IT Security Datenquellen für ISPs

L. Aaron Kaplan
<kaplan@cert.at>

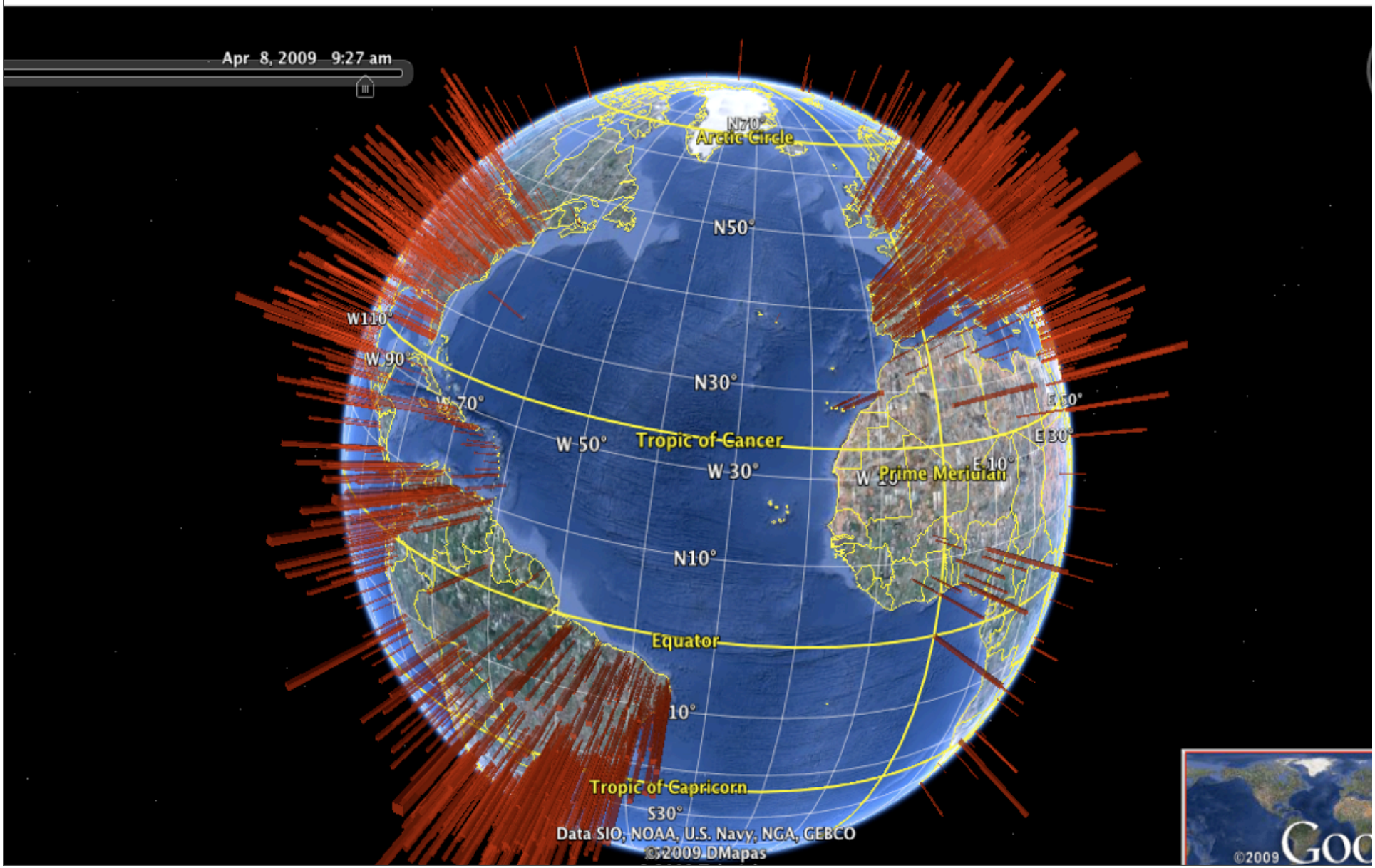
VORAB: NOTIZEN?

CERT.at?

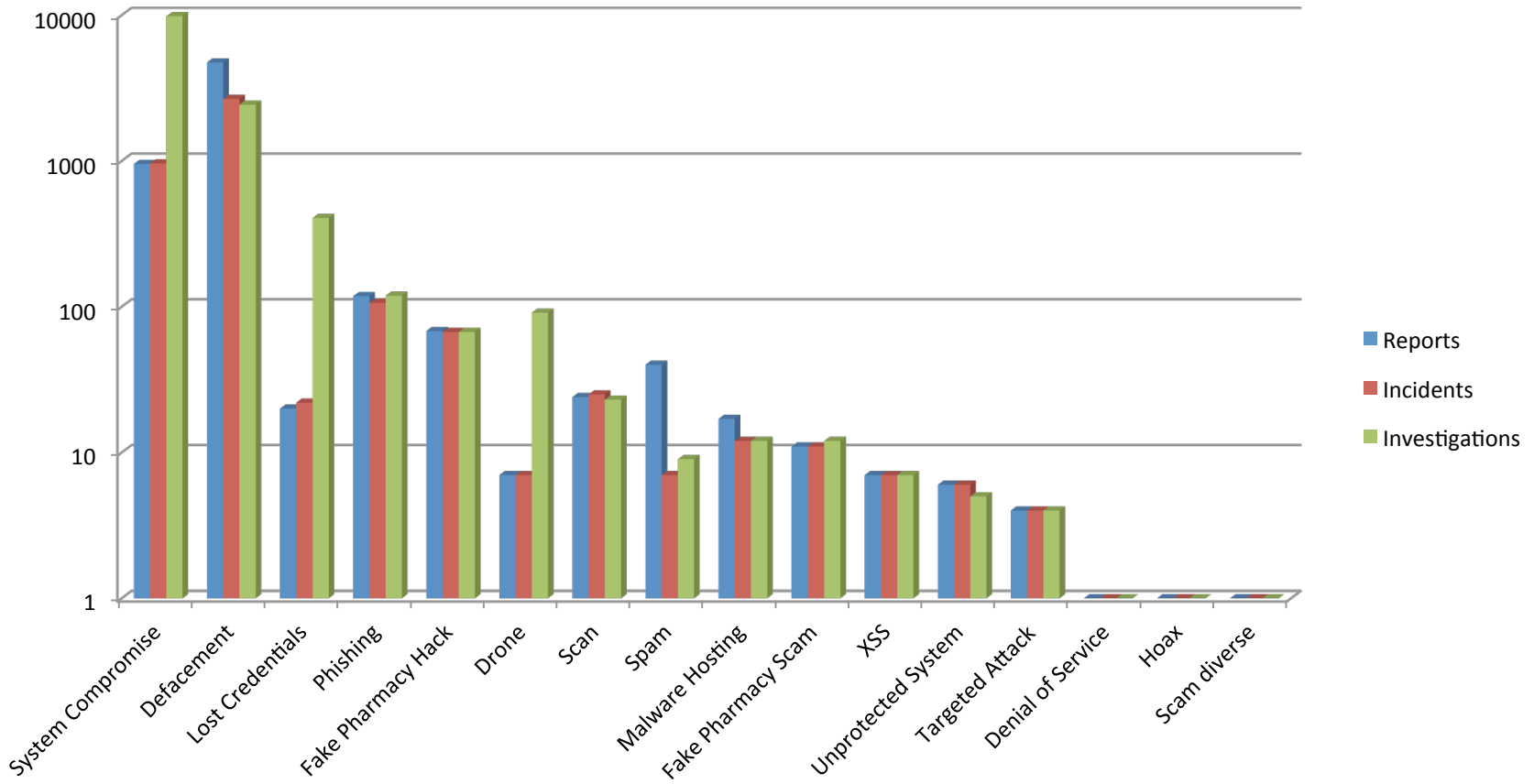
- Projekt innerhalb der nic.at
- Nationales Computer Emergency Response Team für Österreich
- Zentrale IT-Security Vorfalls-Koordinationsstelle für Österreich
- Kooperation mit dem Bundeskanzleramt
- Operational seit April 2008
- Technischer Teil des GovCERTs
- 7 FTEs

Services

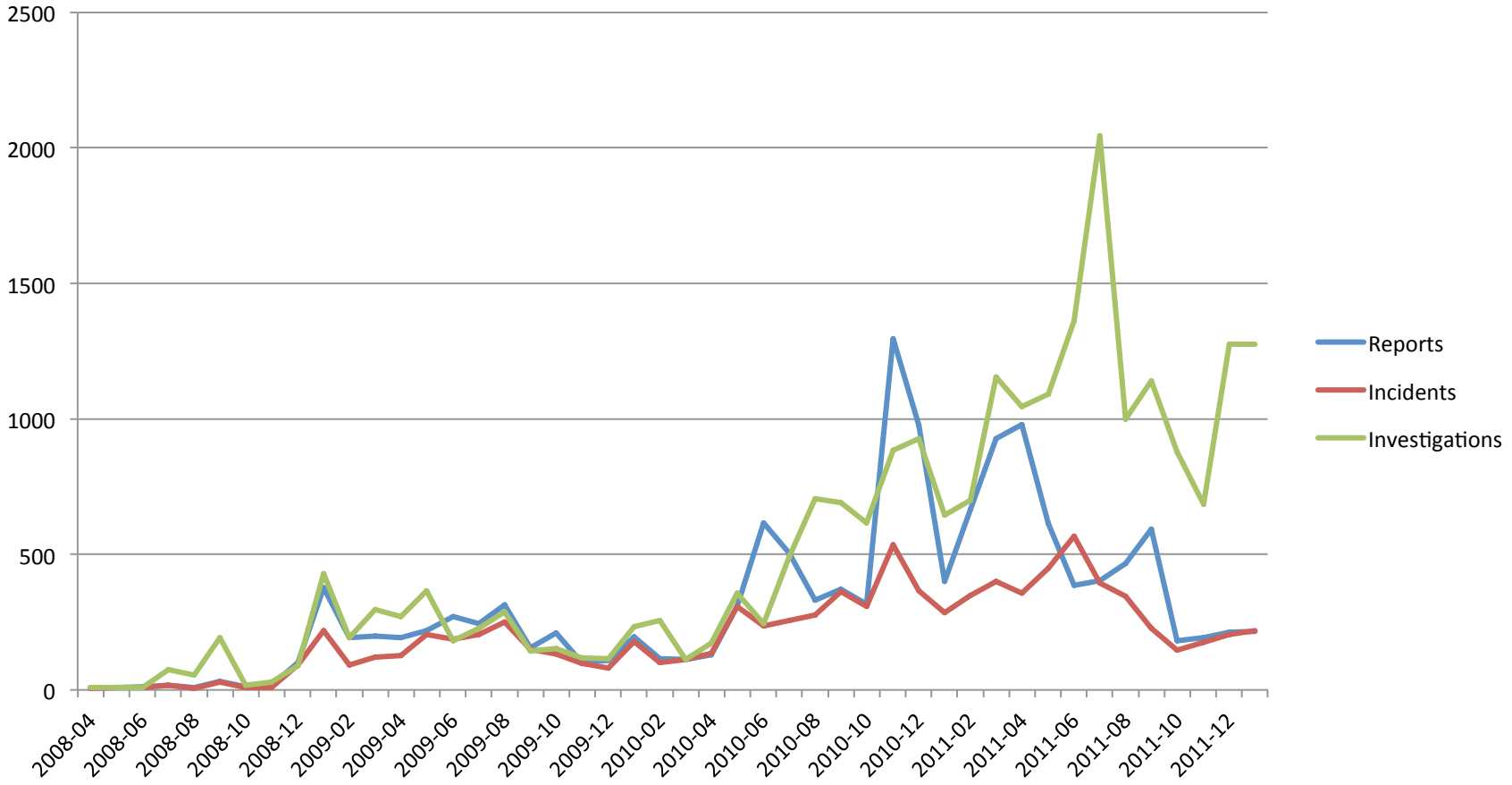
1. Nationaler PoC, govCERT Backend
2. Incident handling coordination
3. Incident handling (vor Ort)
4. Malware Analyse/RE
5. Media outreach & tech watch
6. Vernetzung der IT Security Experten
7. Publikationen, recommendations, best practices


Apr 8, 2009 9:27 am
N70°
Arctic Circle
N50°
W110°
W 90°
N30°
W 70°
W 50°
Tropic of Cancer
W 30°
Prime Meridian
E 10°
N10°
Equator
10°
Tropic of Capricorn
S30°
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
©2009 DMapas
©2009

Kategorisierung der Vorfälle 2011 (logscale)



Langfristiger Trend / Monat 2008-2011



ÜBERBLICK

Überblick


ISPA workshop
Intro CERT.at, 5min
Was ist das Problem?
gehackter webserver
gehackter hoster (CMS hoster, app. hoster)
infizierter client PC / smartphone / tablet
verwundbarer service
(D)DOS (zB DNS amplification attack)
Warum ist das ein Problem?
privacy
folge-probleme
1 Atomkraftwerk f. Spam
Trends
Was ist unser Problem bei CERT.at?
Wie ist die patchrate ?
Best practices im Ausland
botfrei.de
cert.fi / FICORA
Wie ist die Sicht der ISPs?
Was koennen wir verbessern?
Wie ersparen sich ISPs Arbeit?
Feeds
reaktiv
Pro-aktive Suche
meta
ContactDBs
ripe
abuse-c
IRT
CERT.at poca plattform
AS-mappings.txt

PROBLEMBESCHREIBUNG

„Cyber“-*

- Cybercrime
- Gehackte PCs, tablets, smartphones
- Gehackte Webserver
- Verwundbare Services
- DDOS oder PCs/Server, die bei (D)DOSes mitmachen
- „Cyber-war“ (i.e. Angriffe via unsere zivile Infrastruktur (ISP Netze als Transport))

„Cyber“-* (2)

- Infektion -> Kunde ruft beim call center an, dass „das Internet nicht geht“
- Gehackter hoster -> viele Kunden betroffen
- Datenschutz? Sind die eigenen Systeme sicher? Leaken meine Kundendaten?
- Ist meine eigene Infrastruktur unterwandert?
- Begierden der Strafverfolgungsbehörden
- Etc...

„Cyber“- blues

- Margen im ISP biz sind geschrumpft
- Aufwand ist höher
- Jetzt kommt noch „cyber“-* dazu!
- ➔ Nur Arbeit für den ISP und für CERTs

Not my problem?

- Ist das überhaupt das Problem des ISPs?
- Jein. Eigentlich nicht, aber der Aufwand bleibt beim ISP:
  - Anfragen der Polizei
  - Infrastruktur a la VDS
  - Kundenanrufe
  - Mails vom CERT
- All das ist **manuelle** Arbeit → teuer

Not my problem (2)?

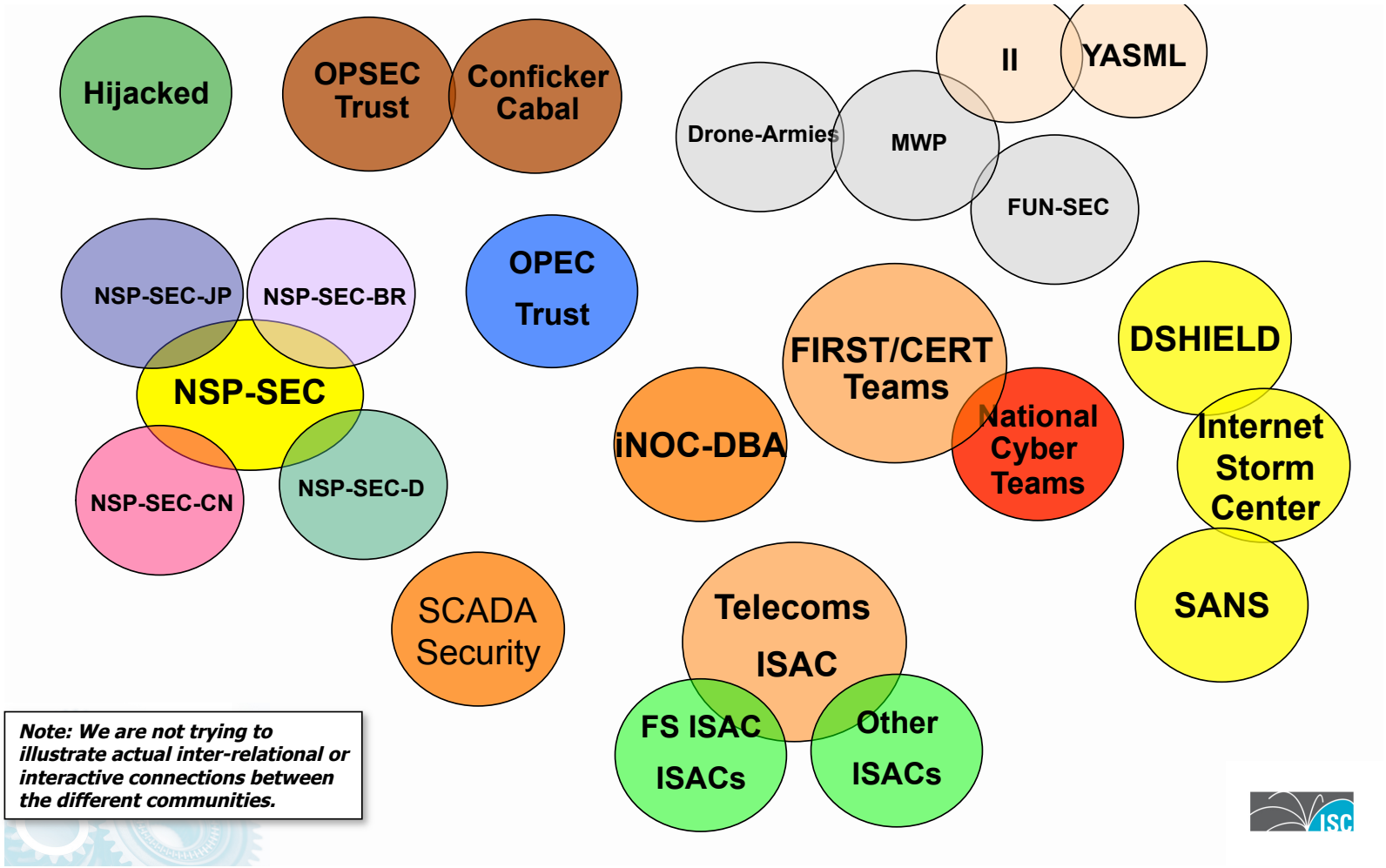
- Stromverbrauch für monitoringsysteme, Spam-processing, IDSen, ...
- Schätzung: 1 Atomkraftwerk nur für Spam processing in 2010
- Was ist mit den eigenen Systemen (KundenDB, WLAN router, CPEs), leaks?
- Route hijacking (Pakistan/Youtube)
- DNS cache poisoning

Trends

- Internet ist nicht mehr das Akademische Netz, nicht mehr das Netz der Pioniere, das Netz der well-behaving netizens
- (manche) Staaten aber auch „cyber“-Kriminelle möchten Kontrolle. Im einen Fall geht es um Macht, Hegemonie, Spionage, Sabotage, etc. im anderen nur um $$$
- Es wird definitiv schlimmer

WAS TUN? WAS KÖNNEN WIR GEMEINSAM MACHEN?

Starke Zusammenarbeit!



Was machen wir bei CERT?

- Mitglied in den meisten solchen Gruppen
- Wenn feeds von diesen Gruppen kommen, dann wird automatisiert und an ISPs / Organisatonen verschickt
- Analyse der Vorfälle & Empfehlungen

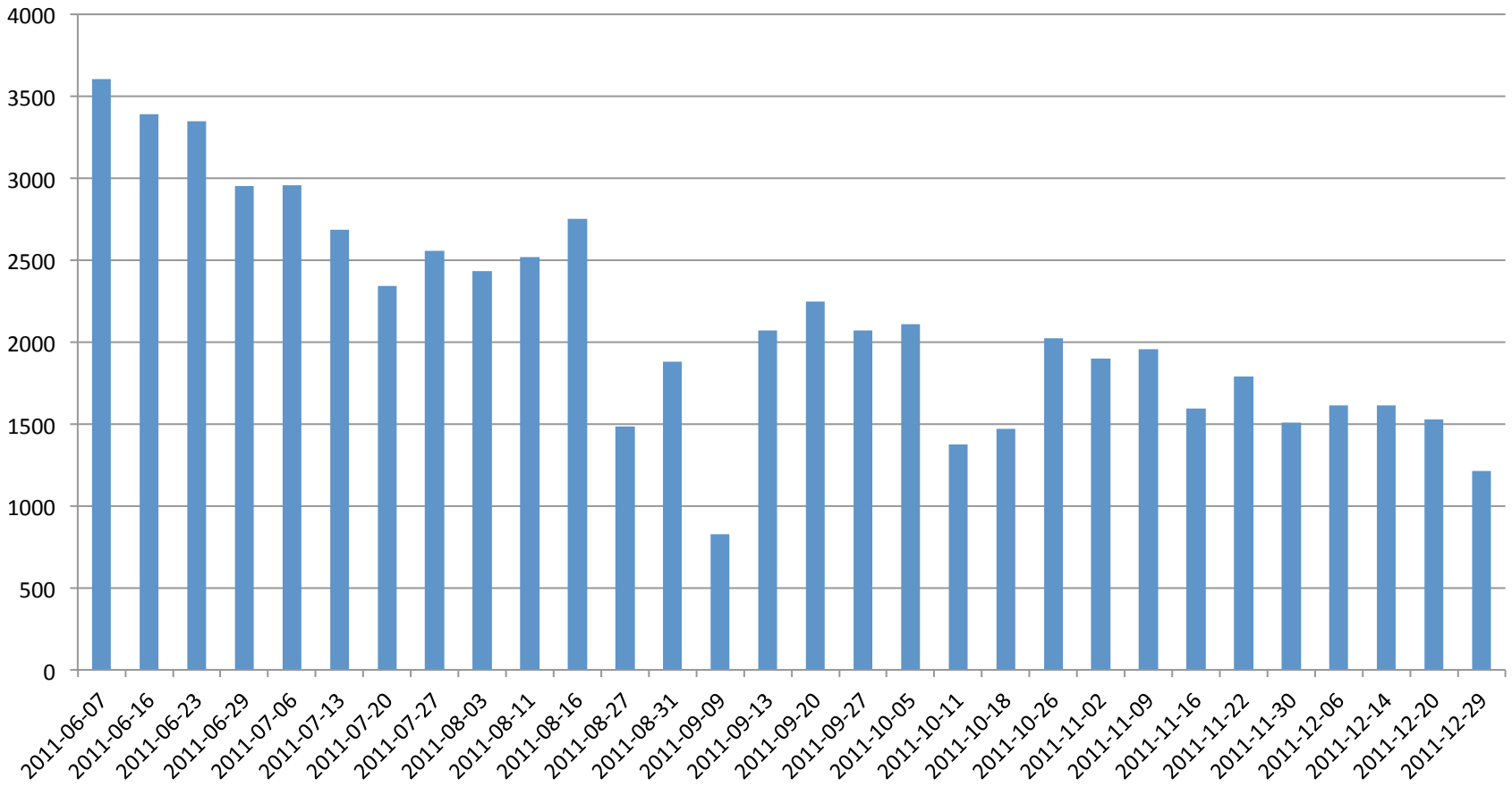
WIE ERFOLGREICH IST DAS?

CERT.at Sicht auf Botnetz

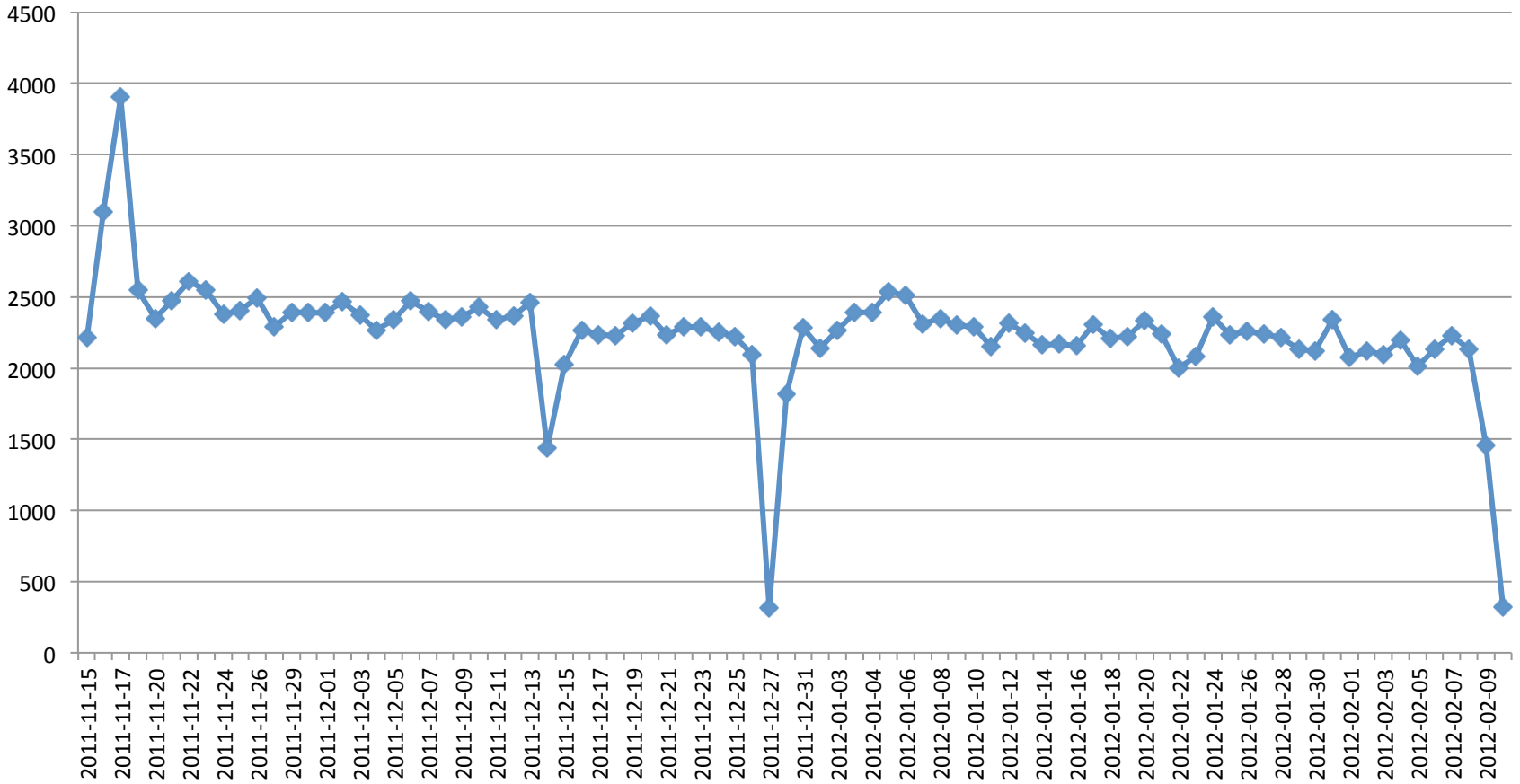
- Wir sehen primär zentralistische Botnetze
- Sinkholes
- CC- und Passwort dropzones
- IRC-basierte Server
- Feeds von Botnetzen, die andere CERTs monitoren
- Sprich: die einfachen
- CERT.at job: informieren, clean-up zuführen

CLEAN-UP RATE

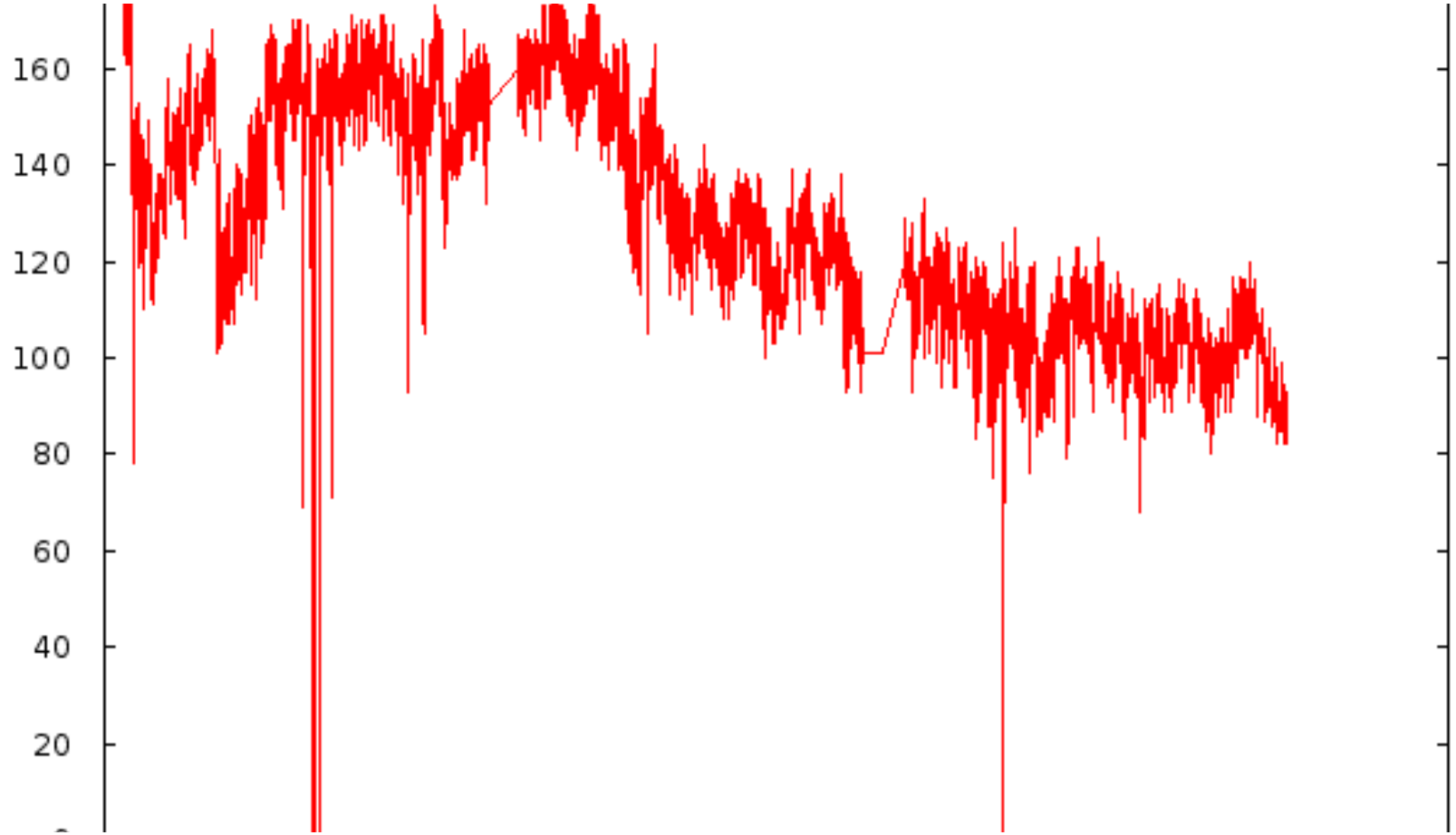
Rustock


4000
3500
3000
2500
2000
1500
1000
500
0
2011-06-07
2011-06-16
2011-06-23
2011-06-29
2011-07-06
2011-07-13
2011-07-20
2011-07-27
2011-08-03
2011-08-11
2011-08-16
2011-08-27
2011-08-31
2011-09-09
2011-09-13
2011-09-20
2011-09-27
2011-10-05
2011-10-11
2011-10-18
2011-10-26
2011-11-02
2011-11-09
2011-11-16
2011-11-22
2011-11-30
2011-12-06
2011-12-14
2011-12-20
2011-12-29

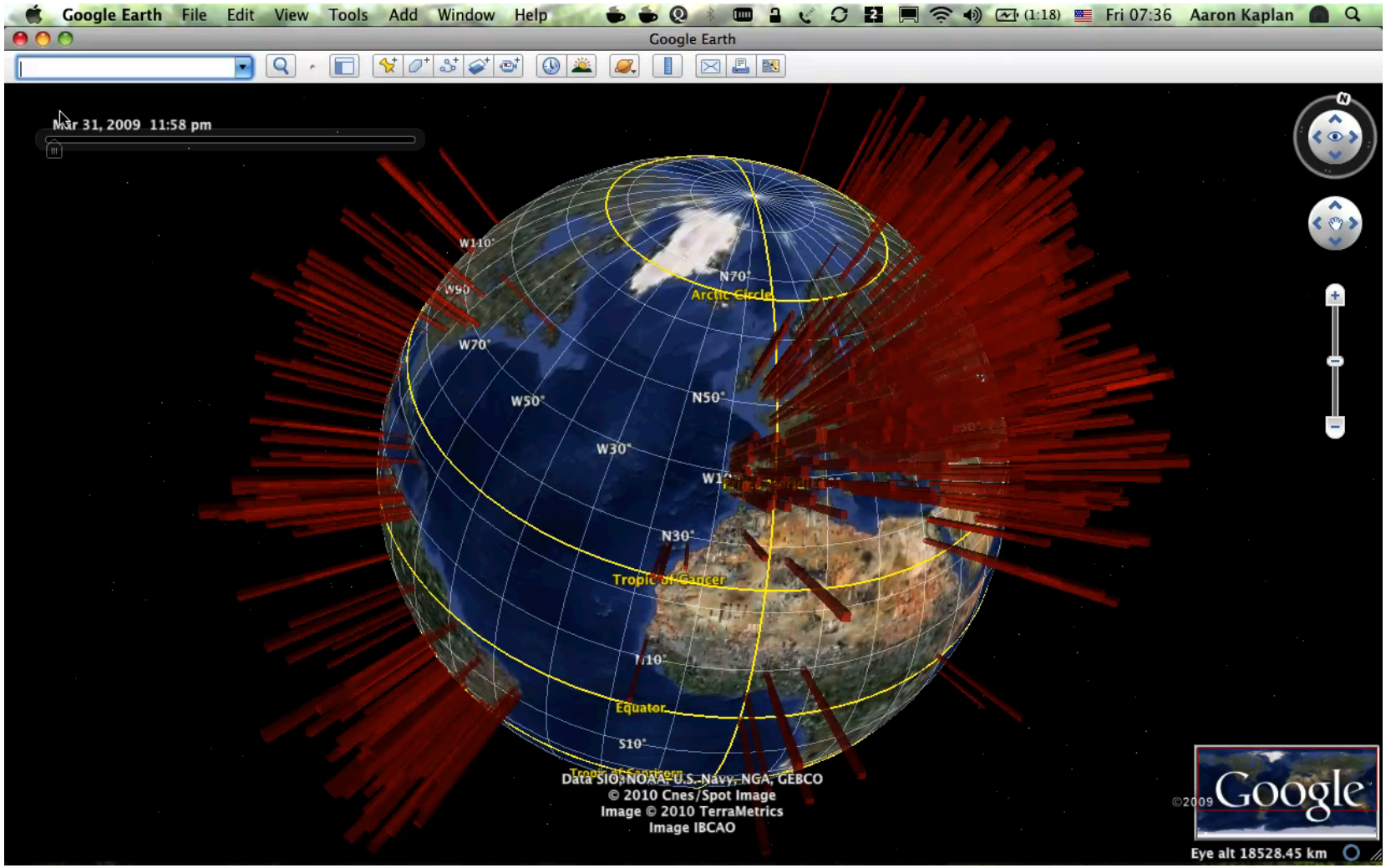
DNSChanger


4500
4000
3500
3000
2500
2000
1500
1000
500
0
2011-11-15
2011-11-17
2011-11-20
2011-11-22
2011-11-24
2011-11-26
2011-11-29
2011-12-01
2011-12-03
2011-12-05
2011-12-07
2011-12-09
2011-12-11
2011-12-13
2011-12-15
2011-12-17
2011-12-19
2011-12-21
2011-12-23
2011-12-25
2011-12-27
2011-12-31
2012-01-03
2012-01-04
2012-01-06
2012-01-08
2012-01-10
2012-01-12
2012-01-14
2012-01-16
2012-01-18
2012-01-20
2012-01-22
2012-01-24
2012-01-26
2012-01-28
2012-01-30
2012-02-01
2012-02-03
2012-02-05
2012-02-07
2012-02-09

Open recursors



Conficker.C


Google Earth File Edit View Tools Add Window Help
Fri 07:36 Aaron Kaplan
Google Earth
Mar 31, 2009 11:58 pm
W110°
W90
W70°
W50°
W30°
N70°
Arctic Circle
N50°
N30°
Tropic of Cancer
Equator
S10°
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
© 2010 Cnes/Spot Image
Image © 2010 TerraMetrics
Image IBCAO
©2009 Google
Eye alt 18528.45 km

Clean up rate

- Exponentiell abflachend
- 20%-30% bleiben infiziert/betroffen

BEST PRACTICES IM AUSLAND

Botfrei.de, XS4ALL.nl

- Walled garden
- Call center wurde zentralisiert
- ISPs beteiligen sich am call center
- Professionelle Beratung
- XS4ALL: gratis AV Paket für Kunde. Kunde clickt „habe AV installiert“ und darf wieder ins Netz
- Initial sehr gutes Feedback

CERT.fi / FICORA

- CERT ist Teil des Regulators
- Druck vom Regulator
- ➔ eines der „saubersten“ Länder (Quelle: Microsoft SIR Report)
- Wünschenswert?

Q&A: WIE GEHEN SIE DAMIT UM?

FEEDS

A) REAKTIV

Shadowserver

- CSV file, Botnet Infektionen

Sehr geehrte Netzbetreiber,

wir wurden informiert, dass die im Anhang genannten IP-Adressen
aus ihrem AS anscheinend Teil eines Botnets (vgl. http://de.wikipedia.org/wiki/Botnet),
genauer gesagt mit der "Grum" bzw. "Tedroo"-Malware (unter anderem
auch für Spam-Mail Versand genutzt) befallen sind (http://en.wikipedia.org/wiki/Grum_botnet).

Diese Daten stammen aus vertrauenswuerdiger Quelle, die Zugriff
auf einen der sog. "C&C"-Server dieser Malware erlangen konnte.

Bitte Ihren Richtlinien entsprechend behandeln.

File Format:
[Timestamp des Zugriffs auf den "C&C"-Server] [IP]
Timestamp-Format ist yyyy-mm-dd hh:mm:ss UTC

Mit freundlichen Gruessen,

n6

- Honeypots, Scan Treffer, Bot Infektionen
- Millionen von rows pro Jahr
- Sehr viel, was in Polen eintrifft
- Status: wird nächste Woche in Probebetrieb gehen

DNSChanger

- Modifiziert Windows „/etc/resolv.conf“ Datei (Systemsteuerung -> Netzwerk)
- Kann via web cross site request forgery WLAN Router von „innen“ umkonfigurieren
- Anderer DNS Server -> Kunden werden abgephisht, pwds ausgespäht, etc.
- Kunden rufen an „mein Internet geht nicht“
- Viele Fälle in Österreich

Torpig / Sinowal

- Klassisches Botnetz
- Meist mit Mebroot kit
- „By November 2008, it was considered that Torpig had stolen the details of about 500,000 online bank account“ (wikipedia Torpig 2012/12/05)

Spyeye/Zeus

- Banking Trojaner
- Jetzt auch auf Android!
- ➔ hebelt 2-faktor Autentifizierung aus
- Regelmäßig werden österr. Banken über Spyeye ausgespäht (bzw. deren Kunden erleichtert)

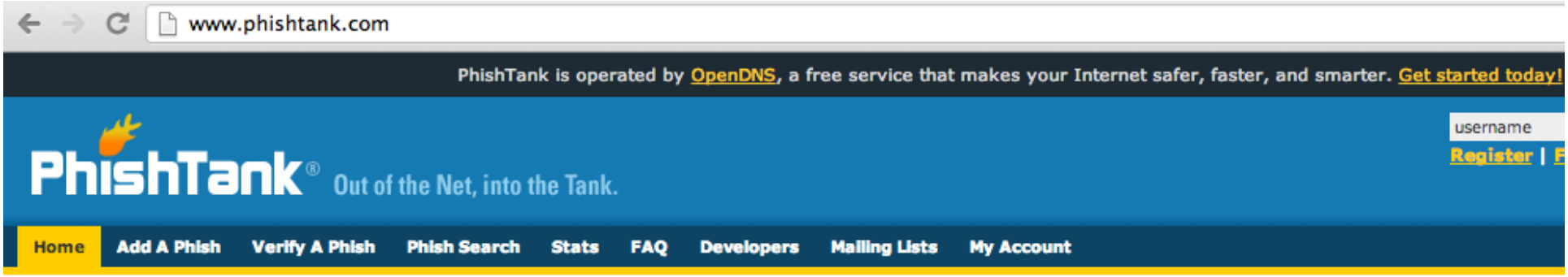
Lulz with Anonymous

- Pwd leaks auf pastebin
- Passiert meist nur, wenn Firmen sich wirklich nicht gut absichern
- Oft keine kriminelle Energie dahinter, eher Aufzeigen von Sicherheitslücken
- Pastebins lassen sich automatisiert auswerten/ durchsuchen
- Problem: pwd cracking ist einfach! ➔ hash ist genauso geheim zu halten wir pwd

EXKURS: DEMO PWD CRACKING MIT OCLHASHCAT

phishtank

- Gratis
- Hat ein gutes API
- Einfache Abfragen, ob eigene domains dort vorkommen -> Alarmierung



Join the fight against phishing

Submit suspected phishes. **Track** the status of your submissions.
Verify other users' submissions. **Develop** software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

http:// Is it a phish?

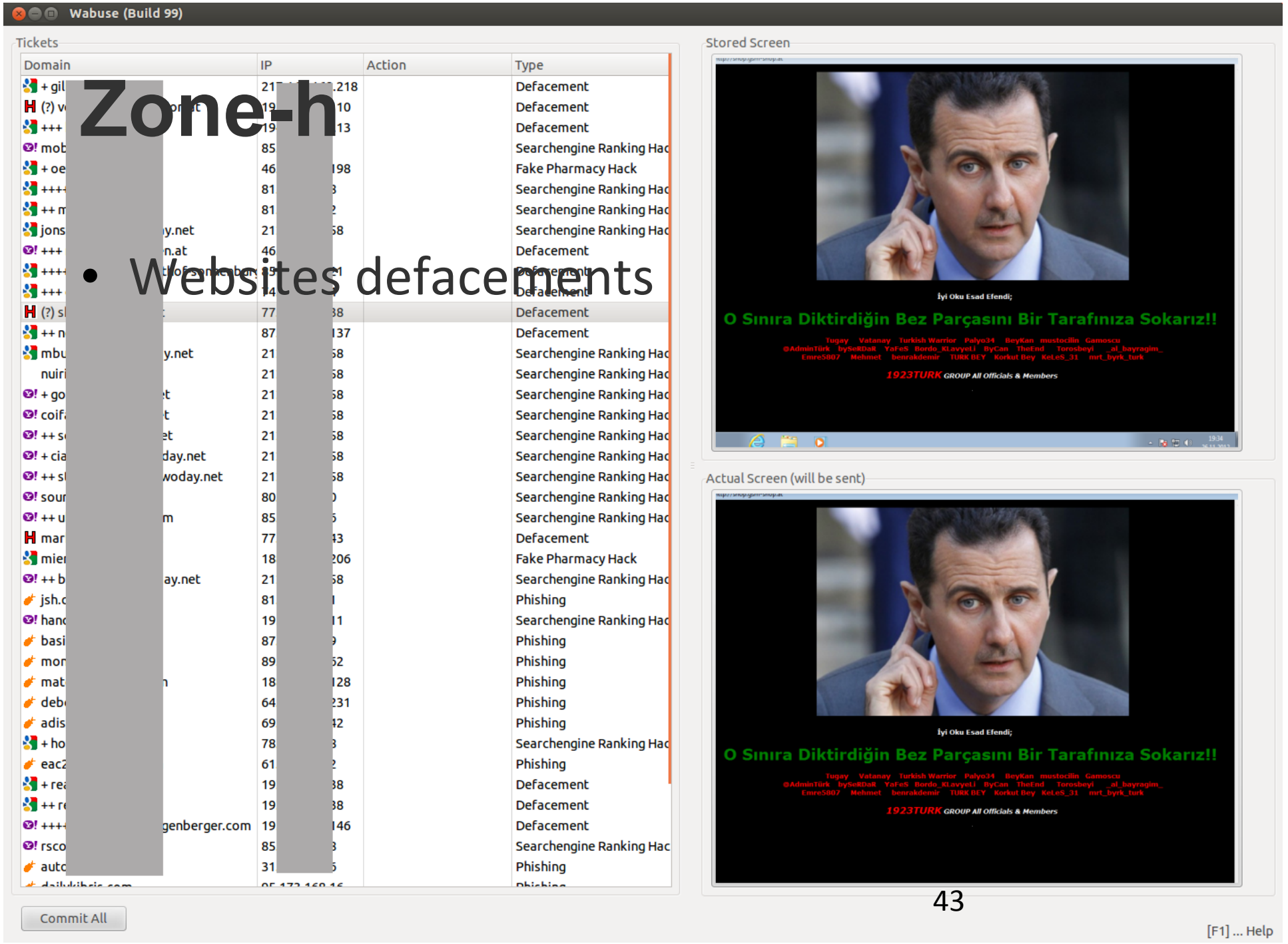
Recent Submissions

You can help! **Sign in** or **register** (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
1643512	http://dsamvicuna.com/templates/sunshine/abn/index...	cleanmx
1643511	http://www.zwatecnologia.com.br/wp-content/gallery...	cleanmx
1643510	http://marigoldtravel.com.bt/index.php/visitor-inf...	cleanmx
1643509	http://bjcurio.com/js/index.htm?us.battle.net/logi...	sec4it
1643507	http://us.battle.net.ok.qe-rs.com/login/en/login.h...	sec4it
1643506	http://e-3d.co.uk/vodafoneshop/important_security_...	paulch
1643503	http://shahalamgallery.com/includes/js/page.net.cl...	capitec
1643502	http://www.adharas.com.br/templates/atomic/html/mo...	ShinobiPhish
1643501	http://us.battle.net.en.ttweb.asia/login/en/login....	sec4it

Zone-h

- Websites defacements

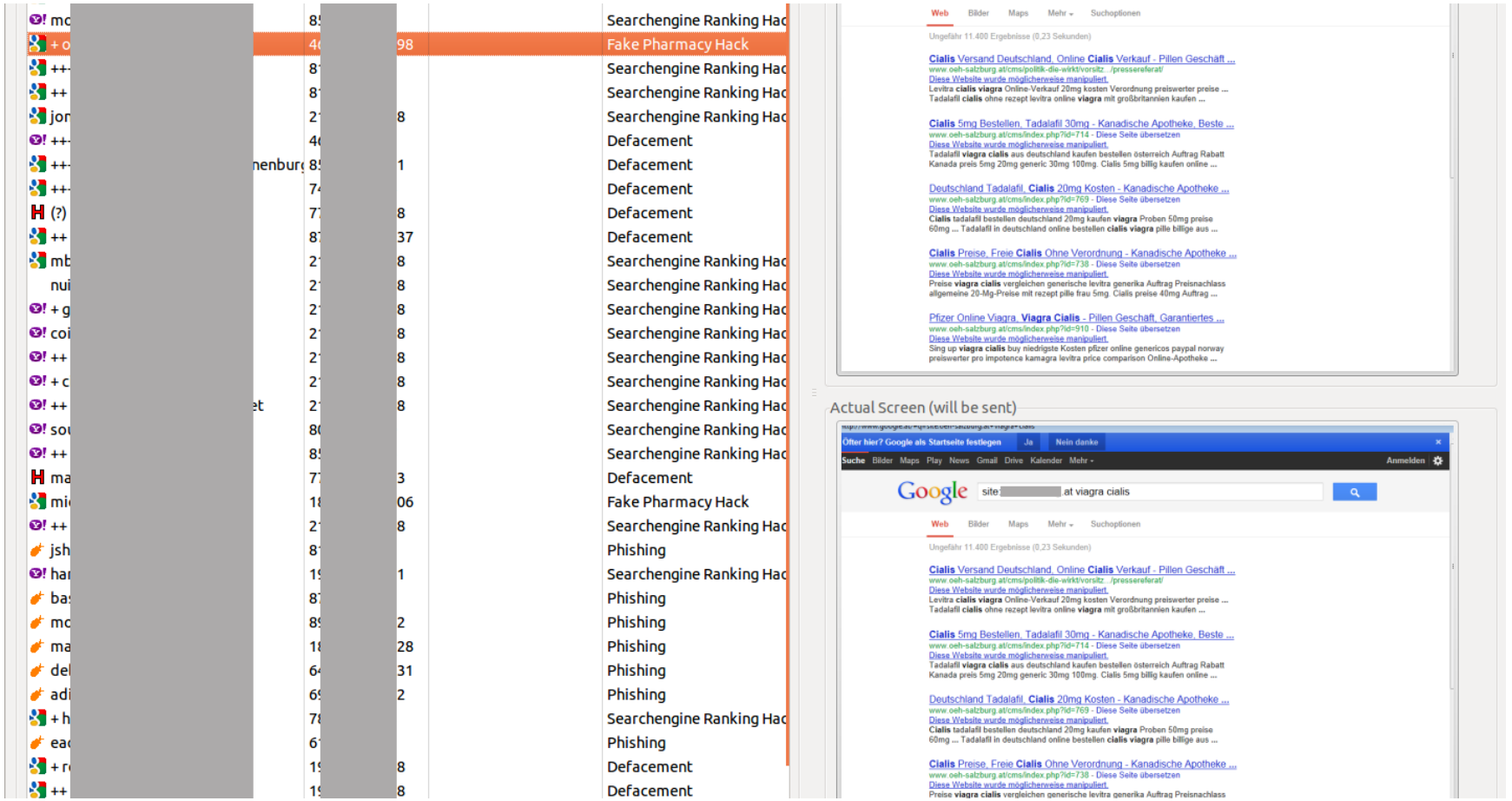


Google conditional hacks

- Schritt 1: CMS p0wned
- Schritt 2: beobachten des pageranks
- Schritt 3: wenn referrer == google , dann Viagra Werbung

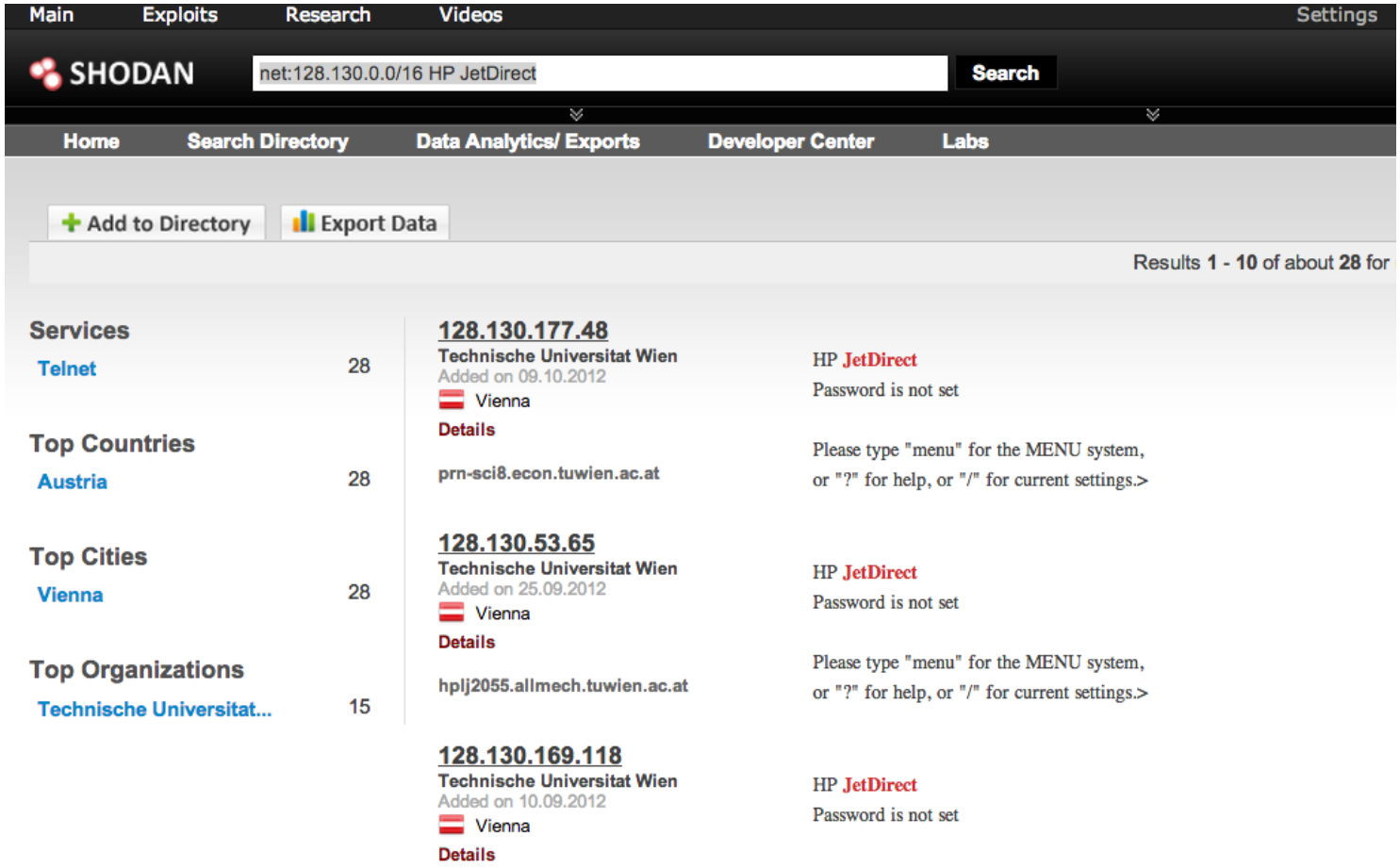
- Ist natürlich erweiterbar...

Google conditional hacks



B) PROAKTIV

Shodanhq


Main
Exploits
Research
Videos
Settings
SHODAN
net:128.130.0.0/16 HP JetDirect
Search
Home
Search Directory
Data Analytics/ Exports
Developer Center
Labs
Add to Directory
Export Data
Results 1 - 10 of about 28 for
Services
Telnet 28
Top Countries
Austria 28
Top Cities
Vienna 28
Top Organizations
Technische Universitat... 15
128.130.177.48
Technische Universitat Wien
Added on 09.10.2012
Vienna
Details
prn-sci8.econ.tuwien.ac.at
HP JetDirect
Password is not set
Please type "menu" for the MENU system,
or "?" for help, or "/" for current settings.>
128.130.53.65
Technische Universitat Wien
Added on 25.09.2012
Vienna
Details
hplj2055.allmech.tuwien.ac.at
HP JetDirect
Password is not set
Please type "menu" for the MENU system,
or "?" for help, or "/" for current settings.>
128.130.169.118
Technische Universitat Wien
Added on 10.09.2012
Vienna
Details
HP JetDirect
Password is not set

C) META

Meta

- Automatisierungsgrad I1-I6
- Qualität schwankt. Wir schicken nur die besten feeds aus
- Formate:
  - CSV
  - X-ARF (basiert auf RFC 5965, YAML)
  - IODEF (XML)

ContactDBs

- RIPE:
  - Abuse-C Feld ist neu
  - IRT Objekt

Q&A: WAS KÖNNEN WIR VERBESSERN?

Q&A: WIE ERSPAREN SICH ISPS ARBEIT?

Q&A: RECHTL. DIMENSIONEN?

ZUSAMMENFASSUNG

IT-Security = Wettlauf

- Angreifer sind im Vorteil
- „Der der Computer besser programmieren kann, gibt ihnen Befehle“ (anons)
- Aufruf: Teilnahme an CERT.at Runden, Informationsaustausch, aggressive Vernetzung untereinander
- Konstante Betreuung und idealerweise Assurance der eignen Systeme ➔ Investitionen! ☹
- Von anderen und von deren Fehlern lernen
- Logging auch verwenden
- Updates updates updates
- (externe) Pentests
- netflow

IT Security == Kooperation

- IT Security Stammtisch CERT.at
- Sektor-spezifische Gruppe „ATC“
- Austausch von Wissen/know-how erleichtert uns allen die Arbeit

IT SECURITY IS NOT AN ISLAND