Angriff auf Estland

Bernhard Tittelbach

RealRaum Graz

7. Mai 2009

"Cyber-Attacke" auf estländische Infrastruktur
vor Hintergrund innenpolitischer Integrationsprobleme

Outline

Estland / Internet-Land

- Hauptstadt: Tallinn
- Unabhängigkeit seit 1991
- 1,3 Millionen Einwohner
- $\frac{1}{3}$ russischer Herkunft
- neoliberales Wirtschaftssystem
- starkes Wirtschaftswachstum
- NATO u. EU Mitglied seit 2004
- TLD .ee
- staatliche Garantie auf kostenlosen Internetzugang, frei nutzbare WLANs

Estland in Europa (David Liuzzo, Wikipedia)

Estland / Internet-Land

- Internetbanking seit 1997
  - fast 100% Nutzung
  - Studie: 17% weniger online-Banking wäre nicht bewältigbar
- Personalausweis / PKI Chipkarte
- e-Goverment Musterschüler
  - Nutzung bes. durch Unternehmen
  - Krankenversicherung, Steuererklärung, Anträge
- Internet-Voting
  - Kommunalwahlen Oktober 2005
  - Parlamentswahl März 2007
- SMS-Voting 2011

Estland in Europa (David Liuzzo, Wikipedia)

Estland - Geschichtlicher Hintergrund

1885.. Russifizierungskampangne

1939 Deutscher Geheimvertrag mit Russland

1940 Russland annektiert Lettland, Litauen und Estland

↓ russische Ansiedelungspolitik

1988.. Loslösung von der Sowjetunion

1991 Wiederherstellung der Staatsouveranität

↓ Einführung: neoliberales Wirtschaftssystem u. schlanke transparente Verwaltung

1999.. stetig steigendes Wirtschaftswachstum

2004 NATO- und EU-Beitritt

Estland in Europa

Angriff auf Estland via Internet

Im Vorfeld:

- Verlegung russischen Kriegerdenkmals
  von Hauptplatz Tallinn auf Militärfriedhof

Symbolträchtig:

estn. Russen: 30 Mill. russ. Kriegsopfer im 2. WK

Estländer: 51 Jahre russische Besatzung und Unterdrückung

- Protest aus Moskau - Ernste Konsequenzen angedroht
- friedliche Proteste $\longrightarrow$ Straßenkrawalle
- Toter 19-jähriger russischer Demonstrant

Angriff via Internet: 3 Wochen Chaos

- 27. April 07, Freitag Abend, DDOS-Attacke startet
  Regierungs-Seiten/e-Gov nicht mehr erreichbar
- Defacement estnischer Webseiten, XSS, anti-estnische Propaganda
- 1.Mai, Webseiten russischer Oppositionsgruppen „down“
- graduell stärker werdende Attacken
- 4.Mai, Angriff auf größte estländische Zeitung „Postimees“
- 6.Mai, Angriff auf größte estländische Bank „Hansapank“
- 9.Mai, DDOS-Höhepunkt, russ. Feiertag Sieg über Hitler
- 11.Mai: Attacken flauen ab
- 16.Mai: Angriff auf zweitgrößte Bank „SEB Eesti Ühispank“
- 18.Mai: Online-Zeitungen u.-Banking wieder erreichbar

Während des Angriffes bekannte Fakten (1)

- Keine Erpressungsversuche
- Kein Datendiebstahl
- Keine Attacke auf kritische Regierungsinfrastruktur

Statistiken von Arbor Networks, Jose Nazario

- 128 unabhängige DDoS Attacken:
  - 115 ICMP Flooding
  - 4 TCP SYN Floods
  - 9 Floods mit generischem Traffic
- verschiedenste Bandbreiten und Dauer:
  - unter 10 bis 95 MBit/s.
  - Hauptsächlich zw. 10 und 30 MBit/s
  - 3/4 der Angriffe dauerten maximal eine Stunde
  - 5.5% länger als 10h

Während des Angriffes bekannte Fakten (2)

- Nicht Einheitlich, Komposite-Attacke:
  - Skriptkiddies (low skill)
  - Bot-Netze (high skill)
- P2P organisiertes Botnetz, vermutlich Storm
- Ziele: Web-Seiten und -Dienste
  - estländische Regierung und Außenministerium
  - estländischer Banken
  - bekannter Politiker und Parteien (Liberale Reform Partei)
  - russischer Oppositionsgruppen
    - Websites des Anderen Russlands
    - Partei der Nationalbolschewisten

Beeinträchtigungen

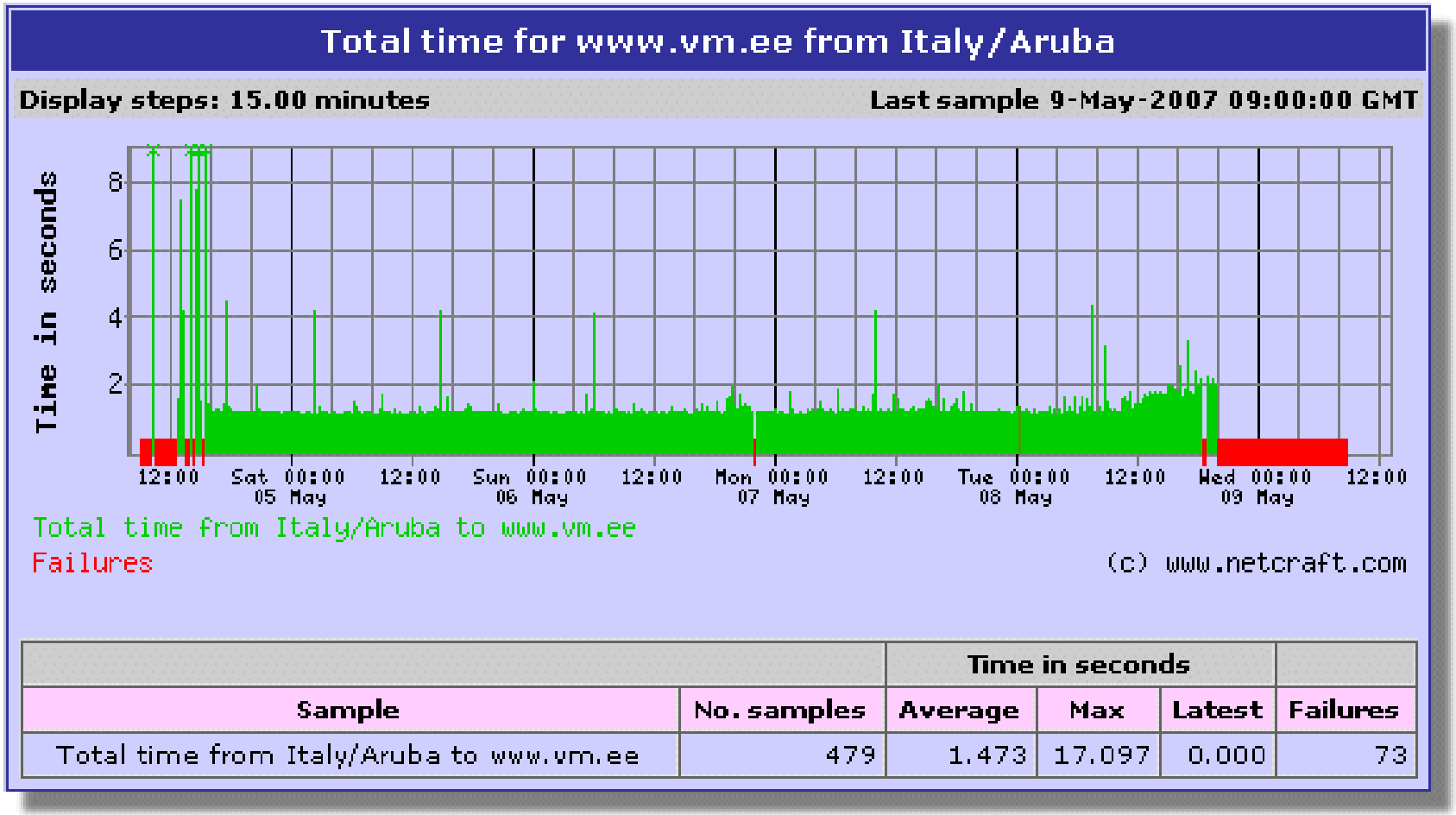
- E-Goverment
- Kreditkartenzahlungen (Ende April)

  Tanken und Einkauf von Konsumgütern teilweise unmöglich
- Online-Banking (Tagesweise offline)
- Nachrichten und Informationsdienste
- E-Mail-System des Parlaments

Verteilung der Angriffe auf Ziele (Jose Nazario)

Attacken	Ziel	IP Eigentümer
35	195.80.105.107	pol.ee
7	195.80.106.72	www.riigikogu.ee
36	195.80.109.158	riik.ee, peaminister.ee, valitsus.ee
2	195.80.124.53	m53.envir.ee
2	213.184.49.171	www.sm.ee
6	213.184.49.194	www.agri.ee
4	213.184.50.6	
35	213.184.50.69	www.fin.ee (Ministry of Finance)

Beeinträchtigungen Ping-Statistik



		Time in seconds			
Sample	No. samples	Average	Max	Latest	Failures
Total time from Italy/Aruba to www.vm.ee	479	1.473	17.097	0.000	73

Arbor Networks, Jose Nazario

Politische Reaktionen: Instrumentalisierung I

estnische Botschafterin in Moskau:

Rückverfolgung auf IP Adressen der russischen Regierung deren Kompromittierung als unwahrscheinlich gilt

- estnischer Außenminister beschuldigt Russland (2007-05-17)
- Verteidigungsminister bringt Fall vor EU und NATO

estnischer Ministerpräsident (2007-05-29)

In Estland wurde das Modell eines neuen Cyber-Krieges getestet. [...] Beteiligung Russlands absolut keine Frage

Politische Reaktionen: Instrumentalisierung II

Pressesprecher der Nationalbolschewisten

Eine DDoS-Attacke von solchem Ausmaß kostet nicht weniger als 100.000 Dollar. Unsere politischen Gegner verfügen nicht über solche Summen, daher können wir niemand anderen verdächtigen als den Geheimdienst FSB.

- Moskau beteuert Unschuld (IP Spoofing)

Technische Gegenmaßnahmen

- Angriff auf Unternehmen und öffentliche Dienste
- $\longrightarrow$ Neue Definition von kritischer Infrastruktur

Erstmaßnahmen d. Website-Admins:

- DROP-Rule für ausländ. IPs, im speziellen .ru
- Text-Only Modi
- Traffic Shaping

Technische Gegenmaßnahmen

Im Weiteren:

- EE-CERT: Koordinierte DROP-Rules an TIX Gateways
- Frw. Bürgermeldungen zum Durchkämmen von Router Logs
- Hilferuf an NATO und TERENA[1]
  - Hilfegesuch an akkreditierte Teams und FIRST[2]
  - Besserung innerhalb von 24h
  - ab 3.Mai: CSIRTs[3] aus versch. Ländern helfen Attacken zu blockieren
- oberste Priorität: Dienste am Laufen und Erreichbar halten
- Praktische und Schnelle Ad-Hoc Hilfe
- Analyse der Attacke nur wo sofortiger praktischer Nutzen

[1] Trans-European Research and Education Networking Association
[2] Forum for Incident Response and Security Teams
[3] Computer Incident Response Team

Hintergrund - Kreml ?

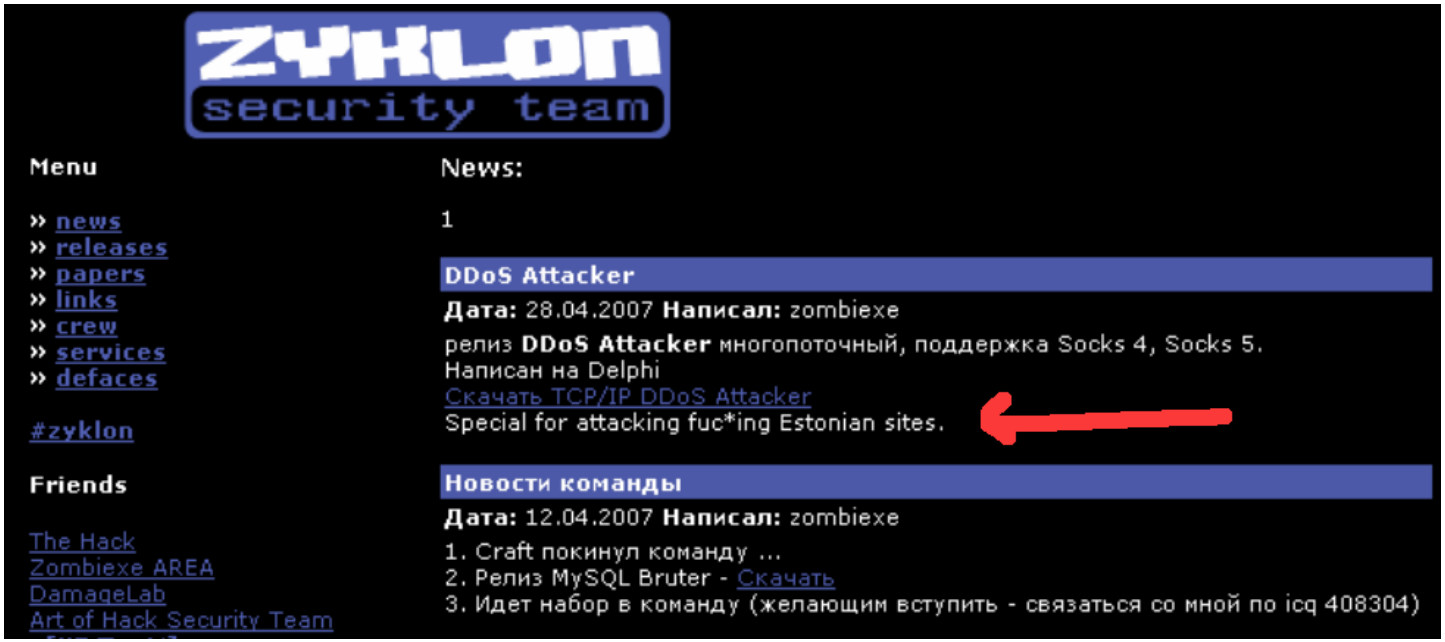
- FSB bekannt für gezielten Einsatz von „Cyber-Slander„
- Für Kreml war Attacke aber zu primitiv
- EE-CERT Aarelaid (2007-06-12):

  „Keine Beweise daß Russland hinter Angriffen“

- Kooperation mit estländischer Untersuchung hat Moskau eindeutig ausgeschlossen.

Hintergrund Volkszorn

- „Cyber-Krawall“, aufgebrachte „Skript-Kiddies“
- Anleitungen und PING/DNS-Flooding Skripte in russischsprachigen Foren
- verantwortlich für kleine bis mittelgroße Attacken



Bot-Net Test

- 20-jähriger estnischer Student Dmitri Galushkevich
- PayPal-Konto, Spendenaufruf in Webforen, Zweck: BotNet-Attacke
- politisches Motiv:
  „War mit Verlegung des Denkmals nicht einverstanden„
- Unbekannter stellt 2 seiner Bot-Netze zur Verfügung
- Bot-Net Attacke mit $100 Mbit/s$ hatte größten Effekt
- Vermutlich BotNet-Test, Demonstration und Werbung
- Verurteilung: Geldstrafe: 1100 Euro (17,500 kroons)
- keine weiteren Verdächtigen seit 2008-01-25

2008-01-25

Nachfolgen

14. Jänner 2008

- 4 (russische) Organisatoren der Massenunruhen vor Gericht
- Erneut DDOS Attacken auf estnische Server
- Volumen vergleichsweise gering
- Diesmal leicht managebar

14. Mai 2008

- Estland erhält NATO-Excellence-Center für Cyber Defense
- Forschungszentrum mit beratender Aufgabe

Schlußfolgerungen

- Neudefinition von Kritischer Infrastruktur: Inter-Unternehmenskommunikation und öffentliche Kommunikation
- Kommunikation und Vertrauen zw. CERTs, CSIRTs, etc war ausschlaggebend.

Artikel und Links I

- http://www.pcworld.com/article/135503/hackers_evaluate_estonia_attacks.html
- http://www.heise.de/newsticker/Unbekannte-attackieren-estlaendische-Regierungs-Websei meldung/89013
- http://www.heise.de/newsticker/Estland-beschuldigt-Russland-des-Cyberterrorismus--/meldung/89857
- http://www.heise.de/security/DDoS-Attacke-auf-Estland-Keine-Verbindung-nach-Moskau-news/meldung/90501
- http://www.heise.de/newsticker/DDoS-Angriffe-auf-estnische-Server-waren-kein-Cyberwar meldung/91055

Artikel und Links II

- http://www.infoworld.com/article/08/01/24/Student-fined-for-attack-against-Estonian-Web-site_1.html
- http://www.heise.de/tp/r4/artikel/25/25218/1.html
- Ö1 Matrix vom 10.02.2008