 192.168.0.254/24;
                }
        }
}
ge-0/0/1 {
        unit 2 {
                family inet {
                        rpf-check fail-filter rpf-special-case-dhcp;
                        address 10.40.0.254/24;
                }
        }
}
```

Configuring Unicast RPF Strict Mode

In strict mode, unicast RPF checks whether the incoming packet has a source address that matches a prefix in the routing table, **and whether the interface expects to receive a packet with this source address prefix.**

Remotely Triggered Black Hole Configurations



Picture from packetlife.net showing R9 as a standalone ”management” router for route injection.

`http://packetlife.net/blog/2009/jul/6/remotely-triggered-black-hole-rtbh-routing/`

`https://ripe65.ripe.net/presentations/285-inex-ripe-routingwg-amsterdam-2012-09-27.pdf`

`https://www.inex.ie/rtbh`

Remember those BGP import filters, perhaps try bgpq3

```
hlk@katana:bgpq3-0.1.16$ ./bgpq3 -Jl larsen-data AS197495
policy-options {
replace:
 prefix-list larsen-data {
     91.221.196.0/23;
     185.10.8.0/22;
 }
}
```

http://snar.spb.ru/prog/bgpq3/

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

DDoS in 2014

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.

Proxy servers - protection services

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/

Focus for the near future

Walk through your infrastructure
get a detailed view of data, flows, protocols, bandwidth, ports and services

Make sure your organization is also in control, know your vendors

Create a list of critical phone numbers and contacts, enter it in your phone

Get control of BYOD Bring Your Own Devices

History - summer 2013

DNS: DNSSEC, TCP queries, IPv6 DNS, DNS reply-size testing

More IPv6:

Automatic BGP blackhole routing, perhaps based on input from Suricata/Bro

Conferences:
RIPE66 Dublin hardcore network people `https://ripe66.ripe.net/`
OHM2013 Observe Hack Make `http://ohm2013.org/`

Near future - summer 2014

DNS: DNSSEC, DNS statistics, DNS abuse, DNS rate limiting
Now part of the censurfridns/uncensoredDNS admin group, yay!

More IPv6: Have turned on IPv6 on customer interfaces, now get them to use it.

Automatic BGP blackhole routing, perhaps based on input from Suricata/Bro

Conferences: definitely TheCamp this summer, perhaps RIPE in Autumn

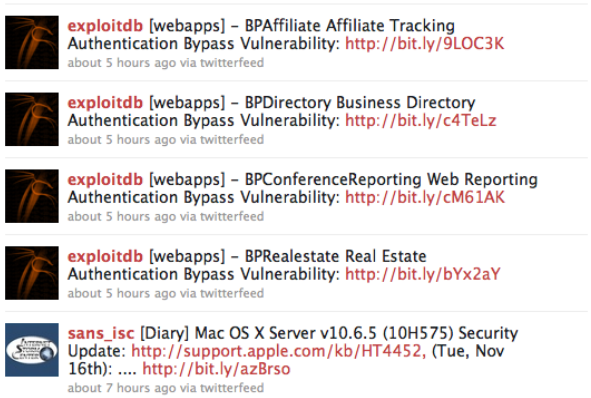
PROSA CTF

PROSA afholder i samarbejde med en mindre gruppe CTF konkurrencer

Robert Chris Larsen er hovedmanden - og tak til ham!

Kilde: `http://ctf2013.the-playground.dk/`

Sources for information



Twitter has replaced RSS for me

Email lists are still a good source of data

Favourite Security Diary from Internet Storm Center

`http://isc.sans.edu/index.html`

`https://isc.sans.edu/diaryarchive.html?year=2013&month=4`

Open Mike night ...

what did I forget? tells us about your favourites ☺

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?

SOLIDO NETWORKS

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

You are always welcome to send me questions later via email