Viren, Trojaner und … der Mensch: Aktuelle Bedrohungen im Internet

Bedrohungen aus dem Internet aus der Sicht eines CERT

Robert Schischka

Inhalt

- Vorstellung CERT.at
- Bedrohungsbilder
- Motivation
- Angriffsvektoren oder „Teufels Werk und User‘s Beitrag“
- Infrastruktur
- Fallstudie RSA
- Gedanken zur Gefährdungslage

Wer sind wir?

GovCERT AUSTRIA

CERT.at

- **CERT.at – das nationale Computer Emergency Response Team**
  - Ansprechpartner für IT Sicherheit im nationalen Umfeld
  - Zielgruppe: österreichische IT Security-Teams und lokale CERTs
  - Vernetzung von und mit anderen CERTs, Sicherheitsteams (weltweit)
  - Koordinationsstelle
  - Initiative von nic.at (österreichische Domain Registry)

- **GovCERT – das Government Computer Emergency Response Team**
  - Zielgruppe: öffentliche Verwaltung und kritische Informationsinfrastruktur
  - Kooperation zwischen Bundeskanzleramt und CERT.at

Was tun wir?

GovCERT AUSTRIA CERT.at

- Informationsverteilung
  - Warnungen
  - Empfehlungen
- Aufbereitung von Sicherheitsinformationen
- Vorfallskoordination
- Unterstützung bei Sicherheitsvorfällen
  - Analyse
  - Task-Forces
- Clearingstelle
- Plattform für Vernetzung der IT-Security Experten in Österreich
- Unterstützung beim Aufbau von CERTs
- Lagebild

Gefahren im Cyberspace

- Malware aller Art
- 0-Days
- Advanced Persistent Threat (APT)
- Wirtschaftsspionage
- Information Leaking – Data loss
- Angriffe auf Infrastruktur
  - Eingriffe ins Routing
  - DNS – Spoofing
  - Zertifikatsmanipulation
  - Hardware (Router, …)
  - Attacken auf ISP, Registries
  - Smart Meter
- Content Diebstahl
- Fake Pharmacy
- Phishing
- Datenmanipulation
- Sabotage
- Identitätsdiebstahl
- SPAM
- Erpressung
- Geldwäsche
- DDOS
- ….

File Edit View History Bookmarks Tools Help

http://[redacted]/anfang.cgi/

Sparkasse

Willkommen

... im personlichen Finanzportal

Dies ist die Homepage, auf der Sie Ihre Online-Banking-Kundendaten bestätigen können.

Wir bitten Sie, alle obligatorischen Felder auszufüllen. Wenn Sie ein obligatorisches Feld frei lassen, wird ein Hinweis angezeigt, in dem Sie aufgefuhrt werden, die fehlenden Felder auszufüllen.

Frau

Herr

Vorname

Familienname

PLZ

BLZ

Nr. TAN

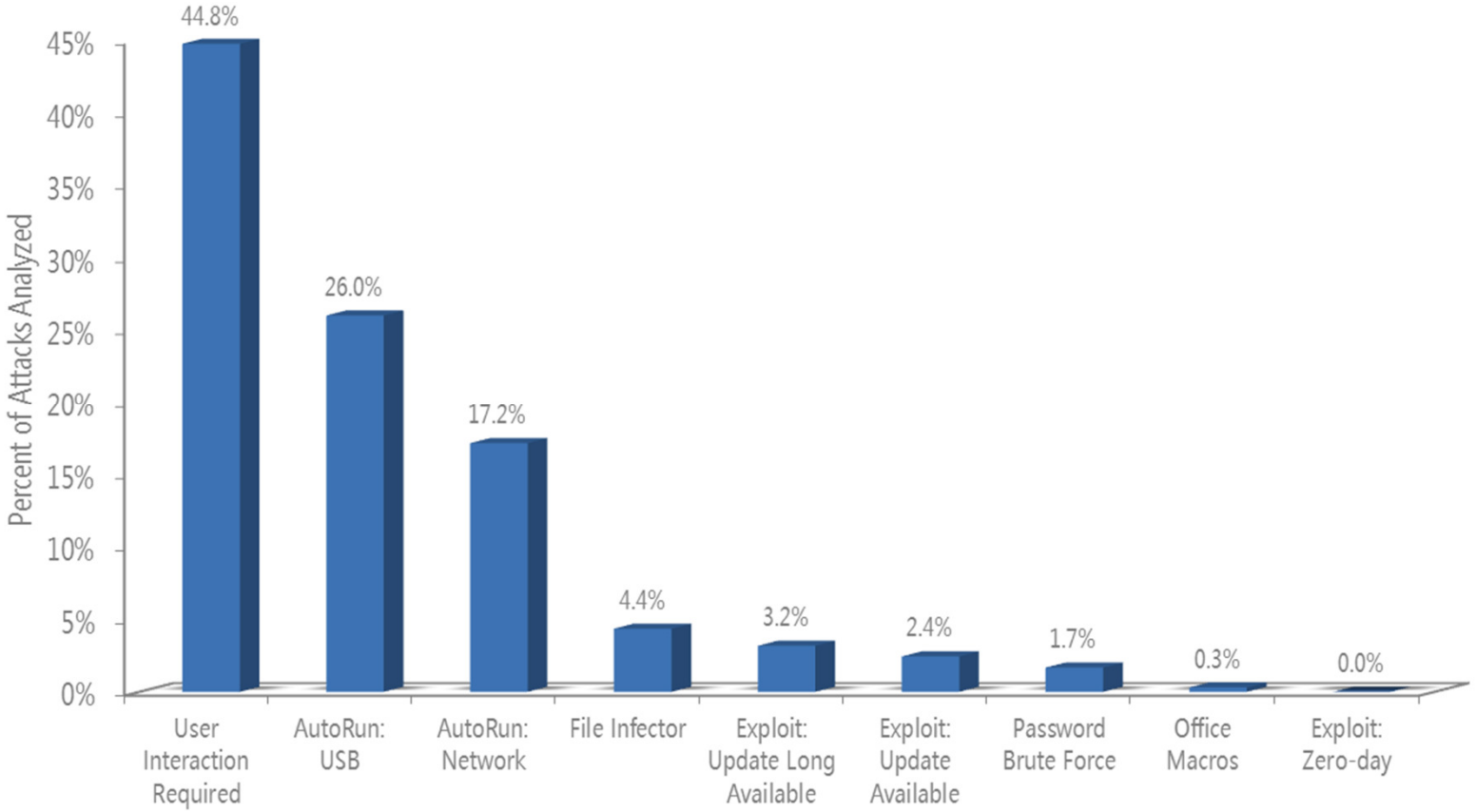
Geben Sie alle unbenutzten TAN-Nummern Ihrer TAN-Liste ein.

Anmeldename oder Legitimations-ID:

Done

2007-11-16 09:44:20 (UTC)

Die guten Nachrichten…



Quelle: Microsoft Security Intelligence Report Vol. 11
Im ersten Halbjahr 2011 vom MSRT erkannte Schadsoftware, sortiert nach dokumentierter Verbreitungsmethode

Die schlechten Nachrichten…

- Häufigster Exploittyp Q1 und Q2 2011
  - 33%-50% Java (JRE, JVM, Java SE)
    Quelle: Microsoft
- Mobile Security
  - „Dialer“
  - Zeus goes mobile
  - Trojaner verändert TAN/ TAC Rufnummer
- Hardware Hacking z.B. StuxNet
- Advanced Persistent Threats

Quelle: CERT.pl

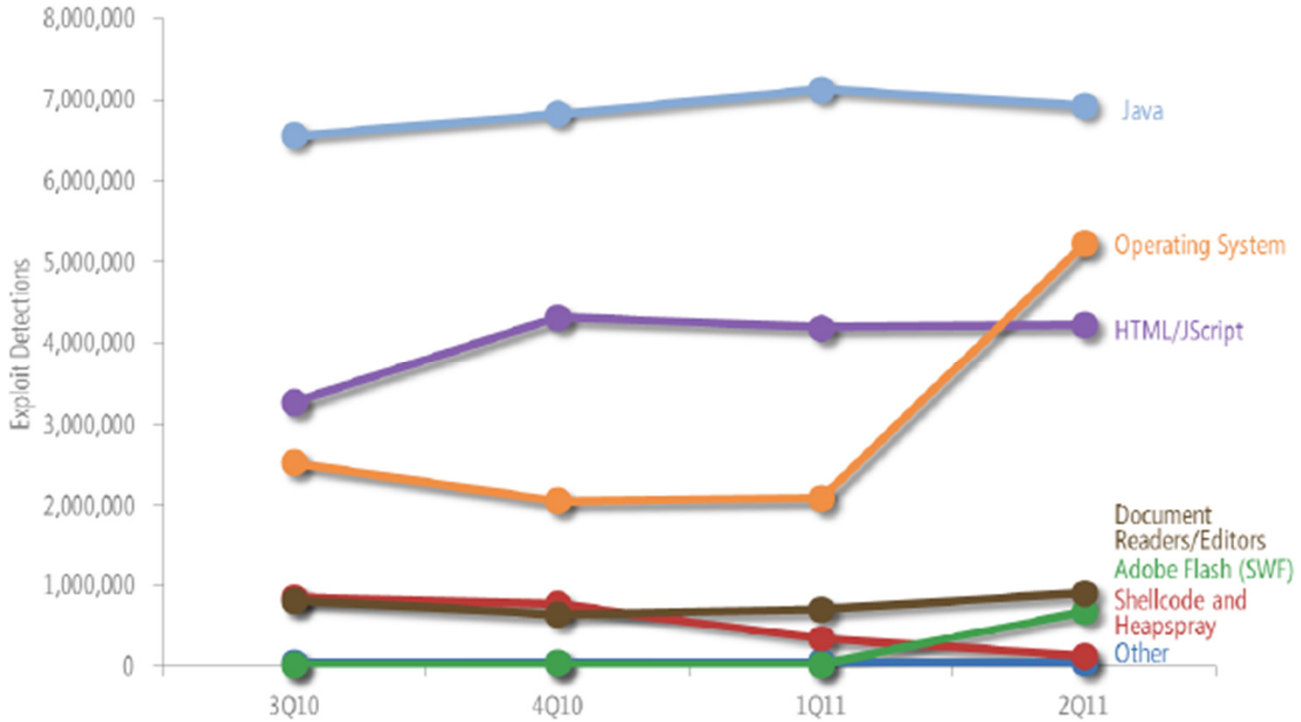
Phishing kommt und geht
… und passt sich an neue Methoden an

- Zugangsdaten
  - Mailaccounts
  - Versteigerungsplattformen
  - Onlinebanking
- TANs
- Kreditkartendaten
- Handysignatur?

- Per Mail
- Manipulation am Client durch Schadsoftware
- Manipulation am Handy durch Schadsoftware

www.cert.pl

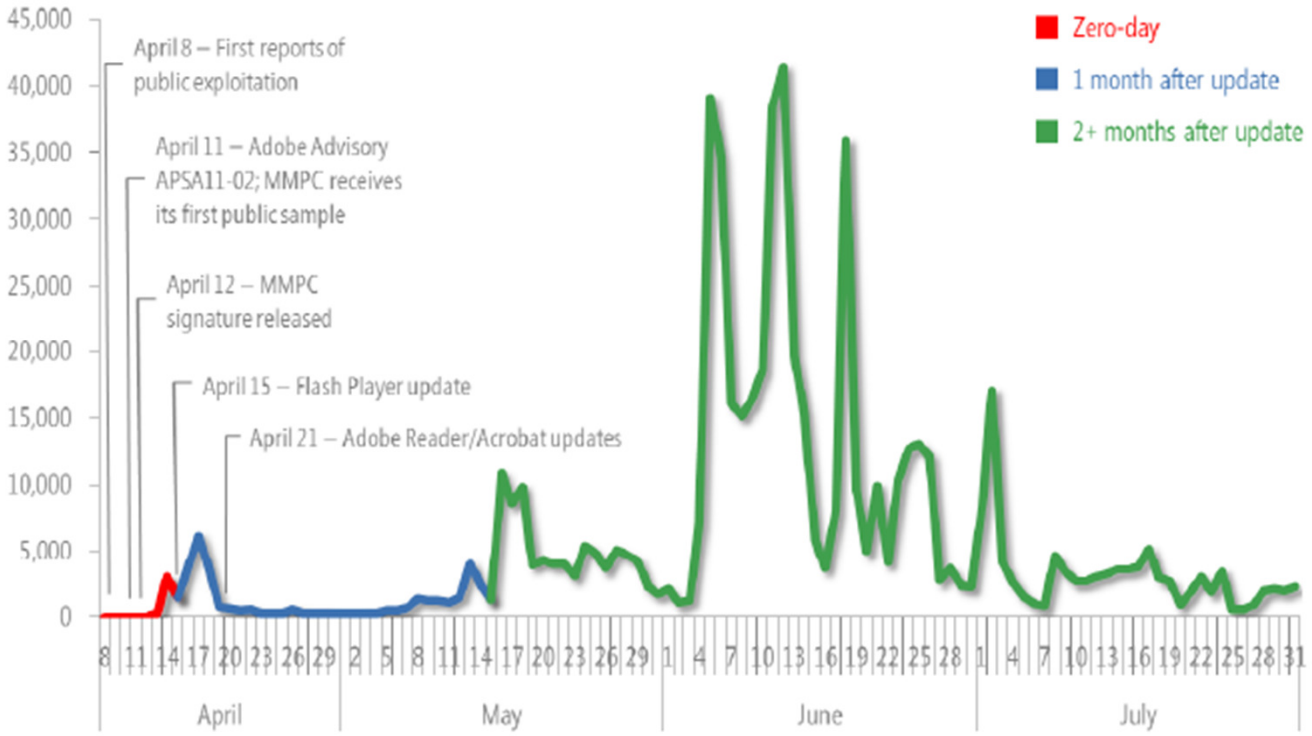
Betriebssysteme sind nicht mehr das größte Problem …



Quelle: Microsoft Security Intelligence Report Vol. 11
Exploits 3Q10 – 2Q11

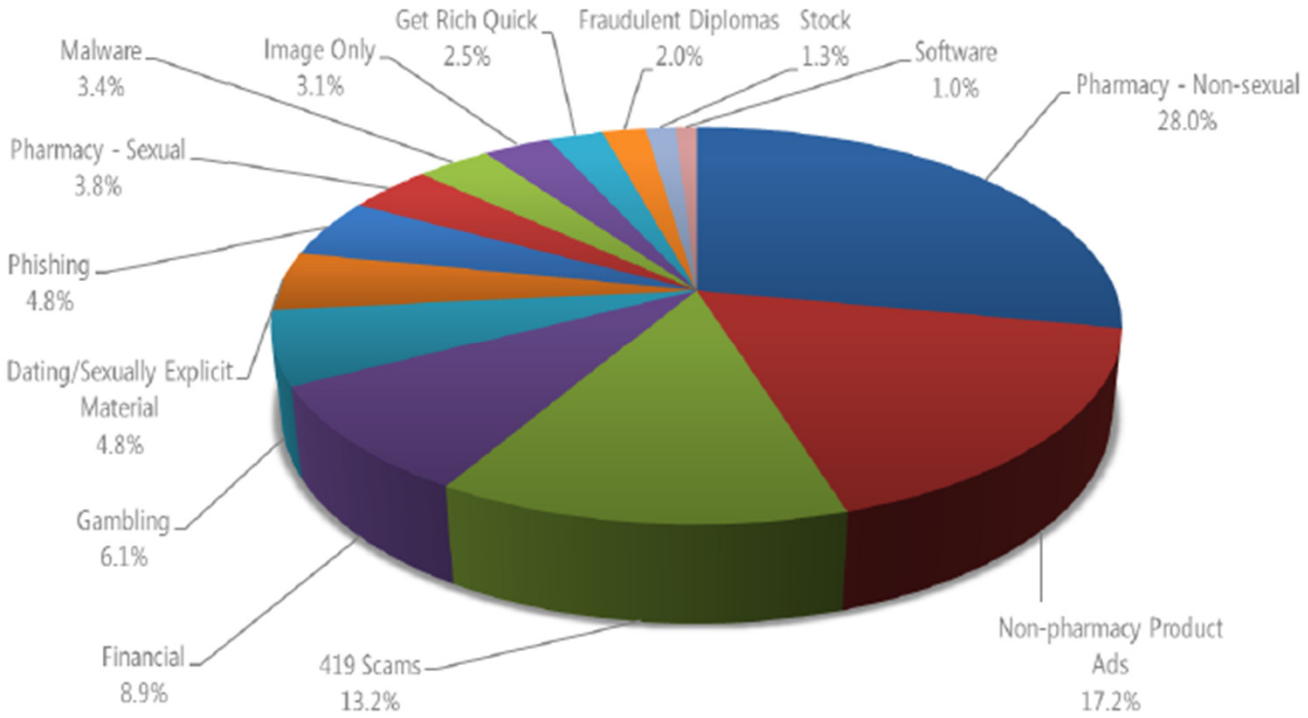
0-Day … oder doch nicht mehr ganz frisch?

Figure 6. Detections of exploits targeting CVE-2011-0611, April–July, 2011



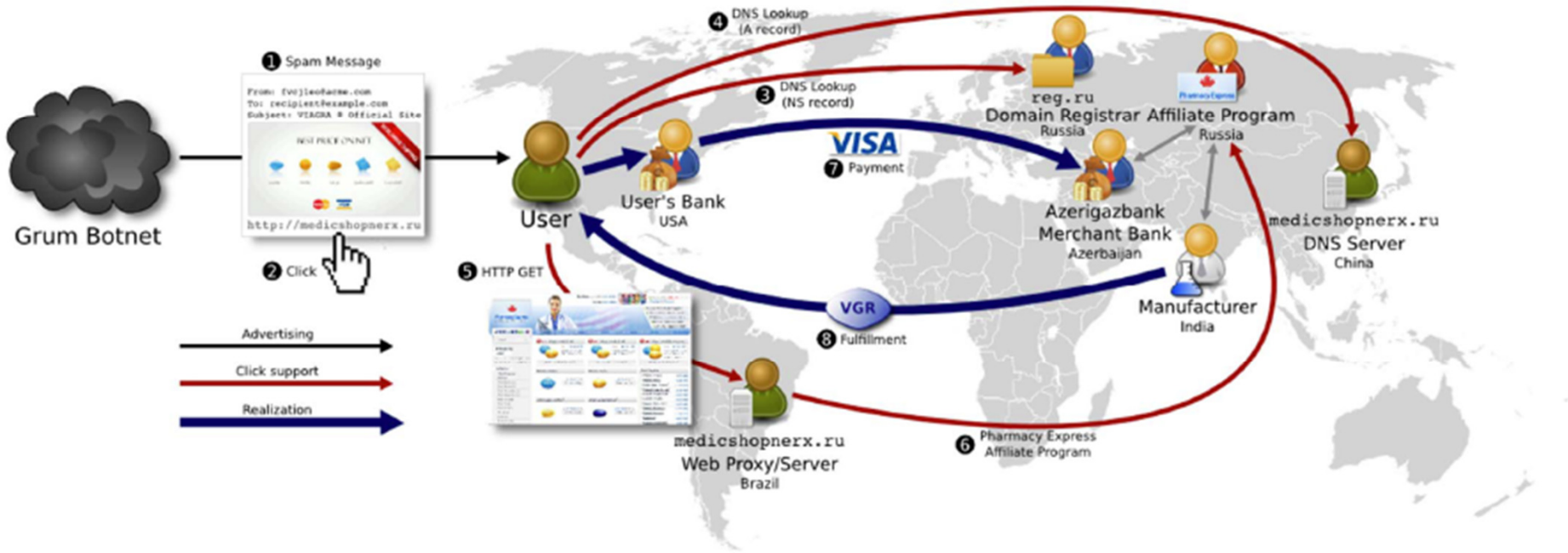
Quelle: Microsoft Security Intelligence Report Vol. 11
Detections of exploits targeting CVE-2011-0611, April–July, 2011

Und manche Problem bleiben …



Quelle: Microsoft Security Intelligence Report Vol. 11
Email - Threats

Das SPAM Ecosystem



Quelle: The Spam Ecosystem: Demand, Revenue and Payments
UCSD Steve Savage

Основные сайты

Brushy

Always great

Bondi Blue

Kettlebell

Life Meant to be

Bench in a park

Stallions RX

Loose weight orangy

Mostly laconic

Red on green

Infrastruktur Angriffe

- weitaus weniger bekannt in der Öffentlichkeit als zB Phishing
- aus Sicht der Relevanz für die Gesellschaft als Ganzes aber wesentlich relevanter
- pot. sehr große Zahl Betroffener in kurzer Zeit
- auch für aufmerksame Benutzer oft nicht erkennbar

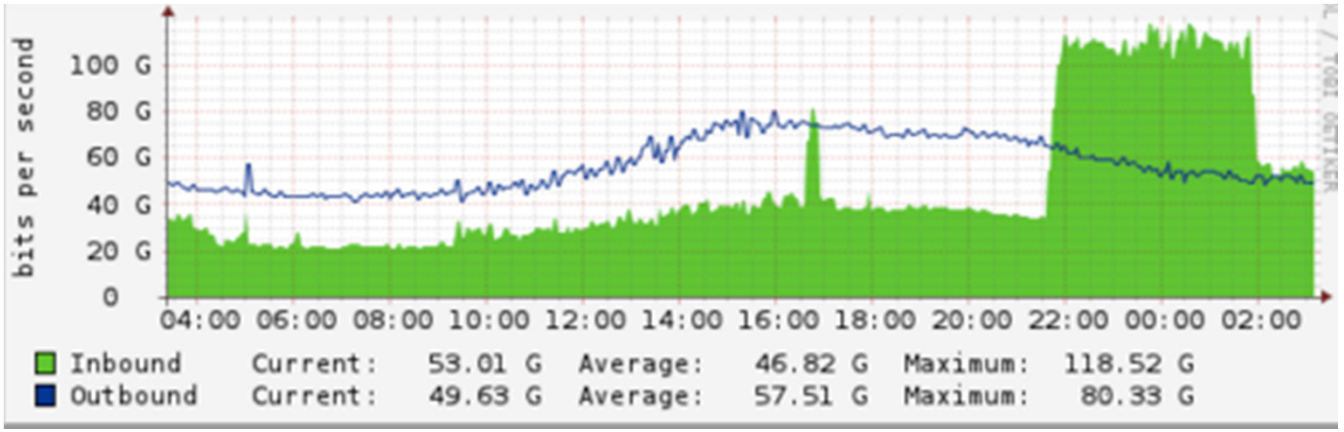
- Beispiele:
  - DDOS-Angriffe
  - Manipulationen des Routings (BGP)
  - DNS-Spoofing
  - Umleitungen im DNS
  - Ausstellung gefälschter Zertifikate – zB DigiNotar in NL
  - Angriffe auf Authentisierungssysteme zB RSA
  - Gefälscht Hardware

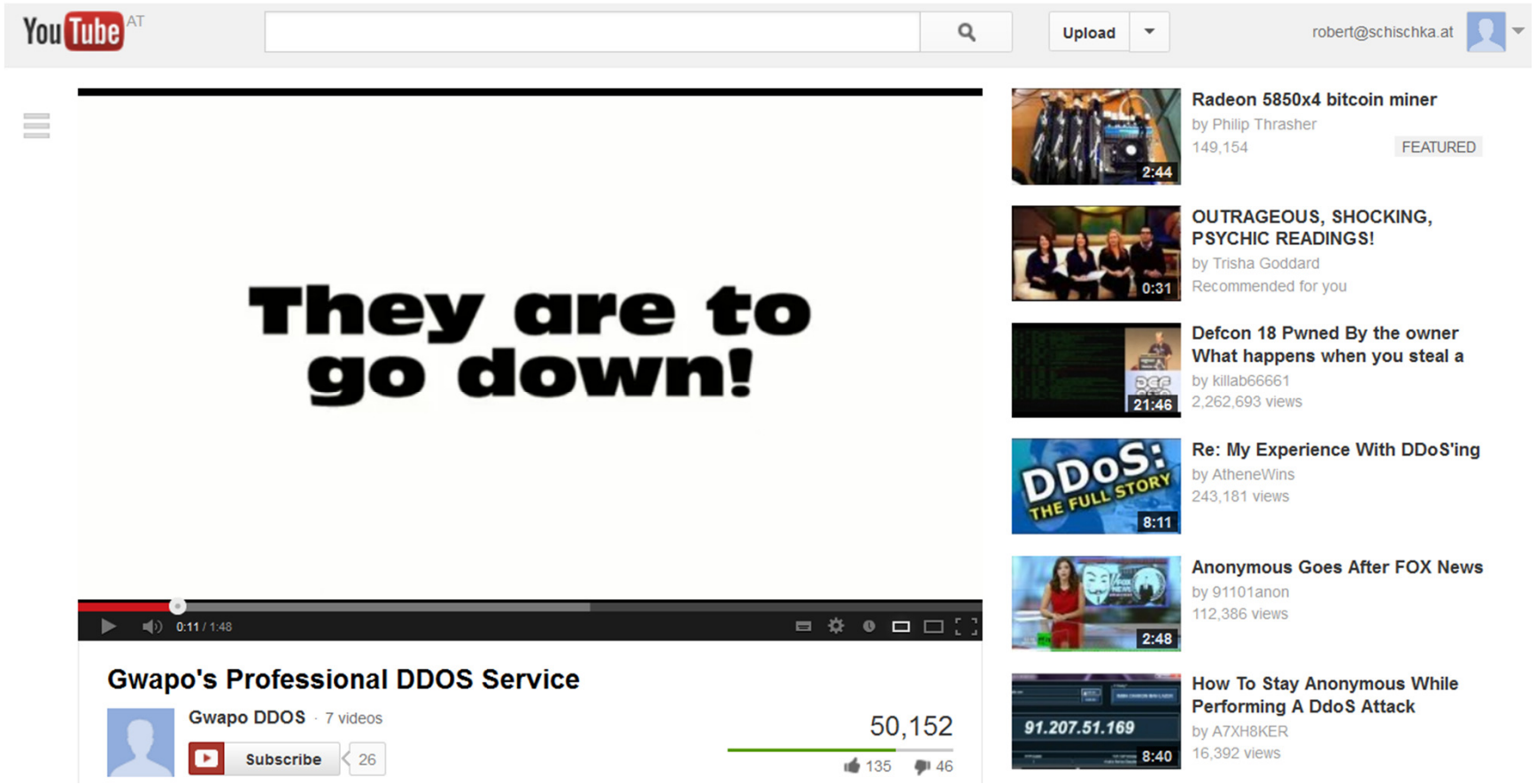
DDOS-Angriffe

- Botnetze - das „Schweizer Taschenmesser“ der Underground Economy erlauben sehr einfach alle Arten von Angriffe
- zunehmende Leistungsfähigkeit der Endgeräte
- Breitbandpenetration → „always on“, fibre to the home ….
- Je nach Applikation ist es nicht trivial DDOS-Angriffe von lediglich „hoher Last“ zu unterscheiden
- DNS wird häufig angegriffen – meist auf Ebene ROOT-Server oder direkt Unternehmensserver oder bestimmte ISPs
- DNS-Reflection-Attacks nehmen stark zu – geringer Anfrage-Traffic führt so hohem Antwort-Traffic der auf „Opfer“ umgeleitet wird
- Angriffe im Bereich von 10-150 Gbit keine Seltenheit
- …. könnte Ihre Infrastruktur damit umgehen, wie sind sie vorbereitet?

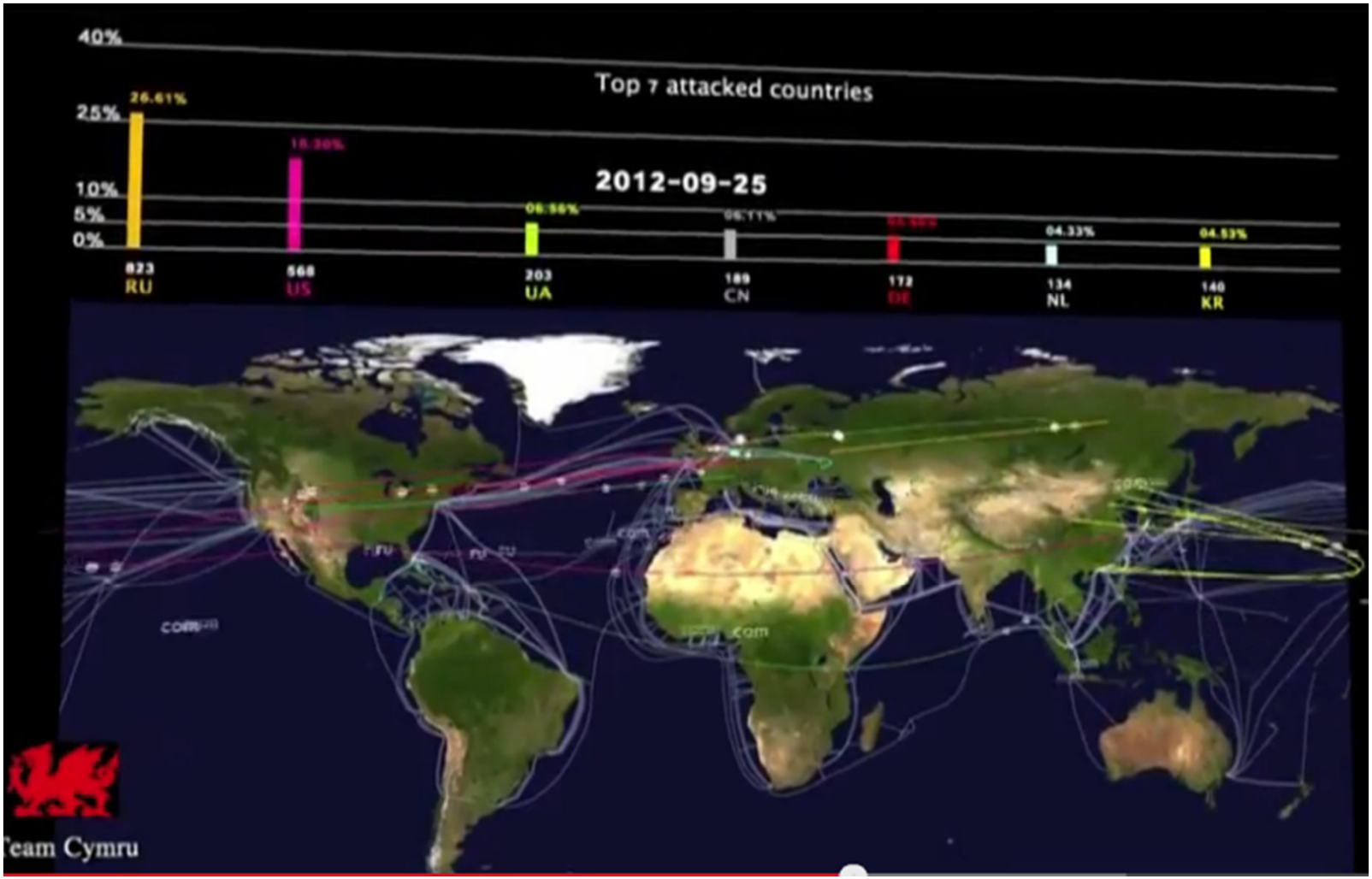
Aktueller DDOS-Fall

- Gegen SpamHaus Webserver
  - DNS Reflection (AFAIK)
- CloudFlare macht Mitigation
  - http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho
  - 75 Gbit/s Layer 3 Attack – Maximal Wert war 300 Gbit/s !!



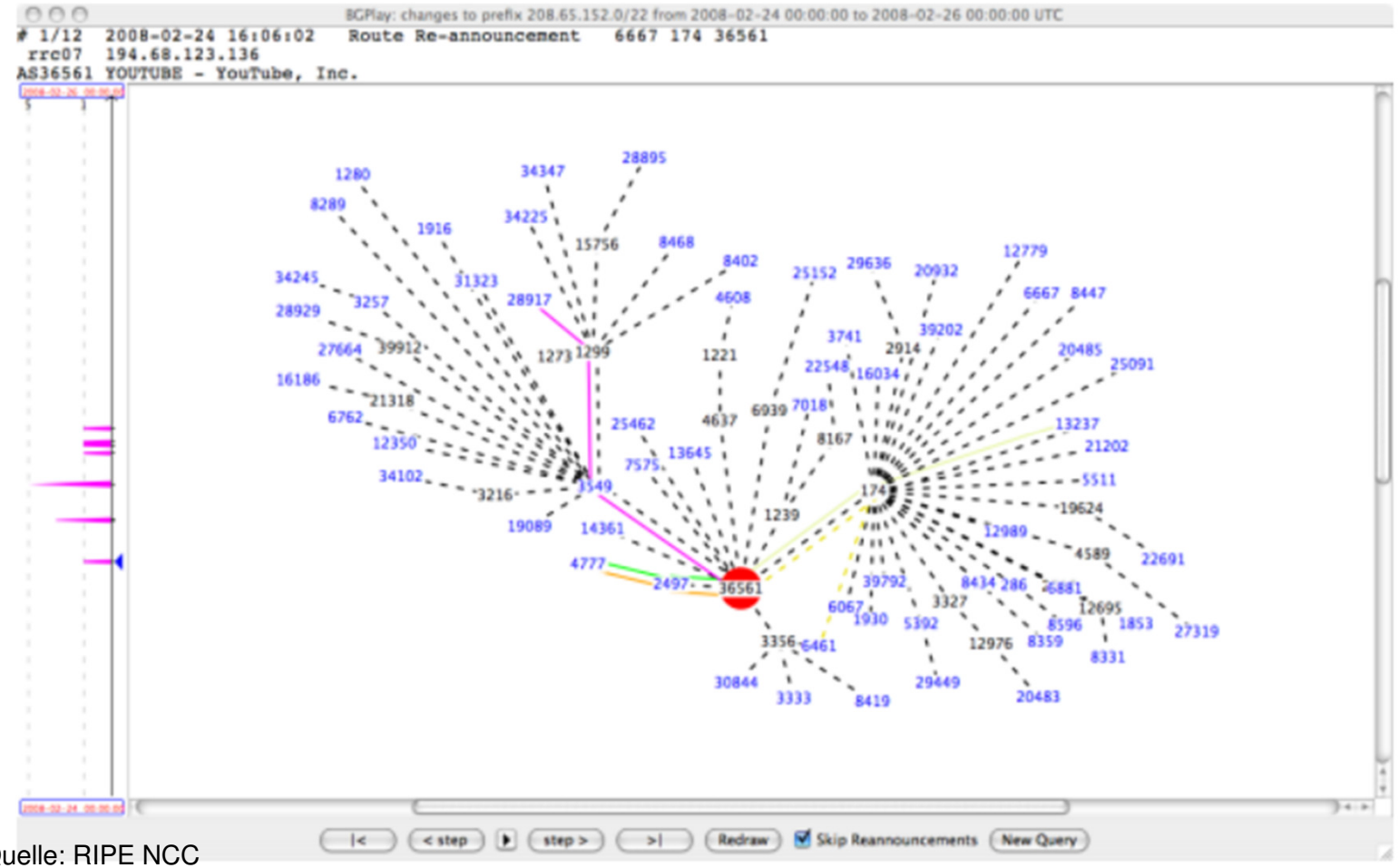

YouTube AT
Upload
robert@schischka.at
They are to go down!
0:11 / 1:48
Gwapo's Professional DDOS Service
Gwapo DDOS · 7 videos
Subscribe 26
50,152
135 46
Radeon 5850x4 bitcoin miner
by Philip Thrasher
149,154 FEATURED
2:44
OUTRAGEOUS, SHOCKING, PSYCHIC READINGS!
by Trisha Goddard
Recommended for you
0:31
Defcon 18 Pwned By the owner What happens when you steal a
by killab66661
2,262,693 views
21:46
Re: My Experience With DDoS'ing
by AtheneWins
243,181 views
DDoS: THE FULL STORY
8:11
Anonymous Goes After FOX News
by 91101anon
112,386 views
2:48
How To Stay Anonymous While Performing A DdoS Attack
by A7XH8KER
16,392 views
91.207.51.169
8:40

Die Welt ist „komplizierter“ als es oft scheint …



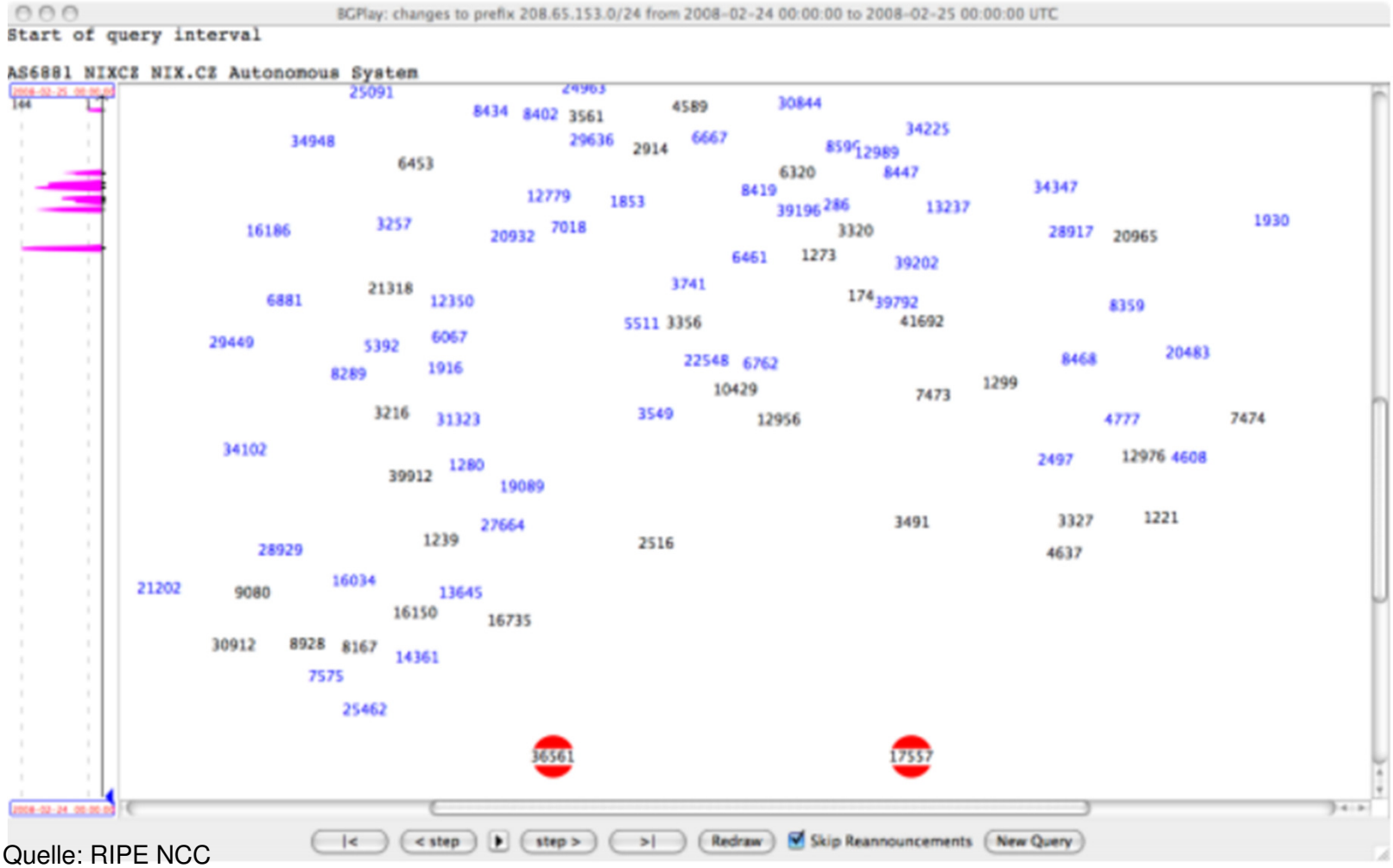
Before, during and after Sunday, 24 February 2008

AS36561 (YouTube) announces 208.65.152.0/22



Quelle: RIPE NCC
http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

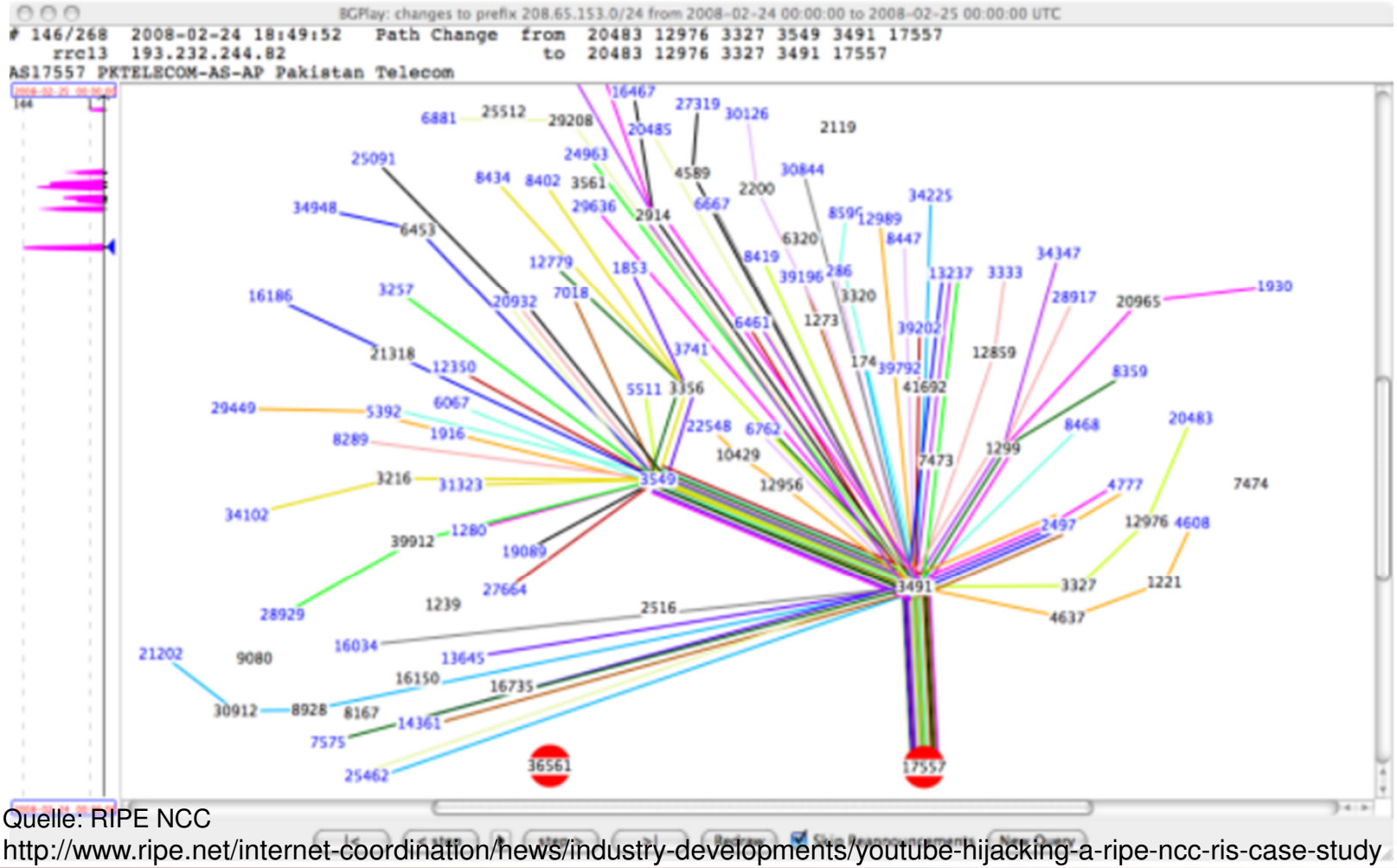
The prefix 208.65.153.0/24 is not announced on the Internet before the event:



Quelle: RIPE NCC
http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

Sunday, 24 February 2008, 18:49 (UTC)

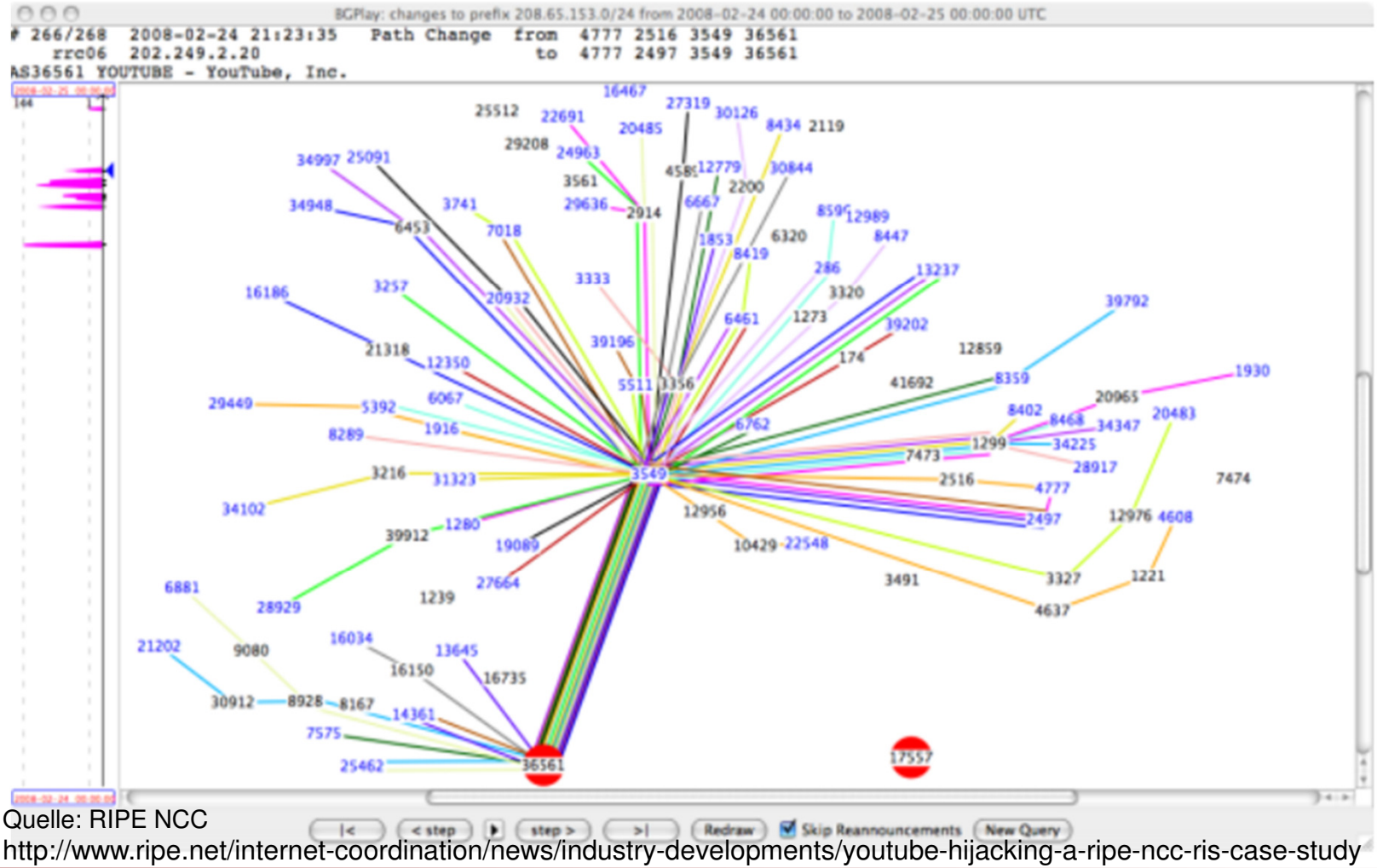
AS17557 (Pakistan Telecom) has been announcing 208.65.153.0/24 for the past two minutes. RIS peers around the world have received the route update, and YouTube traffic is being redirected to Pakistan.



Quelle: RIPE NCC
http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

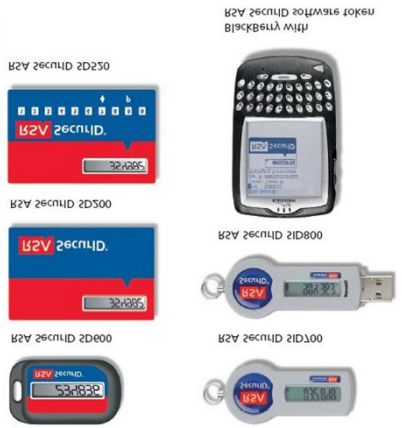
Sunday, 24 February 2008, 21:23 (UTC)

AS36561 (YouTube) has been announcing 208.65.153.0/24 since 20:07 (UTC). The bogus announcement from AS17557 (Pakistan Telecom) has been withdrawn, and RIS peers now only have routes to YouTube's AS36561



Quelle: RIPE NCC
http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

Fallstudie RSA



- Oberflächlich betrachtet:
  - Kein System ist 100% sicher
  - auch bei einem Security-Hersteller kann es Incidents geben

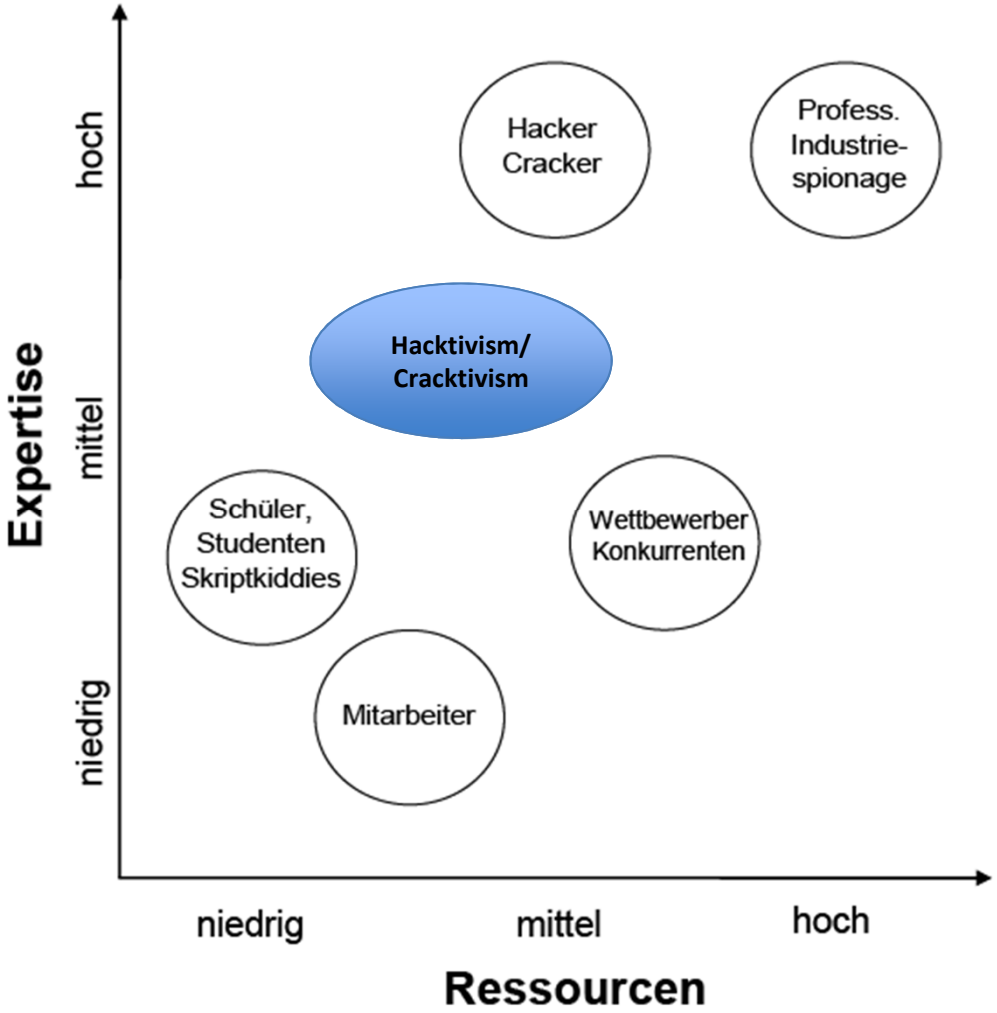
- 2-ter Blick:
  - Vorfall wurde lange heruntergespielt
  - „Informationspolitik“ →NDA
  - Hoffnung PR-Desaster zu verhindern währte nur kurz
  - Austausch der Hardware-Token musste letztlich trotzdem erfolgen
  - aber inzwischen waren Kunden gefährdet → Lockheed Martin …
  - Kernfrage: Warum speichert jemand überhaupt Seed-Values seiner Kunden?
  - Wer ist das eigentliche Ziel? Wie sicher sind ihre Lieferanten?

Gefälschte Hardware – Zusatzfunktionen?

b

Source: <http://www.usedcisco.com/press-my-esm_used_cisco_identifying_fake_chisco.aspx>

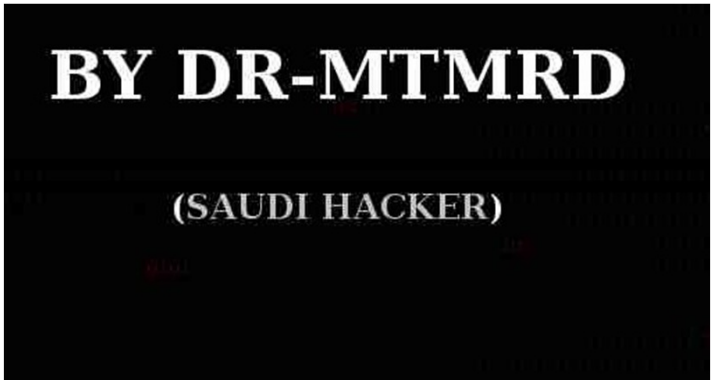
Was ist die Motivation dahinter?



- Persönliche Motive
  - Rache
  - Ruhm
- Politische Motive
  - „Suicide Hacker“
- Hacktivism/Cracktivism
- Ökonomische Motive

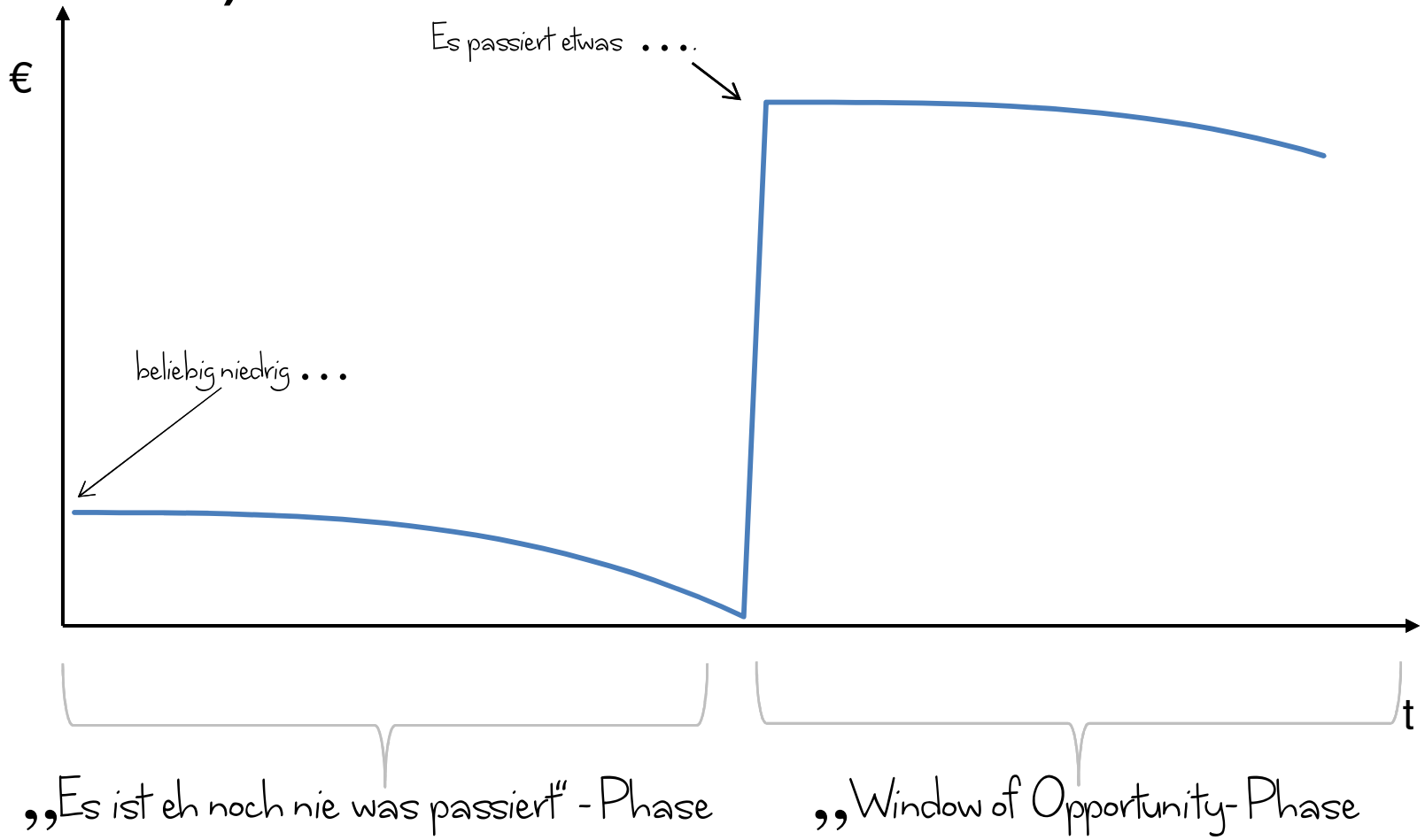
Quelle: Effiziente Reduktion von IT-Risiken im Rahmen des Risikomanagementprozesses, ISEB

Defacements - for fun?

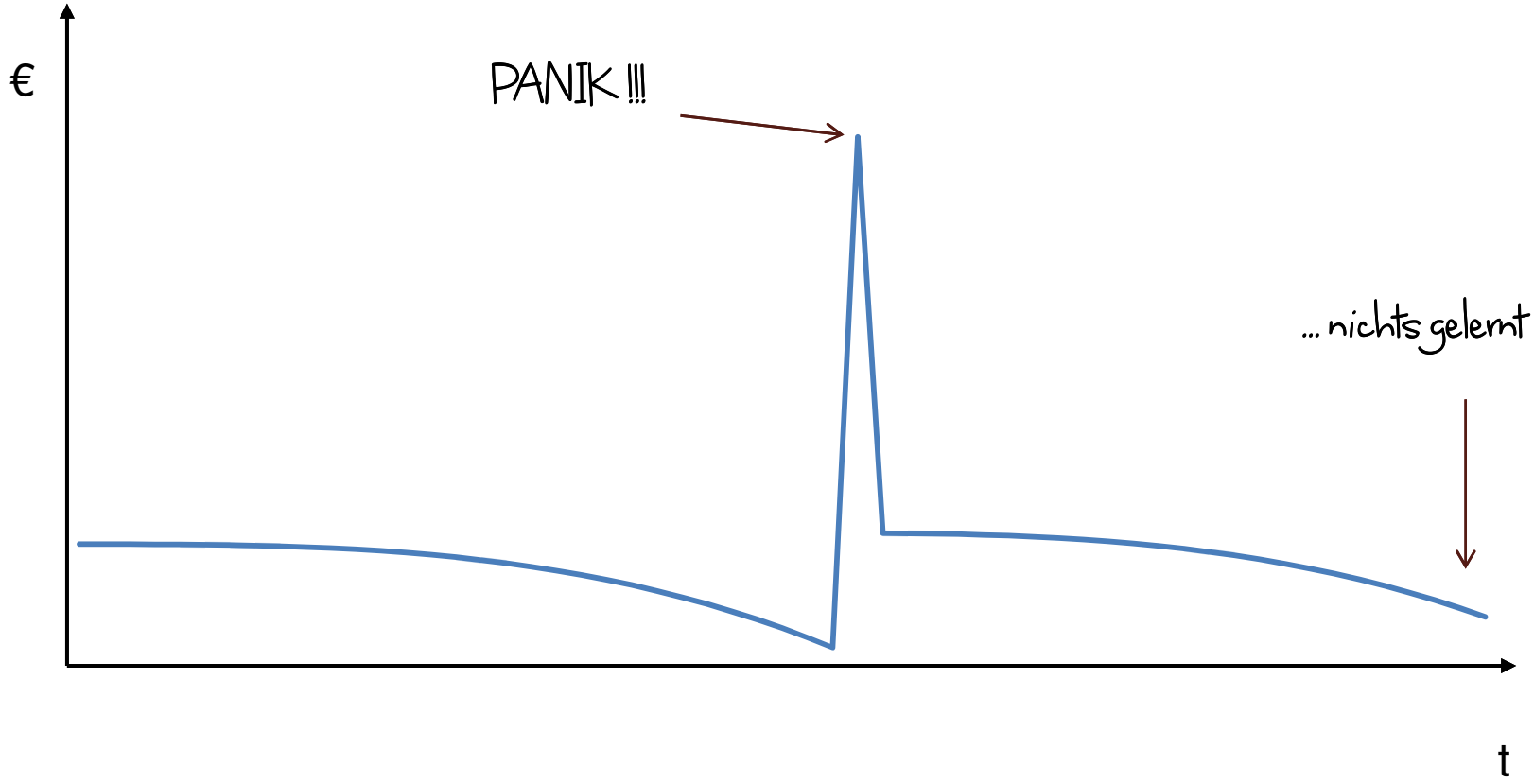



[' OR '1' = '1] For Teh Lulz
„The leak was about this big"
I2P-IRC
#AntiSec
#anon-austria
#anon-germany

Investitionsbereitschaft für IT-Sicherheit (klassisch)



Investitionsbereitschaft für IT-Sicherheit (manchmal auch so …)



Einige Gedanken zur Gefährdungen

- APT und 0-Days sind real ….. aber selten „nötig“
- der weitaus überwiegende Teil der Angriffe benötigt Benutzer-Interaktion
- Social-Engineering wichtige Komponente von vielen erfolgreichen Angriffen
- Fast immer hat es zum Angriffszeitpunkt bereits Updates oder Gegenmaßnahmen gegeben
- Unternehmen mit hinreichend komplexer IT müssen davon ausgehen, dass es Sicherheitsereignisse geben wird
- Ausbau von Response-Fähigkeiten ist daher unumgänglich – Erfahrungen aus der Vergangenheit („… nie etwas passiert ..“) können nicht unbedingt für eine Prognose herangezogen werden
- Krisenkommunikation ist ein wesentlicher Teil des Response-Prozesses – Kommunikationskanäle und Anforderungen haben sich in den letzten Jahren massiv verändert. „Unter der Decke halten“ ist heute immer schwieriger bis nahezu unmöglich
- „Schießen auf den Boten“ ist kontraproduktiv

Fragen?

Kontakt:
Robert Schischka
Karlsplatz 1/2/9, 1010 Vienna, Austria
email: schisch@cert.at

www.cert.at