How we Collaborate and Share

FIRST TC, Kyoto

Wim Biemolt
SURFcert – November 14th, 2012

Oudemirdum

24	Willem Biemolt	Utrecht	Geen	1.13.43	M40.11

Kyoto?

Collaboration!

SURFnet

SERVICES AND INNOVATIONS

SURFnet helps researchers, teachers and students work together using ICT. See the complete overview of services.

SURFnet focusses on the following areas:

Network infrastructure

Have fast and secure internet via the innovative network of SURFnet >

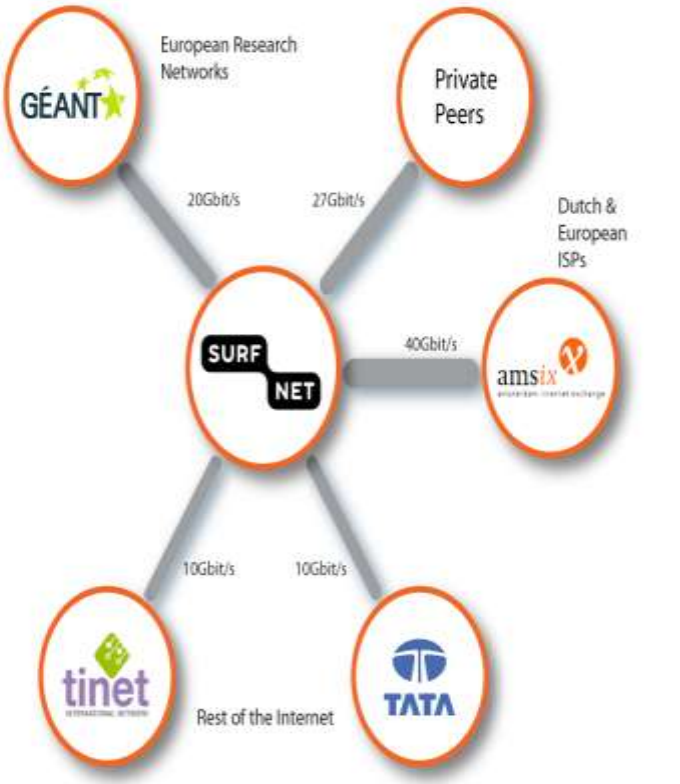
SURFinternet / SURFlichtpaden / SURFdomeinen / SURFinternetpinnen / eduroam / more

Collaboration infrastructure

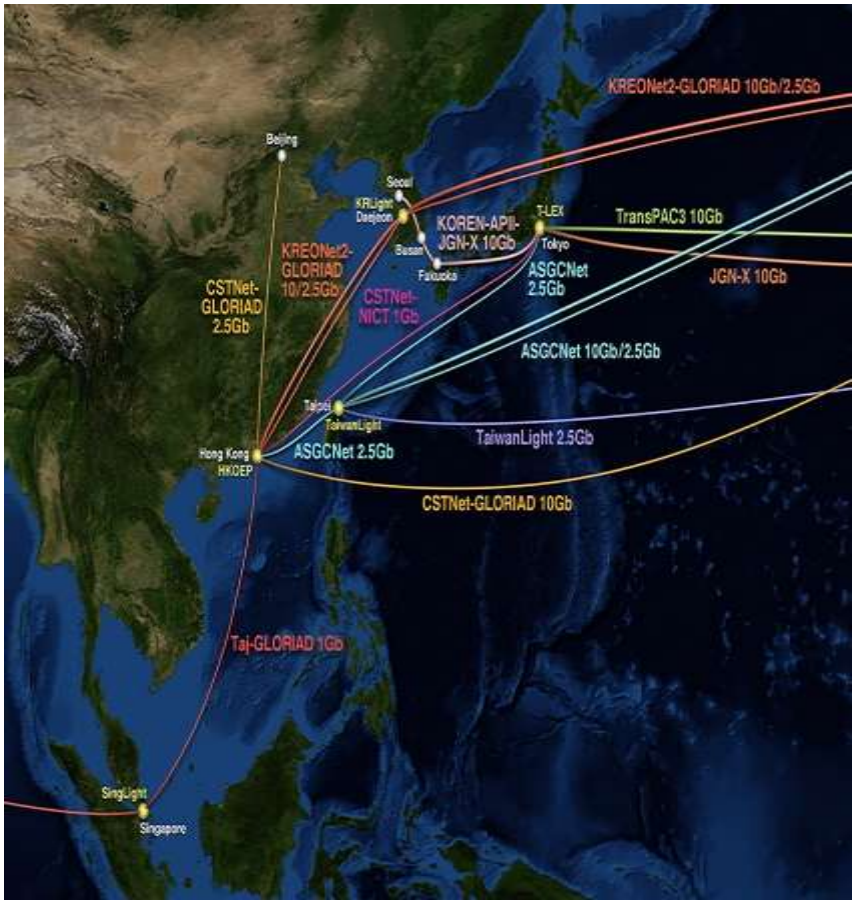
Online collaboration is getting easier. Information sharing, conferencing, email, appointments and more >

SURFconext / SURFcontact / Unified Communications / MediaMosa / more

Global connectivity

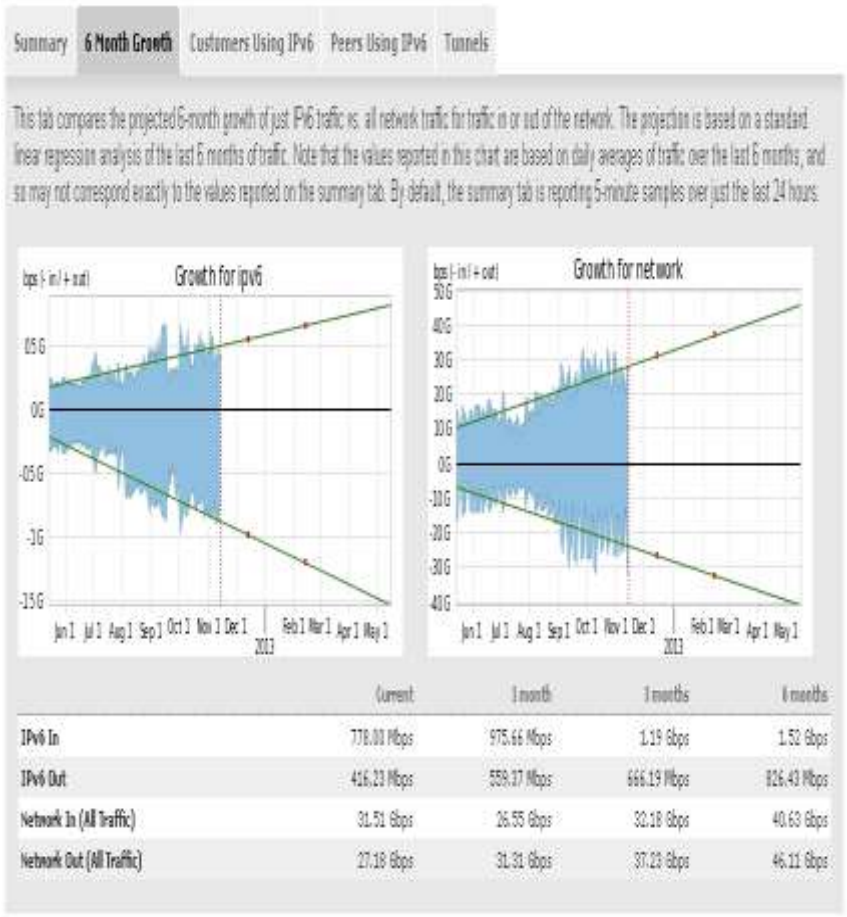


Global IP connectivity - October 2010



IPv6


Summary
6 Month Growth
Customers Using IPv6
Peers Using IPv6
Tunnels
DETAILS
Period: Today
Update
This dashboard analyzes IPv6 traffic passing in or out of the network. It includes both native IPv6 traffic as well as tunneled traffic such as Teredo and IP protocol 41 traffic. The IPv6 share of all network traffic is calculated based on the most recent ("Current") measurement.
bps [-in/+out]
Nov 2012
Wed 14
native
teredo
proto41
Current IPv6 traffic:
887.6 Mbps
IPv6 share of all network traffic:
2.5%
Maximum:
4.7 Gbps
Average traffic:
1.2 Gbps
95th Percentile:
2.2 Gbps
Number of Customers Using IPv6: 184
Number of Peers Using IPv6: 1


Summary
6 Month Growth
Customers Using IPv6
Peers Using IPv6
Tunnels
This tab compares the projected 6-month growth of just IPv6 traffic vs. all network traffic for traffic in or out of the network. The projection is based on a standard linear regression analysis of the last 6 months of traffic. Note that the values reported in this chart are based on daily averages of traffic over the last 6 months, and so may not correspond exactly to the values reported on the summary tab. By default, the summary tab is reporting 5-minute samples over just the last 24 hours.
Growth for ipv6
bps [-in/+out]
Growth for network
bps [-in/+out]
Current
1 month
3 months
6 months
IPv6 In
778.03 Mbps
975.66 Mbps
1.19 Gbps
1.52 Gbps
IPv6 Out
416.23 Mbps
559.37 Mbps
666.19 Mbps
826.43 Mbps
Network In (All Traffic)
31.51 Gbps
26.55 Gbps
32.18 Gbps
40.63 Gbps
Network Out (All Traffic)
27.18 Gbps
31.31 Gbps
37.23 Gbps
46.11 Gbps

Security

DNSSEC

« ION Mumbai: A Raging Success! Four IPv6 Sessions Coming Up at IETF 85 in Atlanta »

Excellent whitepaper/tutorial from SURFnet on deploying DNSSEC-validating DNS servers

How do you get started with deploying DNSSEC-validating DNS servers on your network? What kind of planning should you undertake? What are the steps you need to go through?

The team over at SURFnet in the Netherlands recently released an excellent whitepaper that goes into the importance of setting up DNSSEC validation, the requirements for using validation, the planning process you should use, etc.

As we note on our resource page about the whitepaper, the document then walks through the specific steps for setting up DNSSEC validation in three of the common DNS resolvers:

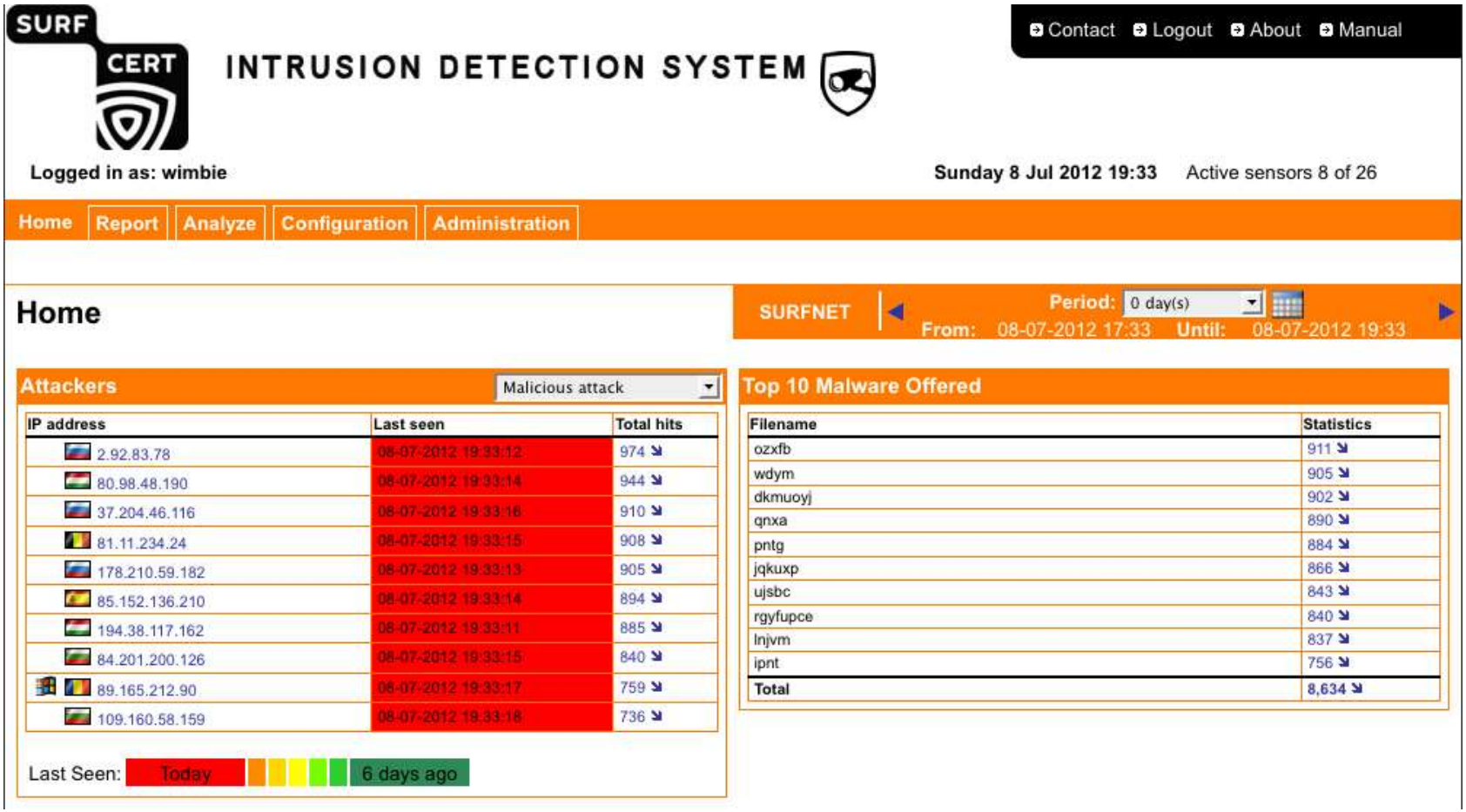
- BIND 9.x
- Unbound
- Microsoft Windows Server 2012

For us to get DNSSEC widely available we need to have DNS resolvers on networks performing the actual validation of DNS queries using DNSSEC. This guide is a great way to get started.

Have you enabled DNSSEC validation on your network?

http://www.internetsociety.org/deploy360/blog/2012/10/excellent-whitepapertutorial-from-surfnet-on-deploying-dnssec-validating-dns-servers/

SURFcert IDS



Changing threats

SpamPot

Last 15-minutes snapshot: targ-NL-01

Period: 2012-09-17 (21h15) to 2012-09-17 (21h30) GMT

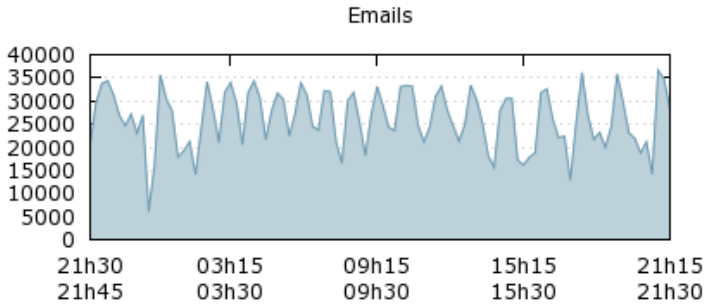
| Country Codes | AS Numbers | Protocols | Ports | Source OSs | Domains | ⇒ more details: CIDR blocks and IP addresses

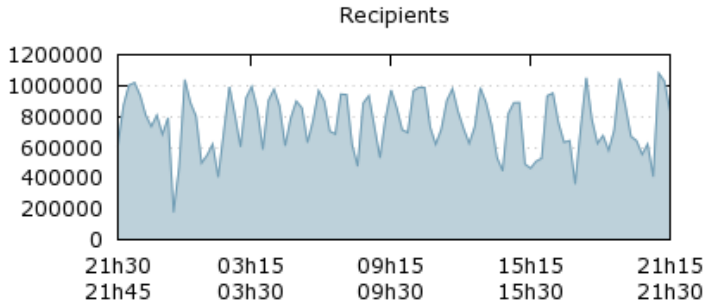
cert.br
Computer Emergency Response Team - Brazil

Summary

Category	Counter	Category	Counter	Category	Counter
Unique Country Codes	15	Emails received	28,269	Message size (max)	195.42 kB
Unique ASNs	30	Recipients targetted	831,951	Message size (avg)	3.88 kB
Unique CIDRs	53	Rcpt domains	1,053	Connections	3,867
Unique IPs	183	Rcpt domains / msg (max)	2	Protocols	4
Source OS fingerprints	6	Rcpt domains / msg (avg)	1.00	Destination ports	3

Graphics showing the number of emails & recipients over the last 24 hours (in chunks of 15 minutes).





SURF NET

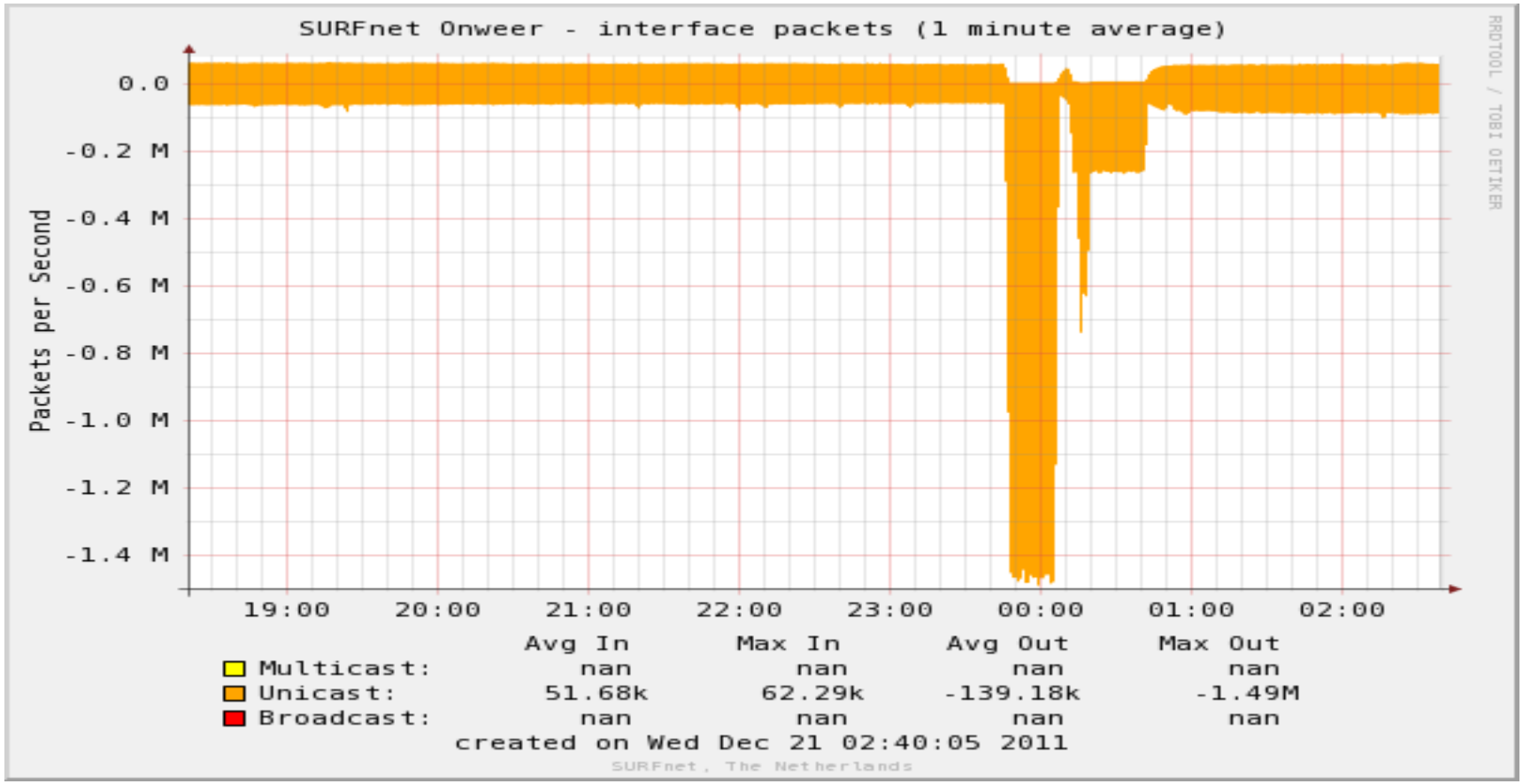
Fantastic!

However …

Packet love


SPAMHAUS
THE SPAMHAUS PROJECT
Home
SBL
XBL
PBL
DBL
DROP
ROKSO
WHITELIST
Blocklist Removal Center
Contacts | Official Statements | Sponsors | FAQs | News Blog
Spamhaus Project Sponsors
Project Sponsors
These organizations maintain our free Public DNSBL servers around the world, and/or provide free service and technical expertise to Spamhaus.
The Spamhaus Project, and the millions of Internet users whose email mailboxes are protected using Spamhaus's free public anti-spam filter systems, owe a special thanks to these organizations.
Bell
ja.net
XS4ALL
1&1
servercentral
BLACKNIGHT SOLUTIONS
ISC
vodafone
SURF NET

SNMP


SURFnet Onweer - interface packets (1 minute average)
Packets per Second
0.0
-0.2 M
-0.4 M
-0.6 M
-0.8 M
-1.0 M
-1.2 M
-1.4 M
19:00
20:00
21:00
22:00
23:00
00:00
01:00
02:00
RRDTOOL / TOBI OETIKER
Avg In Max In Avg Out Max Out
Multicast: nan nan nan nan
Unicast: 51.68k 62.29k -139.18k -1.49M
Broadcast: nan nan nan nan
created on Wed Dec 21 02:40:05 2011
SURFnet, The Netherlands

Secret

OPERATIONS SECURITY TRUST

Login

Mission

OPSEC-Trust (or "ops-trust") forum is a highly vetted community of security professionals focused on the operational robustness, integrity, and security of the Internet. The community promotes responsible action against malicious behavior beyond just observation, analysis and research. OPSEC-Trust carefully expands membership pulling talent from many other security forums looking for strong vetting with in three areas:

1. sphere of trust;
2. sphere of action;
3. the ability to maintain a "need to know" confidentiality.

OPSEC-Trust (or "ops-trust") members are in a position to directly affect Internet security operations in some meaningful way. The community's members span the breadth of the industry including service providers, equipment vendors, financial institutions, mail admins, DNS admins, DNS registrars, content hosting providers, law enforcement organizations/agencies, CSIRT Teams, and third party organizations that provide security-related services for public benefit (e.g. monitoring or filtering service providers). The breadth of membership, along with an action plus trust vetting approach creates a community which would be in a position to apply focused attention on the malfeasant behaviors which threaten the Internet.

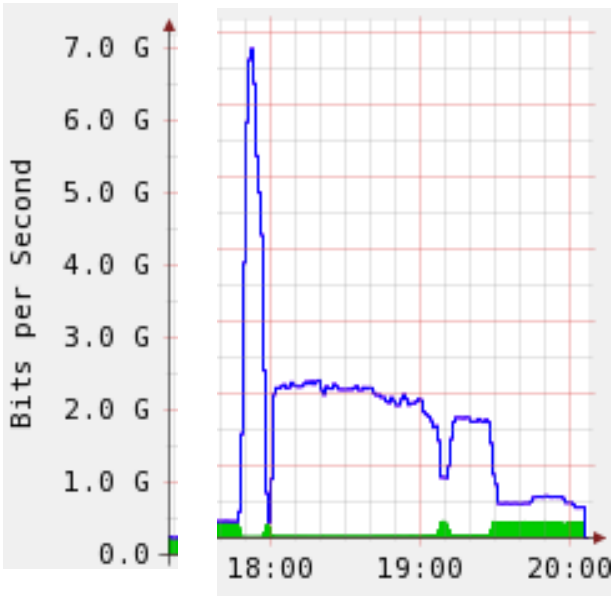
Members:

- will be privy to lists of infected IP addresses, compromised accounts, bot c&c lists and other data that should be acted upon.
- are expected to take appropriate action within their domain of control.
- are expected to contribute data as appropriate and in a fashion that does not violate any laws or corporate policies.

OPSEC-Trust does not accept applications for membership. New candidates are nominated by their peers who are actively working with them on improving the operational robustness, integrity, and security of the Internet.

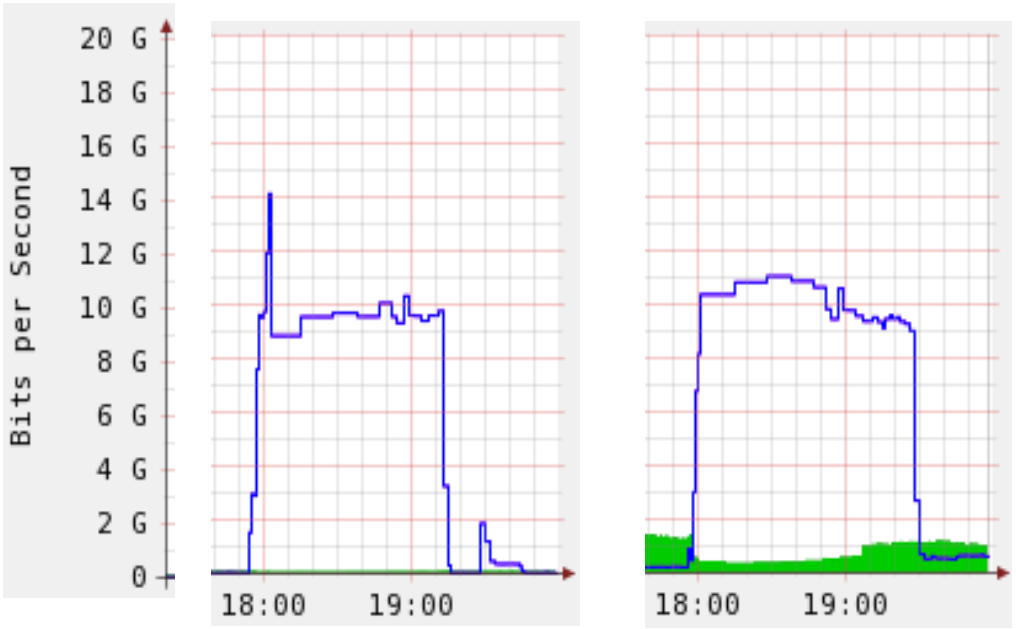
DNS

onweer



Amsterdam

service LAN

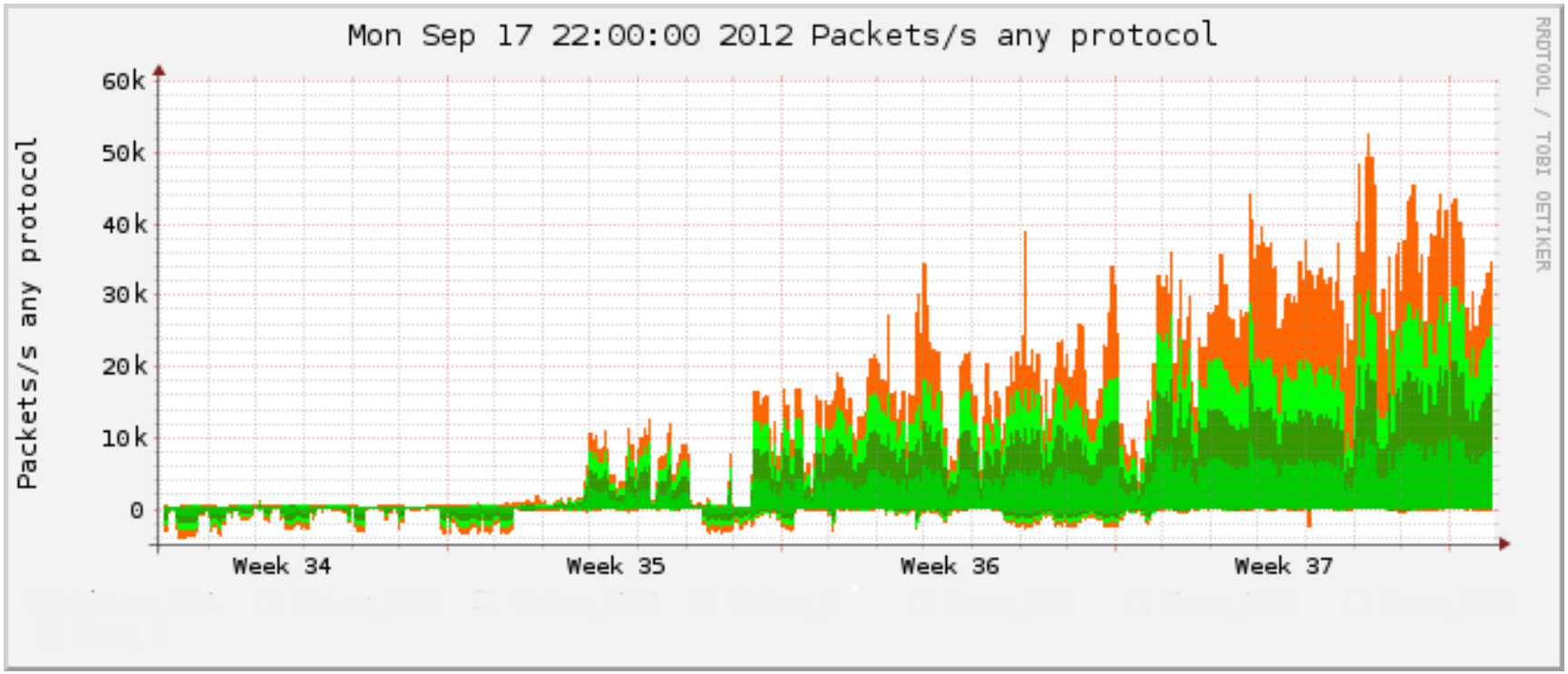


Nijmegen

Amsterdam

What is happening?

Abuse

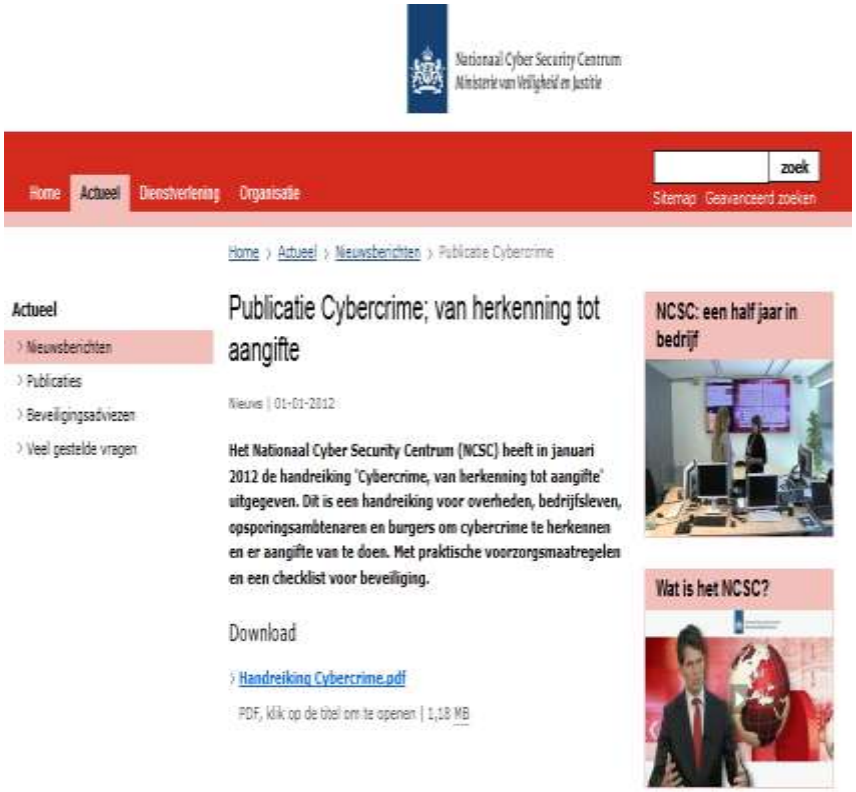

Mon Sep 17 22:00:00 2012 Packets/s any protocol
Packets/s any protocol
60k
50k
40k
30k
20k
10k
0
Week 34
Week 35
Week 36
Week 37
RRDTOOL / TOBI OETIKER

Partners in crime

amsix
amsterdam internet exchange

Report the crime

Very useful


Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie
Home
Actueel
Dienstverlening
Organisatie
zoek
Sitemap Geavanceerd zoeken
Home › Actueel › Nieuwsberichten › Publicatie Cybercrime
Actueel
› Nieuwsberichten
› Publicaties
› Beveiligingsadviezen
› Veel gestelde vragen
Publicatie Cybercrime; van herkenning tot aangifte
Nieuws | 01-01-2012
Het Nationaal Cyber Security Centrum (NCSC) heeft in januari 2012 de handreiking 'Cybercrime, van herkenning tot aangifte' uitgegeven. Dit is een handreiking voor overheden, bedrijfsleven, opsporingsambtenaren en burgers om cybercrime te herkennen en er aangifte van te doen. Met praktische voorzorgsmaatregelen en een checklist voor beveiliging.
Download
› Handreiking Cybercrime.pdf
PDF, klik op de titel om te openen | 1,18 MB
NCSC: een half jaar in bedrijf
Wat is het NCSC?


Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie
Cybercrime
Van herkenning tot aangifte

Measures

TMS


ARBOR Peakflow SP
23:11:15 CET | 12/21/2011
Logged in as: wimbie
System
Alerts
Explore
Reports
Mitigation
Administration
MY ACCOUNT
HELP
LOGOUT
IPv4 TMS Mitigation Status
DOWNLOAD
EMAIL
PRINT
Summary
Name: DoS Alert 417214
Alert: 417214
Prefixes: 145.145.19.14/32
Template: Default IPv4
TMS Group: All
Managed Object: SURFNET
Start Time: 20:55, Dec 21
Stop Time: 23:11, Dec 21
Edit
Start
Stop
bps
pps
Summary
30 Minutes
5 Minutes
1.5 Gbps
1.0 Gbps
500 Mbps
0 bps
22:41:00
22:46:00
22:51:00
22:56:00
23:01:00
23:06:00
23:11
Pass bps
Drop bps
Total
Per TMS
Per Countermeasure
1 Minute
5 Minute
Summary
Dropped: 37.8 Mbps / 3.2 Kpps
660.6 Mbps / 61.8 Kpps
1.8 Gbps / 171.4 Kpps
Passed: 371.4 Kbps / 24.6 pps
549.5 Kbps / 80.2 pps
32.8 Mbps / 3.4 Kpps
Total: 38.1 Mbps / 3.3 Kpps
661.1 Mbps / 61.9 Kpps
1.8 Gbps / 174.8 Kpps
Percent Dropped: 99.03%
99.92%
98.18%
Average Blocked Hosts: 0 hosts
0.2 hosts
0.0 hosts
Download Blocked Hosts
Download Top Blocked Hosts
Countermeasures
Timeframe: Summary
Graph Unit: bps
Sample Packets
Status Countermeasure
Dropped
Passed
ON Invalid Packets 1.6 Gbps 155.9 Kpps
OFF IPv4 Address Filter Lists
ON IPv6 Black/White Lists
OFF IP Location Filter Lists
ON Zombie Detection
ON TCP SYN Authentication
OFF DNS Scoping
ON DNS Authentication
ON TCP Connection Reset
OFF Payload Regular Expression
OFF Source /24 Baselines
OFF Protocol Baselines
ON DNS Malformed
OFF DNS Rate Limiting
OFF DNS NXDomain Rate Limiting
OFF DNS Regular Expression
ON HTTP Malformed
OFF HTTP Scoping
ON HTTP Rate Limiting
OFF HTTP/URL Regular Expression
ON SIP Malformed 2.6 Kbps 0.2 pps
ON SIP Request Limiting
OFF Shaping
OFF IP Location Policing

SURF NET

SURFcert

NETFLOW CERTIFIED SPECIALISTS

Party!

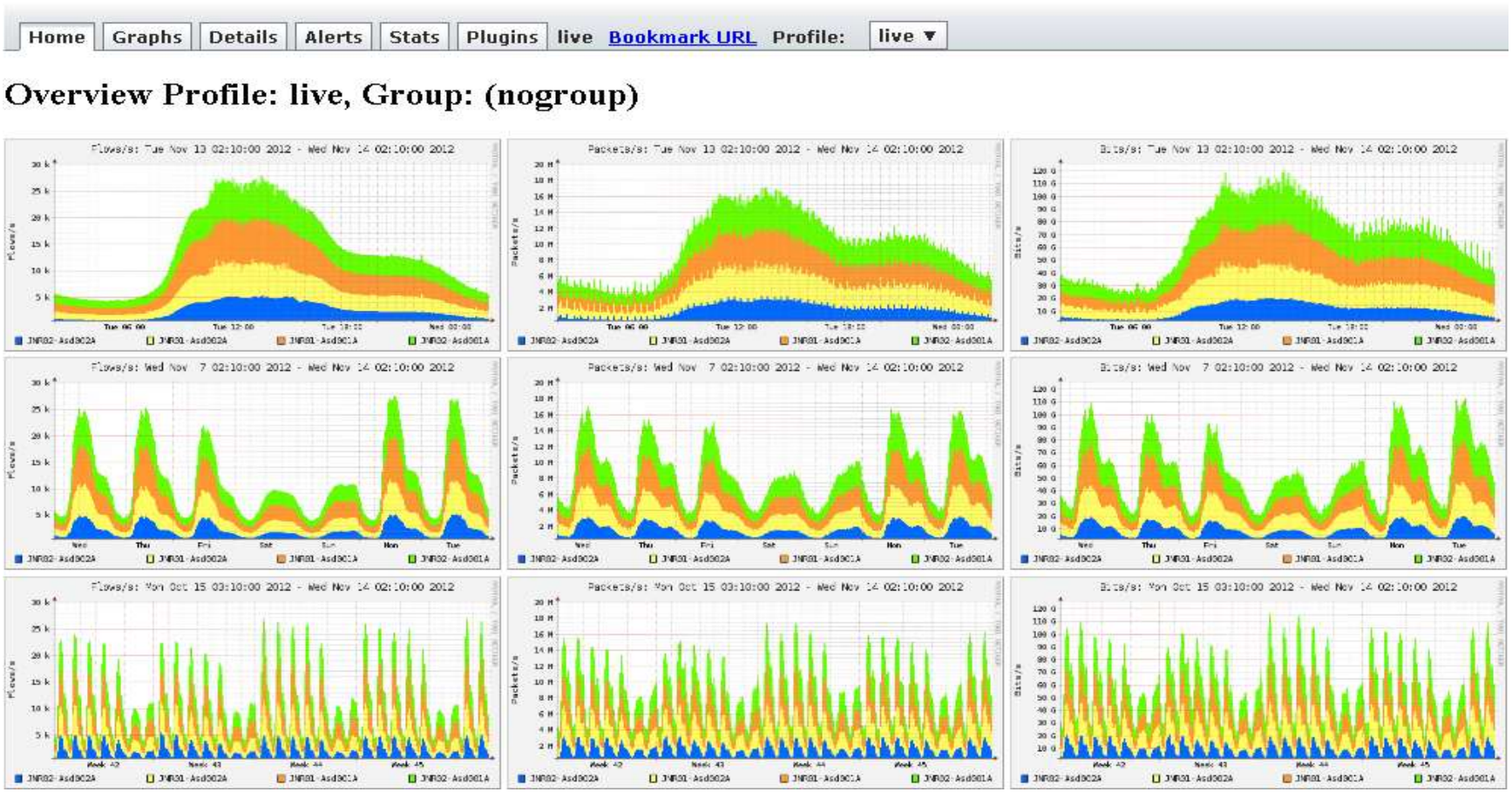
How?

5

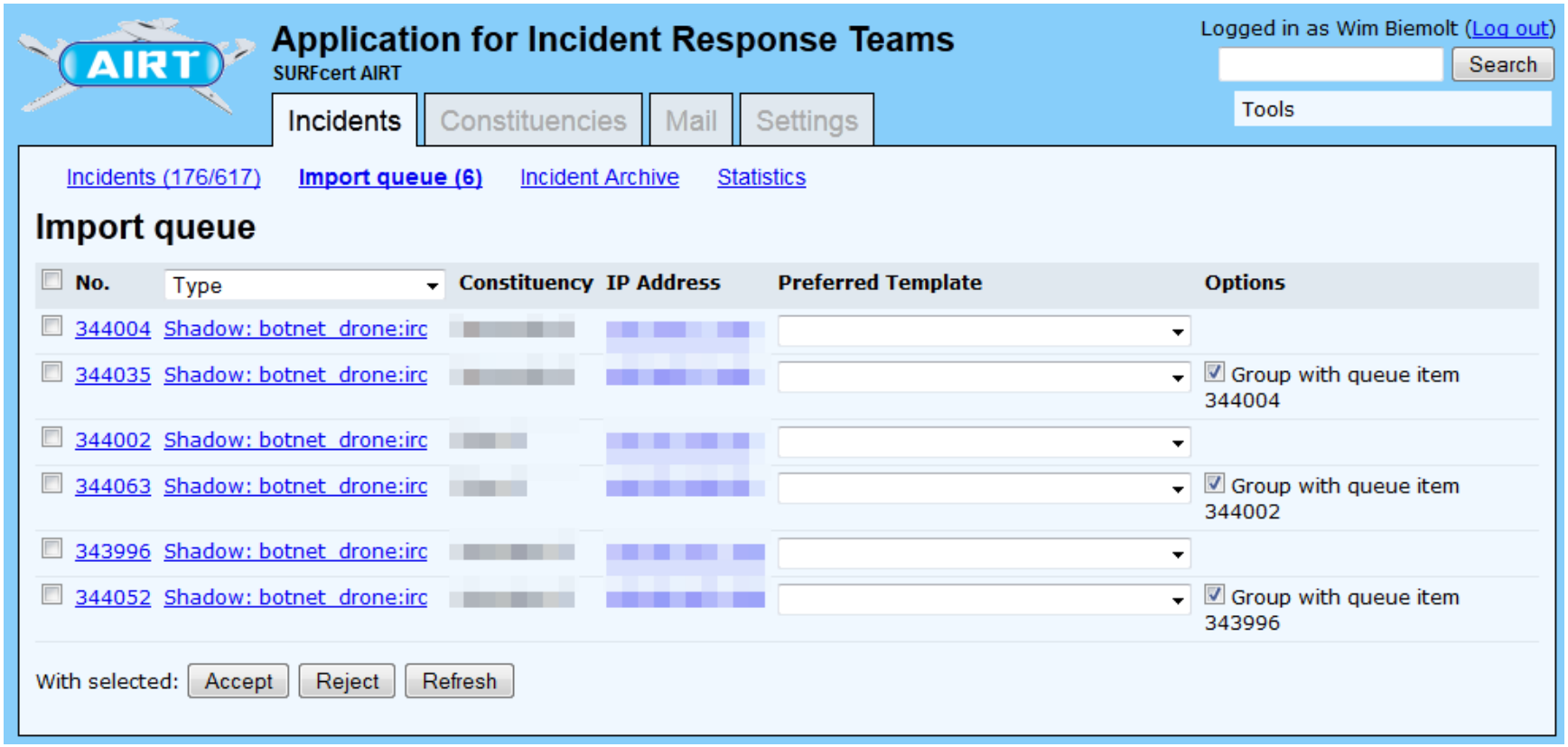
SURF NET

5

netflow


Home
Graphs
Details
Alerts
Stats
Plugins
live
Bookmark URL
Profile:
live
Overview Profile: live, Group: (nogroup)

AIRT

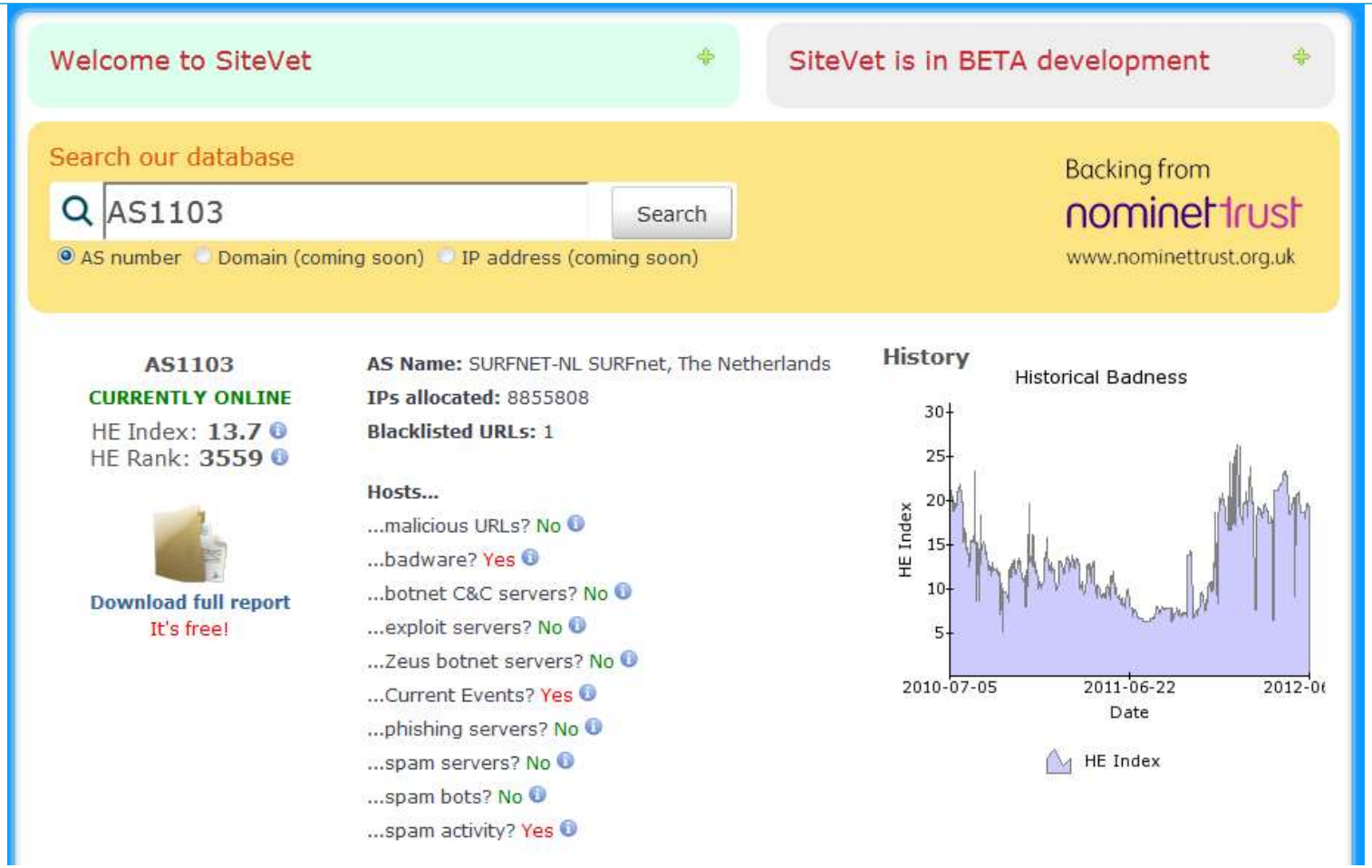


SURF NET

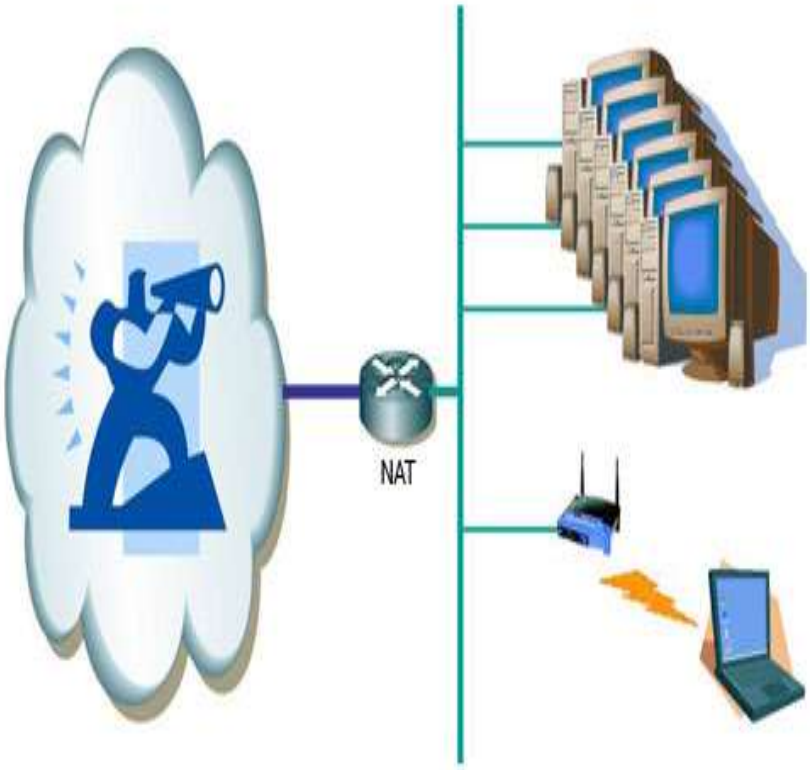
Incidents

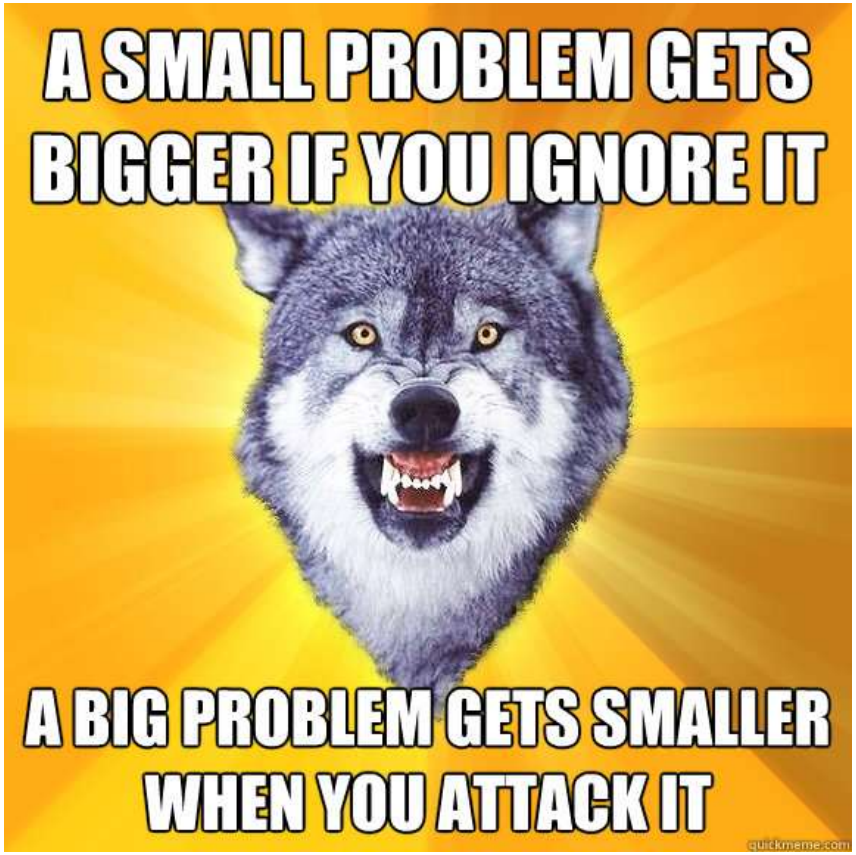
	2010	2011	2012 (H1)
Infected	2531	6373	1948
Probe	36	41	9
Spam	2597	1379	360
Content	6	6	6
Abusive	1	19	4
Denial	807	244	106
Vulnerable	1285	997	510
TOTAAL	7263	9059	2943

Good job!


Welcome to SiteVet
SiteVet is in BETA development
Search our database
AS1103
Search
AS number
Domain (coming soon)
IP address (coming soon)
Backing from
nominet trust
www.nominettrust.org.uk
AS1103
CURRENTLY ONLINE
HE Index: 13.7
HE Rank: 3559
Download full report
It's free!
AS Name: SURFNET-NL SURFnet, The Netherlands
IPs allocated: 8855808
Blacklisted URLs: 1
Hosts...
...malicious URLs? No
...badware? Yes
...botnet C&C servers? No
...exploit servers? No
...Zeus botnet servers? No
...Current Events? Yes
...phishing servers? No
...spam servers? No
...spam bots? No
...spam activity? Yes
History
Historical Badness
HE Index
30
25
20
15
10
5
2010-07-05
2011-06-22
Date
HE Index

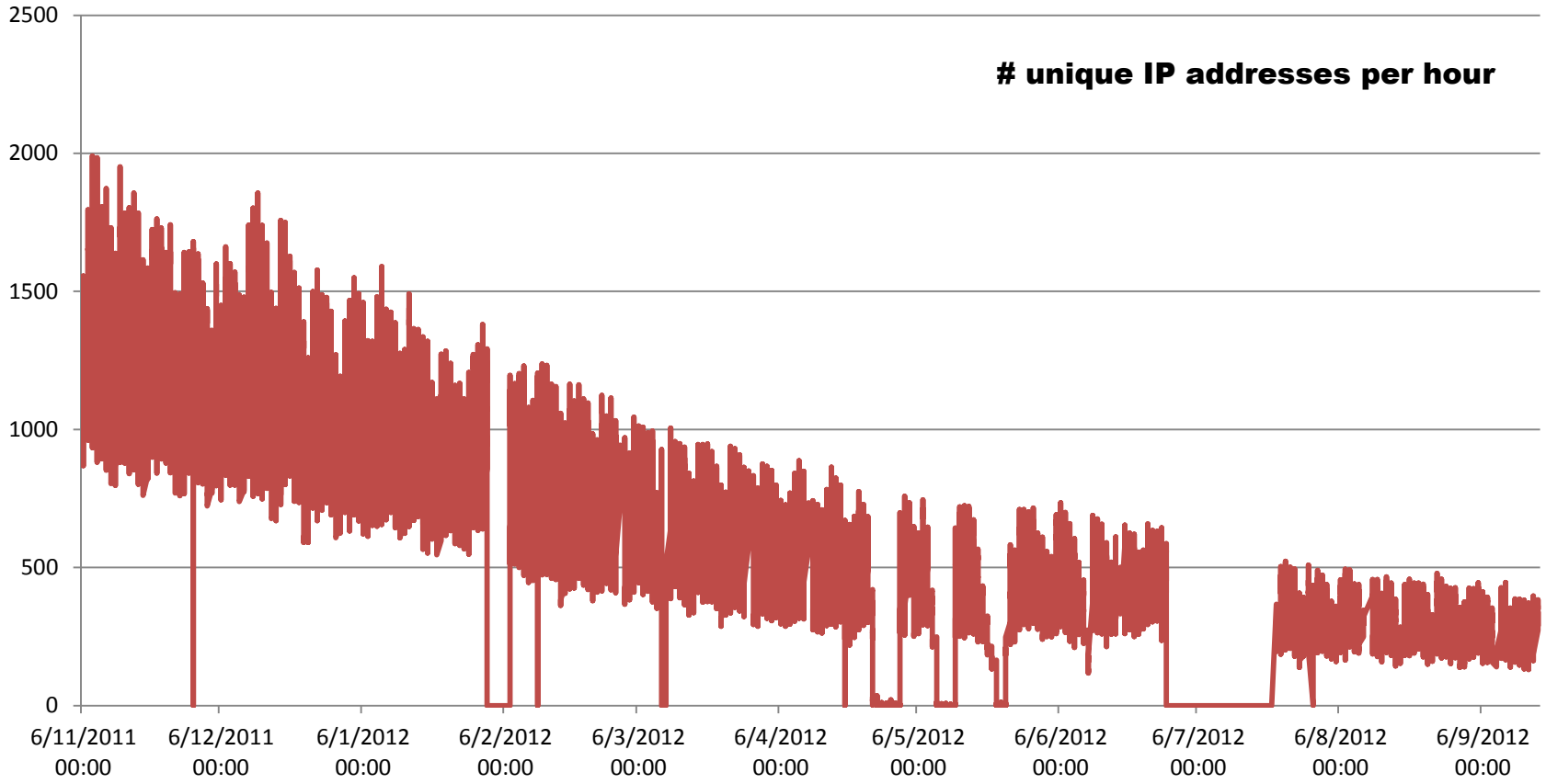
NAT


NAT


A SMALL PROBLEM GETS BIGGER IF YOU IGNORE IT
A BIG PROBLEM GETS SMALLER WHEN YOU ATTACK IT
quickmeme.com

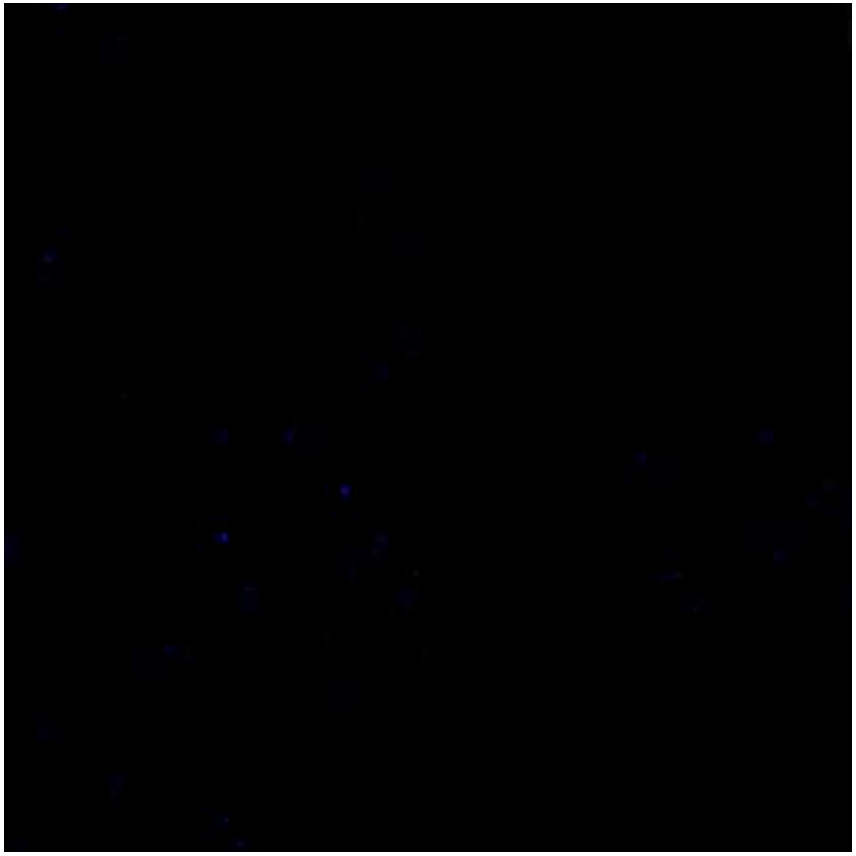
Is that everything?

Hlux/Kelihos Botnet

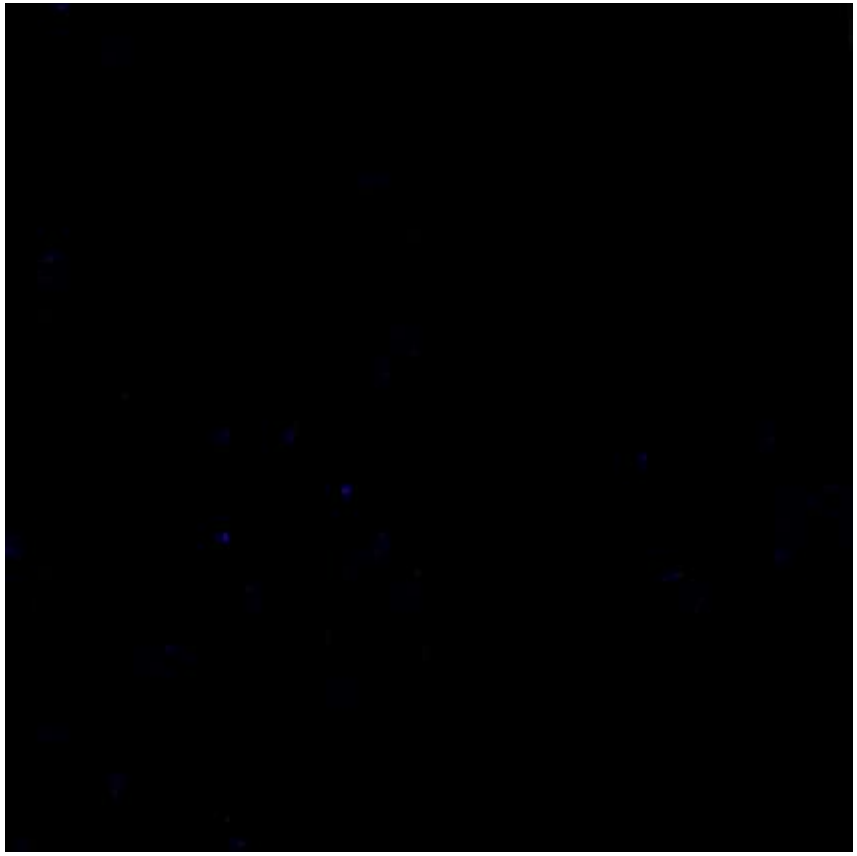


IPv4 Heatmap

September 2012



October 2012

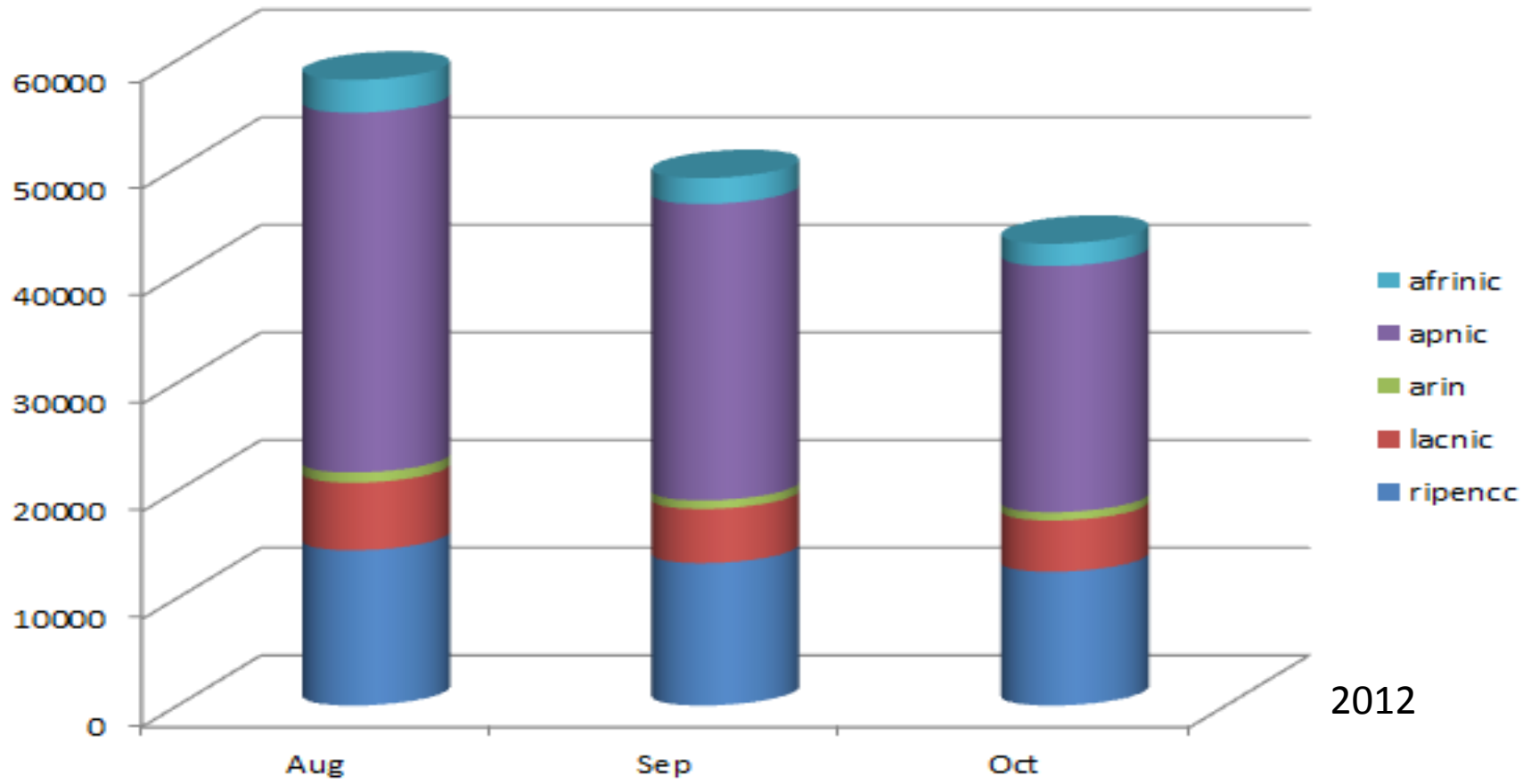


Google maps

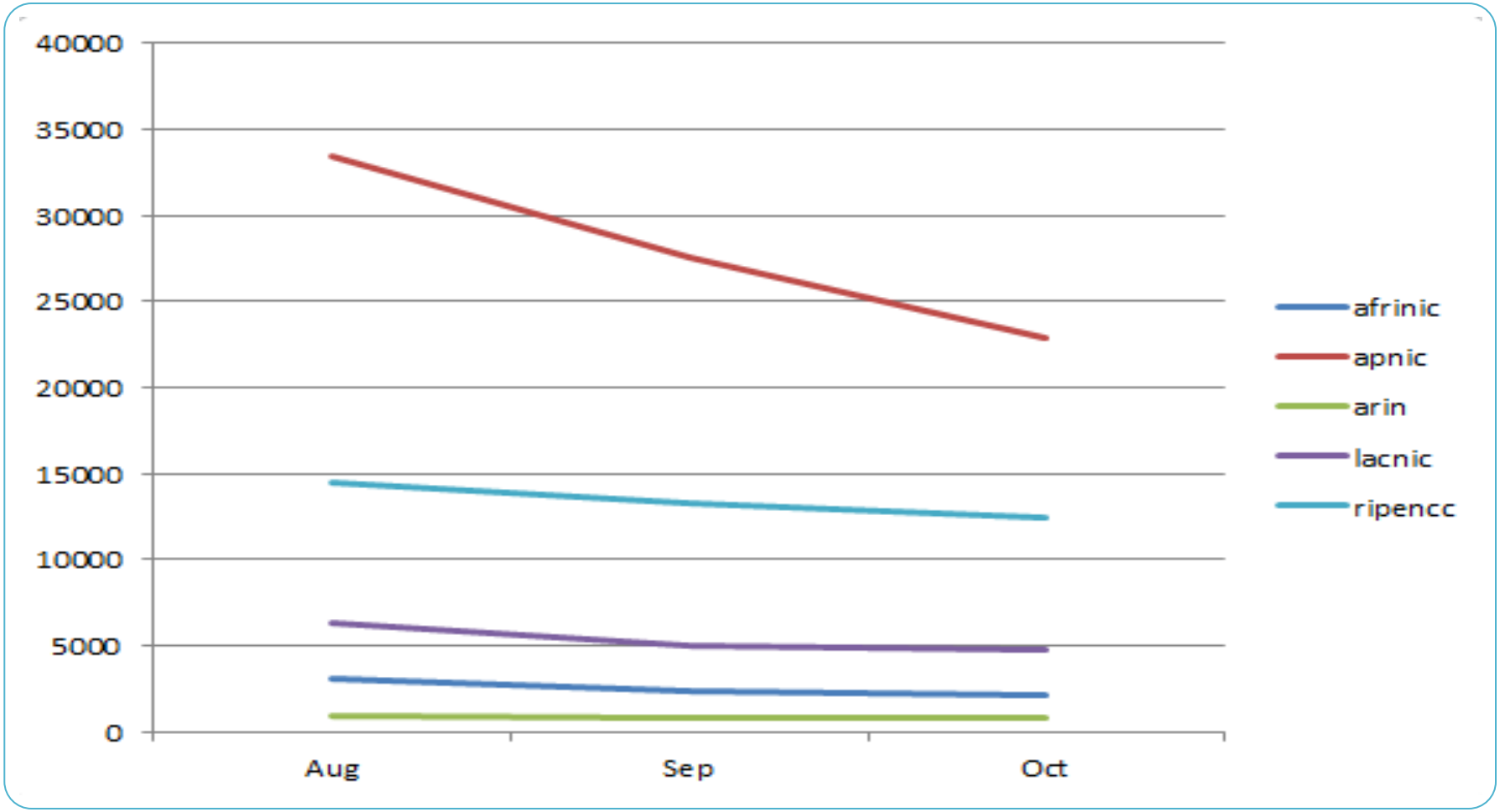
September 2012

October 2012

Region


60000
50000
40000
30000
20000
10000
0
Aug
Sep
Oct
afrinic
apnic
arin
lacnic
ripencc
2012

Slow decline



Abuse Information Exchange

Abuse Information Exchange takes on botnets

24 October 2012

Intensive collaboration between Dutch ISPs and SIDN to tackle botnets

The Hague, 24 October 2012 – Seven Dutch internet service providers have linked up with SIDN to cut the number of their clients' computers snared in botnets. Through the Abuse Information Exchange the group's members will gather and analyse information about botnets centrally. The approach should mean that hijacked computers are detected sooner and help made available to clients at an earlier stage. The net result should be more effective botnet suppression and even greater internet security for the Netherlands. Abuse Information Exchange is expected to be up and running by the start of 2013.

Up to 10% of all computers infected

Botnets are networks of computers that, unknown to their owners, have been infected with a virus or other malware, enabling someone else to control them. Botnets are widely used for sending spam and mounting cyber-attacks. In most cases, botnet software barely affects the infected computer. Consequently, the owners are often unaware that anything is wrong. However, the activities of botnets can cause a lot of harm and inconvenience to others. Research by Delft University of Technology suggests that between 5 and 10 per cent of all computers in the Netherlands have been recruited by botnets. Abuse Information Exchange is determined to get that figure down.

Strength in numbers

Abuse Information Exchange is a joint initiative by the internet service providers KPN, SOLCON, Tele2, UPC, XS4ALL, Zeelandnet and Ziggo, plus SIDN –the company behind .nl domain names – and ECP, the Platform for the Information Society. Abuse Information Exchange will operate a portal, via which people can report botnet problems. The reports will then be analysed and the findings sent to the affiliated service providers. The providers with then have an up-to-date picture of reported infections in their network. Centralised data collection and analysis will enable ISPs to act more quickly and manage costs. At the moment, each individual ISP has to single-handedly gather, analyse and act on information about botnets.

Gert Wabeke, Chairman of Abuse Information Exchange, said, "The botnet problem is too big for any one provider to make inroads alone. However, by working closely together, we can achieve results." SIDN and the Ministry of Economic Affairs, Agriculture and Innovation endorse that view and are therefore backing the initiative financially by covering the cost of starting up the information system. SIDN will also provide technical management of the project.
"This initiative will mean less trouble from botnets for the business community and the general public, and will be a shot in the arm for internet security," Commented Maxime Verhagen, Dutch Minister of Economic Affairs, Agriculture and Innovation. "It's very important for the Dutch economy that ICT is secure and reliable to use."

Abuse Information Exchange strijdt tegen botnets

Door: XS4ALL | Gepubliceerd: 24 oktober 2012

Intensieve samenwerking Nederlandse ISP's en SIDN in bestrijding botnets
Zeven Nederlandse Internet Service Providers slaan samen met SIDN de handen ineen om het aantal besmette computers van hun klanten te verminderen. Onder de naam Abuse Information Exchange gaan de partijen informatie over botnetbesmettingen centraal verzamelen en verwerken. Door informatie centraal te ontvangen worden besmette computers sneller gedetecteerd en kunnen klanten beter en sneller geholpen worden. Daarmee kunnen botnets effectiever bestreden worden en wordt de internetveiligheid in Nederland verder verhoogd. Abuse Information Exchange zal naar verwachting tijdens het eerste kwartaal van 2013 operationeel worden.

Tot 10% van alle computers besmet

Botnets zijn netwerken van computers die zonder medeweten van hun eigenaar besmet zijn met een virus of andere kwaadaardige software. Ze kunnen daardoor door derden worden misbruikt. Botnets worden op grote schaal ingezet voor het versturen van spam en voor het uitvoeren van cyberaanvallen. De botnetsoftware zorgt op de besmette computer meestal voor weinig problemen; vaak wordt de besmetting helemaal niet opgemerkt. Maar botnets kunnen grote overlast en schade veroorzaken aan anderen. Volgens onderzoek van de TU Delft heeft 5 tot 10 % van consumenten jaarlijks te maken met een botnetinfectie, Abuse Information Exchange vindt dat dat percentage omlaag moet.

Slagkracht door samenwerking

Abuse Information Exchange is een initiatief van internetproviders KPN, SOLCON, Tele2, UPC, XS4ALL, Zeelandnet en Ziggo, van SIDN –het bedrijf achter de .nl-domeinnamen– en van ECP, Platform voor de Informatiesamenleving. De organisatie gaat meldingen over botnetbesmettingen via een loket verzamelen en sorteren en stuurt de informatie vervolgens door naar de aangesloten providers. De providers krijgen zo een actueel overzicht van meldingen over besmettingen in hun netwerk. Door deze centrale aanpak kunnen serviceproviders sneller schakelen en kosten besparen. Momenteel moet iedere ISP afzonderlijk de informatie over botnetbesmettingen verzamelen, analyseren en verder verwerken.
Gert Wabeke, voorzitter van Abuse Information Exchange: "Botnets vormen een probleem dat te groot is om door individuele providers aangepakt te worden. Door intensief samen te werken kunnen we een krachtige vuist vormen tegen botnets!" Het Ministerie van Economie, Landbouw en Innovatie en SIDN staan achter deze visie en ondersteunen het initiatief door, de opstartkosten van het informatiesysteem te financieren. SIDN zal ook het technisch beheer van Abuse IX uitvoeren.
"Deze aanpak zorgt voor minder overlast voor ondernemers en burgers en vergroot de veiligheid van internet" aldus minister Verhagen van EL&I. "Veilig en betrouwbaar gebruik van ICT is van groot belang voor de Nederlandse economie".

Uitbreiding

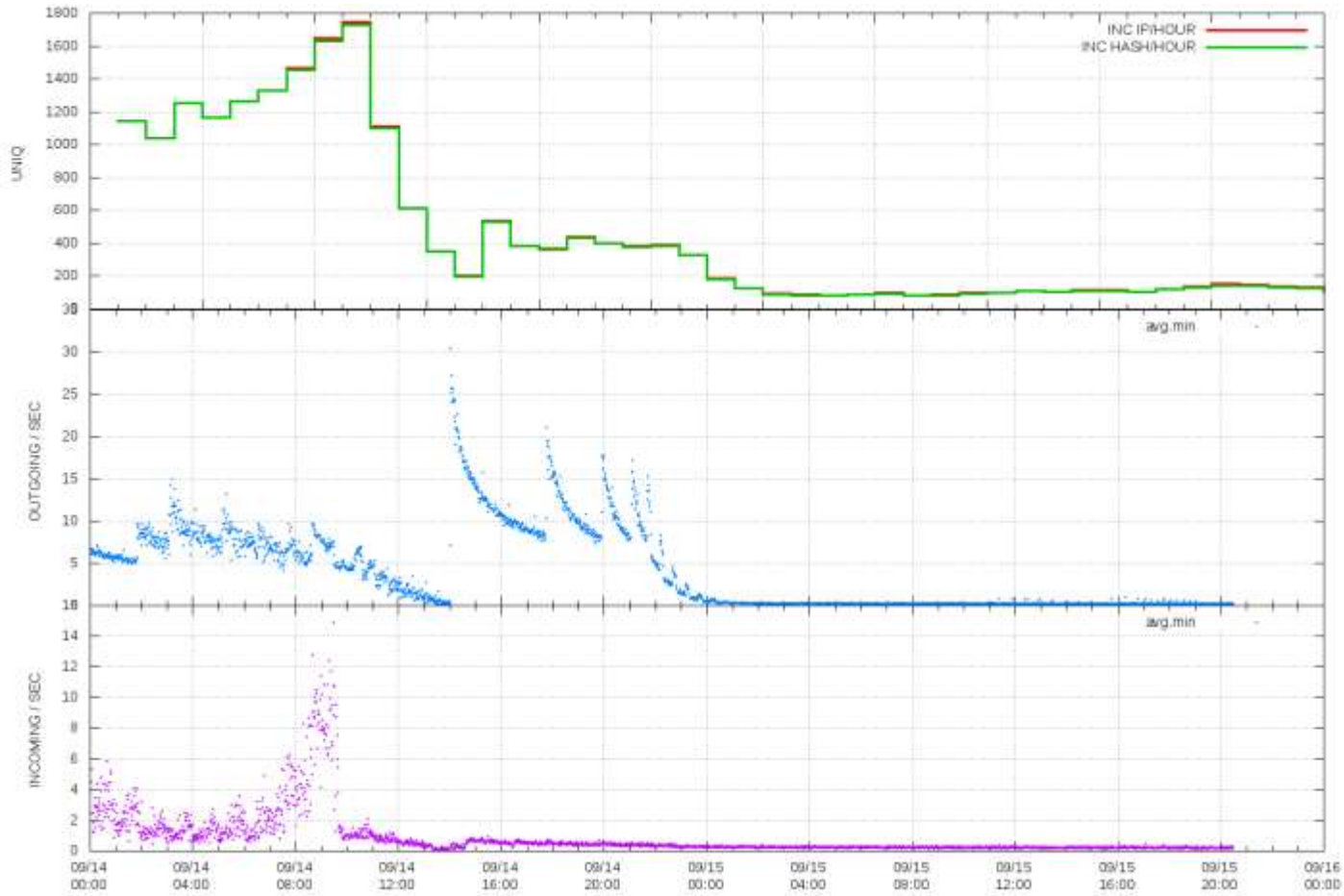
De ambitie van Abuse Information Exchange is het internet in Nederland zowel qua internettoegang als qua webdiensten veiliger te maken. De vereniging wil daarom uitbreiden en nodigt andere partijen zoals internetbedrijven, mobiele operators en hostingproviders uit zich bij het initiatief aan te sluiten.

SURF NET

2nd Hlux/Kelihos Botnet

Status

Zeus


INC IP/HOUR
INC HASH/HOUR
UNIQ
avg.min
OUTGOING / SEC
avg.min
INCOMING / SEC
09/14 00:00
09/14 04:00
09/14 08:00
09/14 12:00
09/14 16:00
09/14 20:00
09/15 00:00
09/15 04:00
09/15 08:00
09/15 12:00
09/15 16:00
09/15 20:00
09/16 00:00

Busy!

IP spoofing allowed?

Warning by executable

Nederlands | English

POLITIE
Korps landelijke politiediensten
Netherlands Police Agency

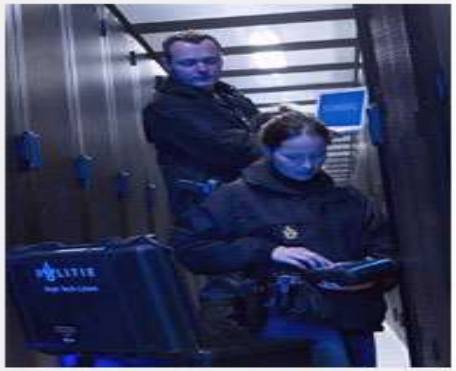
Home • Aangifte • Persbericht • Over de politie

Uw computer is besmet!

Als uw computer deze pagina automatisch heeft geopend, dan is het zeer waarschijnlijk dat uw computer is geïnfecteerd met malware en deel uit maakt van een botnetwerk.

Dit bericht wordt u aangeboden door het Team High Tech Crime van het Korps Landelijke Politiediensten (Nationale Recherche), met als doel eigenaren van geïnfecteerde computers te waarschuwen.

Nationale Recherche haalt berucht botnet neer
Het Team High Tech Crime (THTC) van de Nationale Recherche heeft maandagmiddag een berucht botnet neergehaald, dat sinds juli 2009 wereldwijd tenminste 30 miljoen computerinfecties heeft veroorzaakt. Het gaat om het Bredolab netwerk, dat door cybercriminelen wordt gebruikt om op grote schaal andere virussen te verspreiden en nieuwe botnets aan te maken.
In nauwe samenwerking met een Nederlandse hostingprovider, het Nederlands Forensisch Instituut (NFI), het internet security bedrijf Fox-IT en GOVCERT, het computer emergency response team van de Nederlandse overheid, zijn vandaag 143 computerservers afgesloten van het internet.



Waar kunt u meer informatie vinden:

Voor meer informatie over de infectie en het verwijderen ervan:
https://www.waarschuwingsdienst.nl/Risicos/Virussen+en+malware/Ontmanteling+Bredolab.html.

FOX-IT EXPERTS IN IT SECURITY GOVCERT.NL OPENBAAR MINISTERIE LANDELIJK PARKET POLITIE Korps landelijke politiediensten Netherlands Police Agency

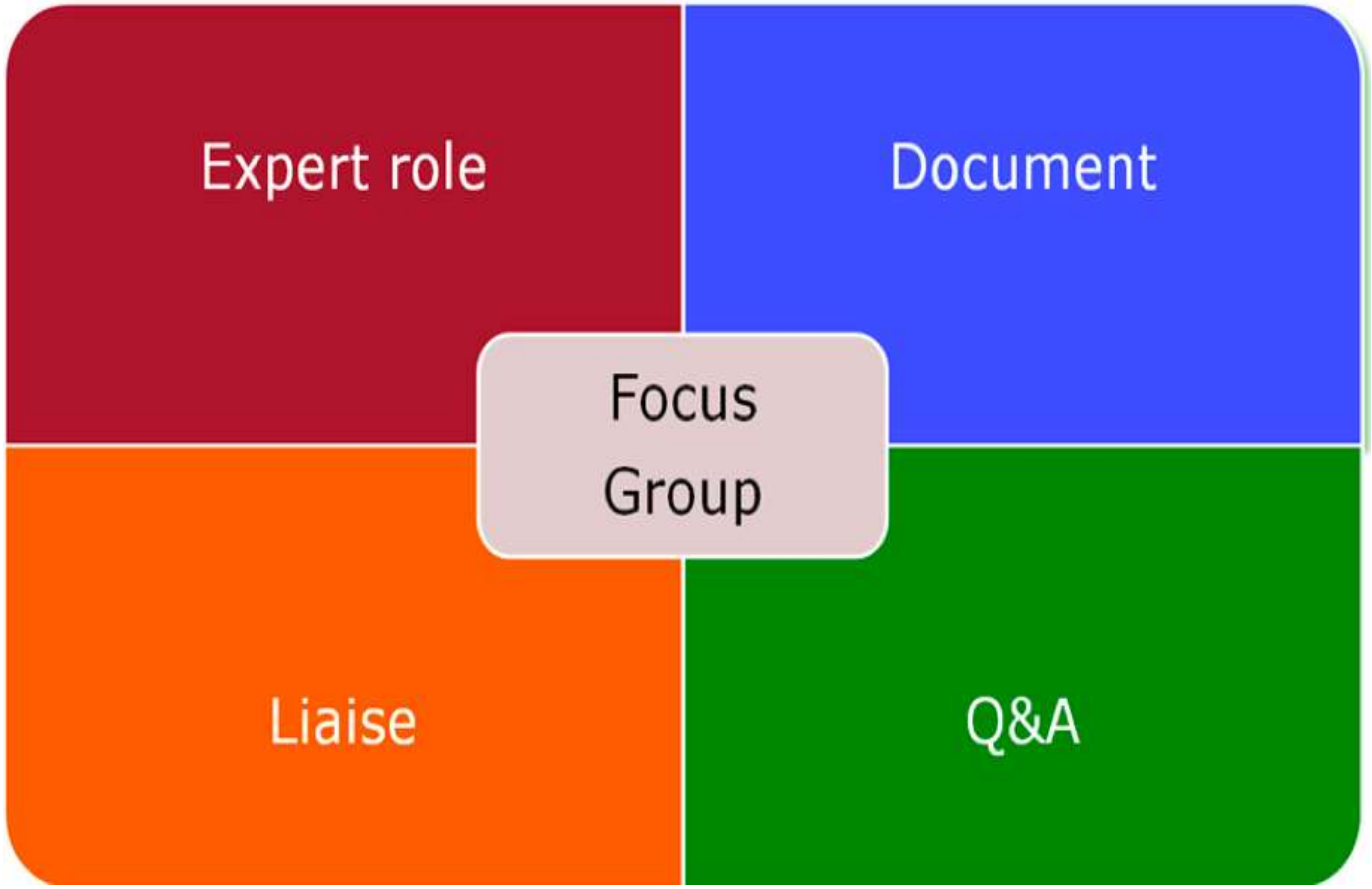
SURF NET

Favor?

Together strong

SCIRT

Goals



Focus

	Software audits		Risk management
	Juridical questions		Virtualization
	wifi		Malware analysis
	IPv6 security		Forensics
	Honeypot & IDS/IPS		Phising

MoU & TLP

Press

Tech / Internet

Gepubliceerd: 9 augustus 2012 14:22
Laatste update: 9 augustus 2012 20:19

Deel:

Dertien universiteiten getroffen door beveiligingslek

AMSTERDAM - Dertien universiteiten blijken kwetsbaar geweest te zijn voor een datalek in de website. In sommige gevallen waren persoonsgegevens toegankelijk.

Foto: Thinkstock

Dat ontdekten de scholieren Daiman en Olivier.

Tijdens het testen van de websites op kwetsbaarheden troffen de scholieren er tientallen aan. Iedere keer bleek het om eenzelfde type lek te gaan, een SQL-injectie.

Dat betekent dat er een zwakheid in de website zit waardoor gecommuniceerd kan worden met de database. Normaal is de database volledig afgeschermd.

De getroffen instellingen zijn de Radboud Universiteit, Rijksuniversiteit Groningen, TU Delft, Open Universiteit, Universiteit Twente en de universiteiten van Tilburg, Utrecht, Rotterdam, Wageningen, Amsterdam, Eindhoven, Maastricht en Leiden.

Na melding bij NU.nl zijn het National Cyber Security Center en het responseteam voor universiteiten SurfCERT ingeschakeld. Daarna hebben de universiteiten de tijd gekregen de lekken te dichten.

Door: NU.nl/Brenno de Winter

Dorifel


Docs
Search Docs
File Edit View Tools Help
Organize Burn New folder
Favorites
Desktop
Recent Places
Downloads
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
Name
Date modified
Type
Size
Contract.doc
8/9/2012 4:20 PM
Microsoft Word ...
408 KB
Contractrcs.doc
8/10/2012 9:00 AM
Screen saver
555 KB
OK
Contract.doc
INFECTED
Contractrcs.doc
2 items

Zeroaccess

Dutch national cooperation (o-IRT-o)

Since 2002

Sinowal

NRC Handelsblad verspreidde Banking Trojan

Vandaag, 13:02 door Redactie

De malware die vanochtend via de websites van het NRC Handelsblad werd verspreid blijkt een beruchte banking Trojan te zijn. Het gaat om de Sinowal-malware, speciaal ontwikkeld voor het stelen van geld van online bankrekening, zo blijkt uit analyse van het Nederlandse beveiligingsbedrijf SurfRight. Aanvallers wisten kwaadaardige advertenties met een exploit op de site te krijgen. Het ging om een exploit voor een recent gepatcht Java-lek.

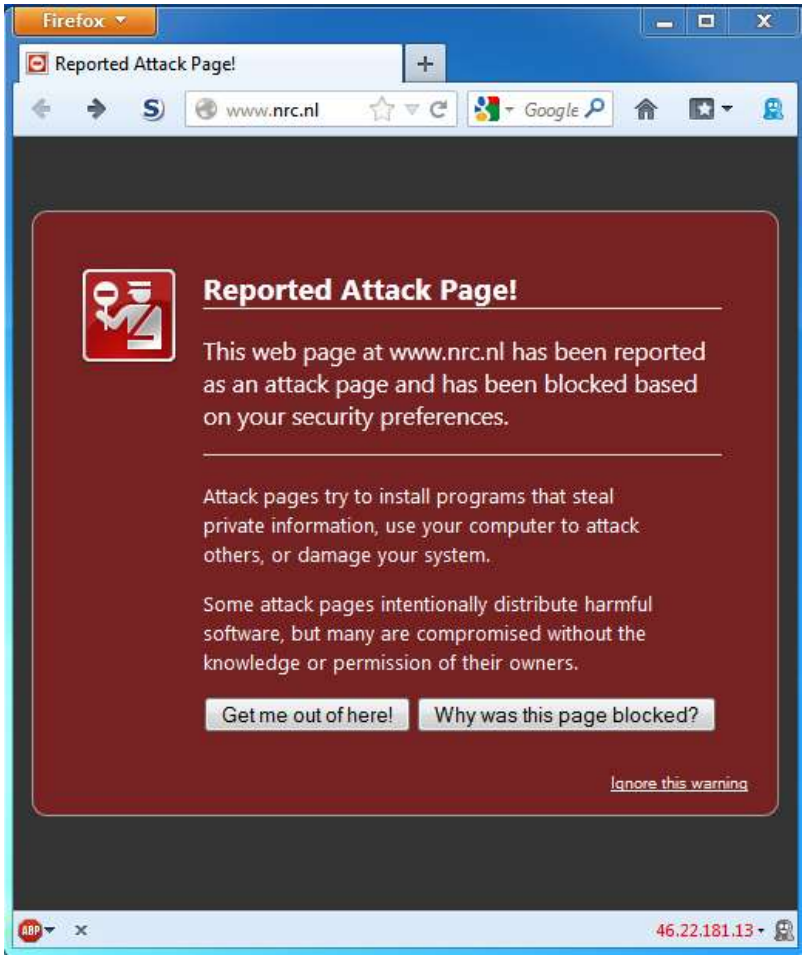
Wie met een kwetsbare Java-installatie de website bezocht werd automatisch geïnfecteerd. Het gaat om kwetsbaarheid CVE-2012-5076, waarvoor onlangs nog een exploit aan hackertool Metasploit werd toegevoegd.

Mark Loman van SurfRight laat tegenover Security.nl weten dat de pagina waar de kwaadaardige advertenties gebruikers naar doorstuurde, de Blackhole Exploit-kit 2.0 bevatte. Dit is een populaire exploit-kit onder cybercriminelen en is verantwoordelijk voor de meeste infecties via 'drive-by downloads'.

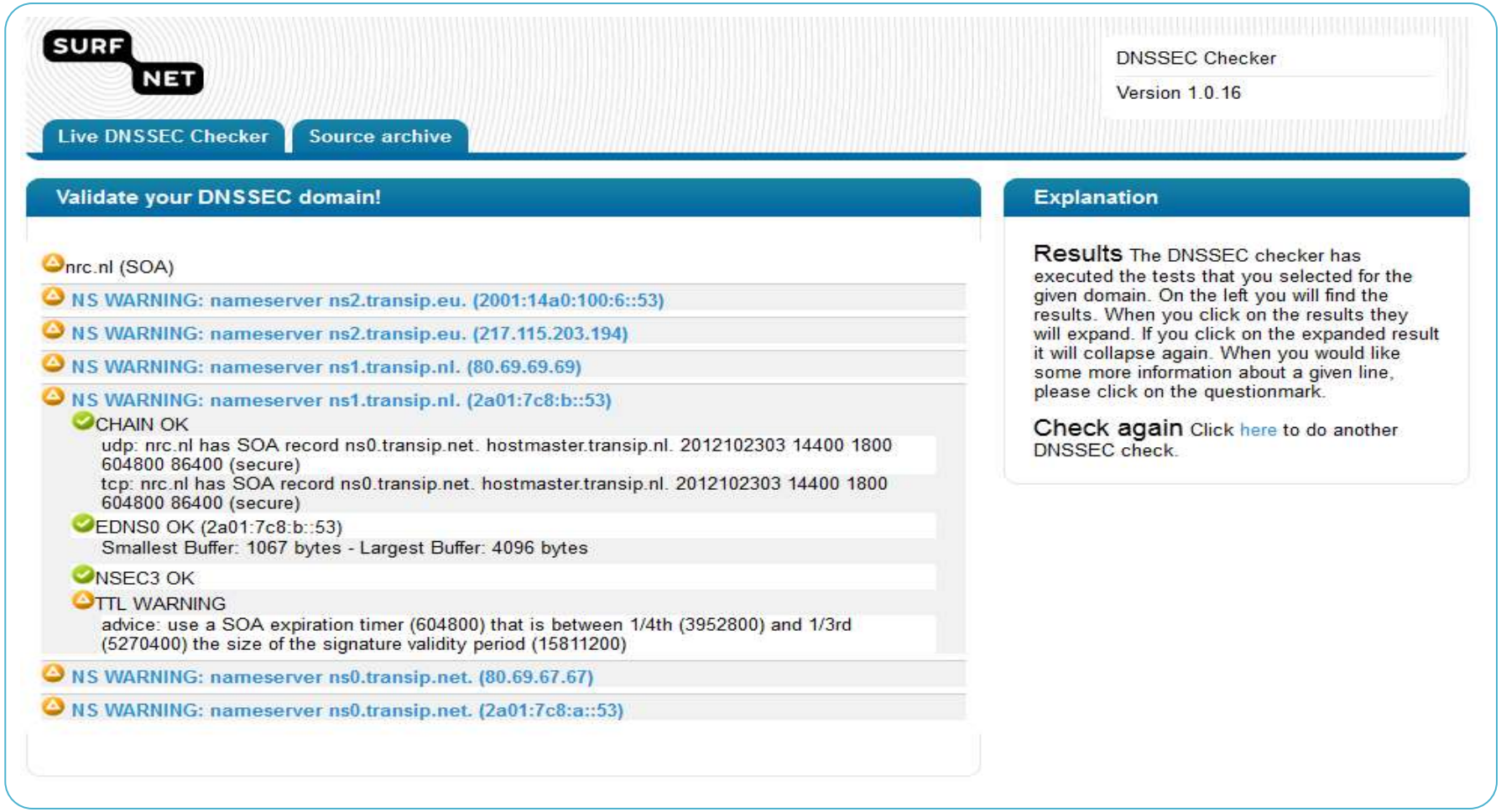
Scan

De advertenties zijn waarschijnlijk van de Belgische adverteerder genaamd Adhese afkomstig. NRC Handelsblad adviseerde bezoekers die voor zeven uur 's ochtends de websites nrc.nl en nrcnext.nl hadden bezocht om het systeem met een virusscanner te scannen.

Uit cijfers van VirusTotal blijkt dat alleen Avast, G Data en Kaspersky Lab de exploit detecteren. De malware zelf wordt door Avast, Sophos, AntiVir en G Data herkend.



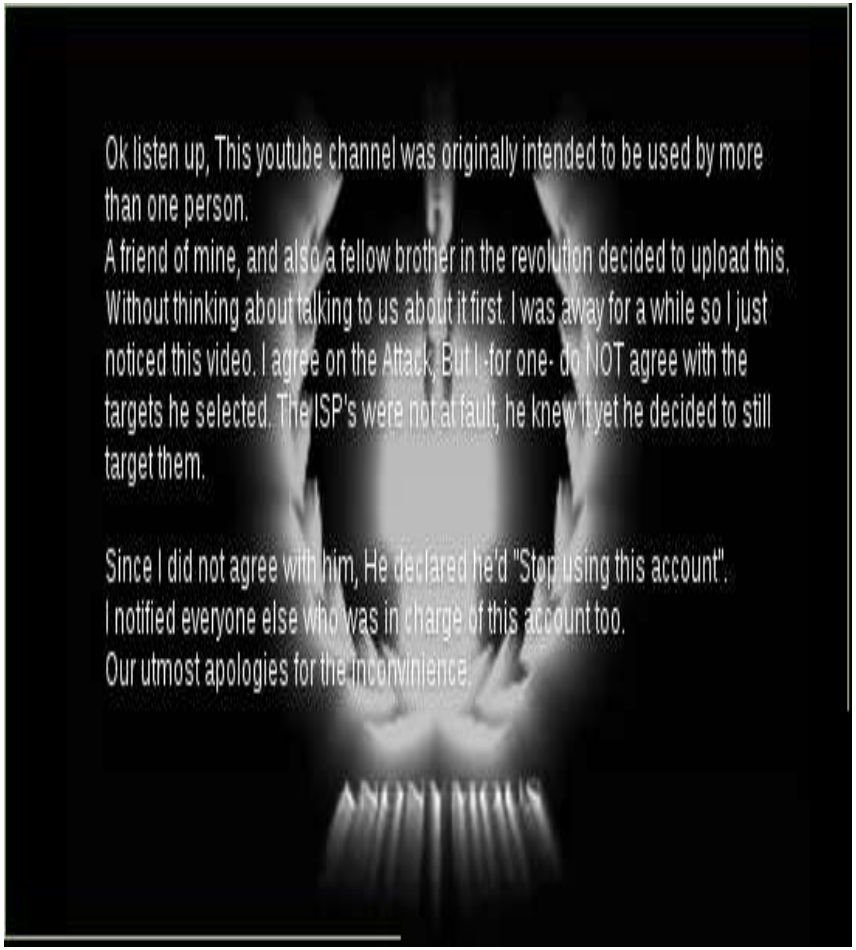
DNSSEC (again)



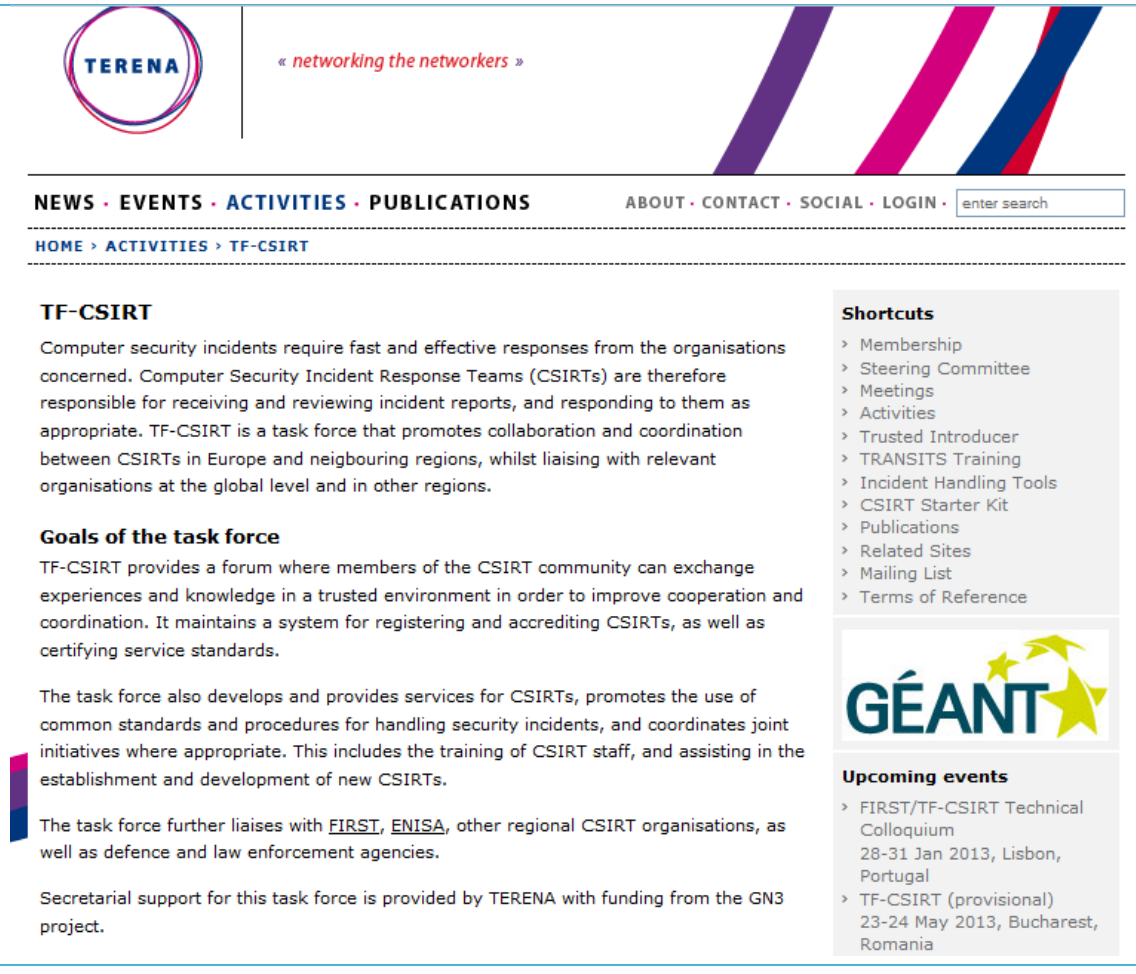
You have them

We have them


PASTEBIN | #1 paste tool since 2002
create new paste | tools | api | archive | faq
PASTEBIN
Follow @pastebin
search...
create new paste | trending pastes
sign up | login | my alerts | my settings | my profile
Op DPB Targets
BY: A GUEST ON OCT 6TH, 2012 | SYNTAX: NONE | SIZE: 0.23 KB | HITS: 2,545 | EXPIRES: NEVER
DOWNLOAD | RAW | EMBED | REPORT ABUSE
Here are the targets for Operation DPB:
http://www.anti-piracy.nl/
www.kpn.com/
www.ziggo.nl/
www.tele2.nl/
www.upc.nl/
www.rijksoverheid.nl/
www.parlement.com/
www.tweedekamer.nl/
www.xs4all.nl/
www.defensie.nl/
#EXPECT US
Public Pastes
Untitled
8 sec ago
Untitled
4 sec ago
Untitled
10 sec ago
Untitled
21 sec ago
Untitled
9 sec ago
Untitled
10 sec ago
Untitled
C | 25 sec ago
Untitled
PHP | 30 sec ago


Ok listen up, This youtube channel was originally intended to be used by more than one person.
A friend of mine, and also a fellow brother in the revolution decided to upload this. Without thinking about talking to us about it first. I was away for a while so I just noticed this video. I agree on the Attack, But I -for one- do NOT agree with the targets he selected. The ISP's were not at fault, he knew it yet he decided to still target them.
Since I did not agree with him, He declared he'd "Stop using this account".
I notified everyone else who was in charge of this account too.
Our utmost apologies for the inconvinience.
ANONYMOUS

TF-CSIRT



SURF NET

CSIRT Training

Trusted Introducer

- Lists teams
- Accredits teams
- Certifies teams
- Trusted security services.

Around the world

APCERT
Asia Pacific Computer Emergency Response Team

Reply | Reply All | Forward | Archive | Junk | Delete

Subject: **Invitation to join APCERT liaison mailing address (TF-CSIRT)**

From: APCERT Secretariat <apcert-sec@apcert.org>

Date: Thu, 01 Nov 2012 16:49:46 +0900

To: jacques.schuurman@surfnet.nl; Me <Wim.Biemolt@surfnet.nl>

Cc: APCERT Secretariat <apcert-sec@apcert.org>

Other Actions

We hope this email finds you well. APCERT has created a new mailing address (apcert-liaison@apcert.org) to promote information sharing with external organizations that APCERT has close collaborative relationships with.

It is our great pleasure to invite TF-CSIRT to utilize our new address whenever you wish to reach APCERT;
for sharing information on incident reports, security issues, events and conferences, projects/researches, and anything else that may be of our mutual benefit or interest.

The address is a closed address, and messages sent to the list will be delivered directly and only to APCERT Member Teams.
APCERT Member Teams
http://www.apcert.org/about/structure/members.html

FIRST


25TH BANGKOK JUNE 2013
ANNUAL FIRST CONFERENCE
BANGKOK, THAILAND
16-21 JUNE 2013


INCIDENT RESPONSE:
SHARING TO WIN
BANGKOK, THAILAND
16-21 JUNE 2013
SAVE THE DATE

FIRST TC


2012
FIRST
Technical
Colloquium
Kyoto, Japan
November 13-15, 2012

Share!

Clearing houses

Conclusion

Wim.Biemolt[at]surfnet.nl

wimbie

www.surfnet.nl

+31 30 2 305 305