



Information
Security Society
Switzerland
> *vormals FGSec*



Top 10 Security Trends

Keynote at e-IRT Open Workshop on e-Infrastructure

Audimax HG F30, ETH Zurich
April 24th, 2008

Dr. Thomas Dübendorfer, CISSP
President ISSS / Software Engineer Tech Lead Google
thomas@duebendorfer.ch



Information
Security Society
Switzerland
> vormals FGSec

Economic Value of Information

E-Underground Economy Prices (Symantec)

Goods and Services	Range of Prices
Bank accounts	\$10–\$1000
Credit cards	\$0.40–\$20
Full identities	\$1–\$15
Online auction site accounts	\$1–\$8
Scams	\$2.50/week–\$50/week for hosting, \$25 for design
Mailers	\$1–\$10
Email addresses	\$0.83/MB–\$10/MB
Email passwords	\$4–\$30
Drop (request or offer)	10%–50% of total drop amount
Proxies	\$1.50–\$30

Source: Symantec Corporation, Threat Report 2007, published April 2008

http://www.symantec.com/content/de/de/about/downloads/PressCenter/Internet_Security_Threat_Report-Zusammenfassung.pdf

E-Underground Economy Prices (GData)

- Game Accounts:
 - EUR 6.- per World of Warcraft (WoW) Account
- Renting out a bot network for DDoS Attack:
 - US\$ 20.- / h
 - US\$ 100.- / day
- E-Mail Addresses:
 - EUR 100.- for 10 million email addresses
 - EUR 140.- for do-it-yourself spam starter package:
5 million email addresses with tool for sending email spam included
 - EUR 350.- for 20 million email addresses
- EUR 35.000 per new exploit

Source: GData Newsletter, Oct 22, 2007,
<http://www.gdata.de/unternehmen/DE/articleview/3920/1/160/>



Information
Security Society
Switzerland
> *vormals FGSec*

Critical Infrastructure Outages

Power Blackout Incidents

- **2003 US/Canada Northeast Blackout (Aug 14)**
 - **50 million people** affected; \$6 billion USD losses
 - Cause: FirstEnergy Corporation's failure to trim trees in part of its Ohio service area, then cascading failures
- **2003 Italy Blackout (Sept 28)**
 - **56 million people** affected during 9 hours
 - Cause: Power line which supplied electricity to Italy from Switzerland damaged by storm, then cascading failures
- **2005 SBB Switzerland Blackout (June 22)**
 - **100'000 passengers captured in trains**
 - Full SBB train network comes to a halt
 - Cause: Too little power in Tessin with cascading effects
- **2008 Florida Blackout (Feb 26)**
 - **2.5 million people** affected
 - Cause: Overheated voltage switch caught fire in a power substation near Turkey Point Nuclear Generating Station

Data Link Outages

- **2006** (Dec 26) Taiwan/Hong Kong:
 - **Six out of seven submarine cables snapped by earthquake** off Taiwan
 - Internet connectivity back to normal after 50 days.
- **2007** (May 3-11): **12 DDoS attacks** at 70+ Mbps on Estonian websites; 7 attacks lasting for 10+ hours
- **2008** (Jan/Feb):
 - **9 cuts of three submarine Internet cables** in the Mediterranean, Suez Canal, Persian Gulf, near Bandar Abbas in Iran and near Penang, Malaysia
 - **91 million people** affected



Sources: <http://home.att.net/~thehessians/quakethreat.html>,
<http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/>



Information
Security Society
Switzerland
> *vormals FGSec*










Bot Networks

Kraken Bot Network

- April 13, 2008:
 - **495,000 computers** in the Kraken botnet
 - botnet has infiltrated 50 Fortune 500 companies
 - largest known active bot network
- Infection path:
 - Manipulated web image that installs a trojan downloader binary (and possibly other infection paths)

Source: http://www.damballa.com/mediacenter/kraken_info.php

Active Bot Networks (ATLAS/Arbor)

COUNTRY	ASN	HOST				
Country	Rank	Attacks per subnet	Scans per subnet	Botnets	Phishing	DoS
 CN (China)	1	419	1.26 MB	27	295	750
 GB (Great Britain)	2	9	25.27 kB	19	47	6759
 US (United States)	3	40	139.20 kB	308	1331	3005
 BE (Belgium)	4	5	146.39 kB	3	0	16
 HK (Hong Kong)	5	0	1.52 kB	6	0	1940
 PL (Poland)	6	26	64.35 kB	8	865	220
 DE (Germany)	7	16	45.10 kB	73	177	692
 ZA (South Africa)	8	0	78.81 kB	2	0	21
 RU (Russian Federation)	9	11	20.08 kB	10	538	619

Source: <http://atlas.arbor.net/>, Apr 22nd 2008



Information
Security Society
Switzerland
> vormals FGSec

Third Parties Controlling Information

Who controls your information?

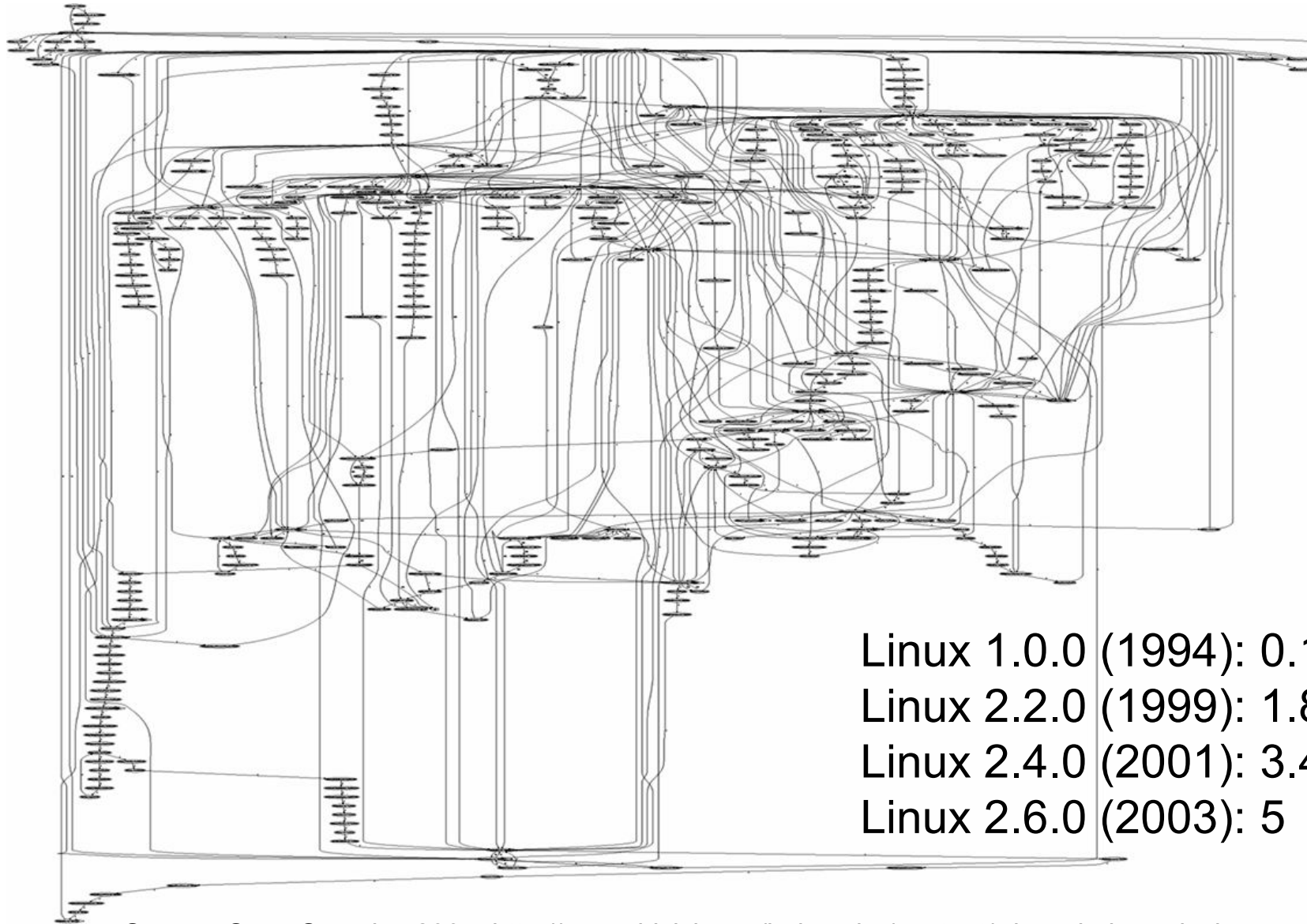
- Webmail
 - 2003 (July 21): Swiss Freemail Provider Sunrise has lost email account data of **550'000 customers** (Freesurf, Freesurf plus und Weboffice)
- Credit Card Records
- Medical Records
- Voice Carriers
 - Paris Hilton / T-Mobile phone data hack



Information
Security Society
Switzerland
> *vormals FGSec*

Complexity

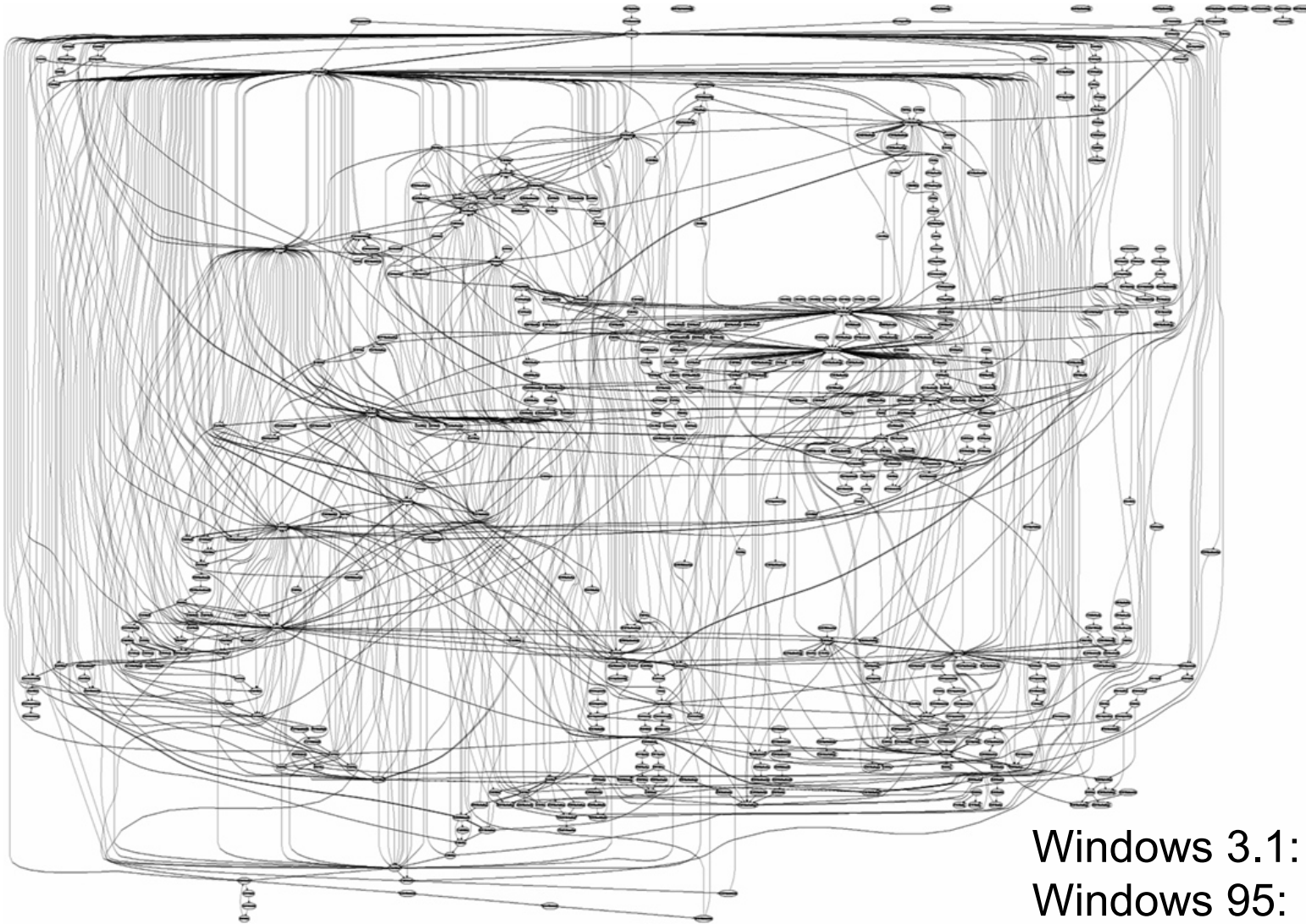
Linux: Serving A Single Web Page (Apache)



Linux 1.0.0 (1994): 0.18 mill. LOC
Linux 2.2.0 (1999): 1.8 mil.
Linux 2.4.0 (2001): 3.4 mill.
Linux 2.6.0 (2003): 5 mill.

Source: Sana Security, 2004; http://www.thisisby.us/index.php/content/why_windows_is_less_secure_than_linux

Windows: Serving A Single Web Page (IIS)



Windows 3.1:	2.5 mill. LOC
Windows 95:	15 mill.
Windows XP:	40 mill.
Windows Vista:	>50 mill.

Source: Sana Security, 2004



Information
Security Society
Switzerland
> *vormals FGSec*

Criminals

Criminals Run E-Underground business

- Biggest threat currently
- Professional! No longer hobbyist hacker that looks for bragging rights
- Lack of worldwide regulations and uniform law enforcement

Crimes:

- Identity theft (steal credentials)
- Industry espionage
- Spam (>70% of all emails in 2007 acc. to Symantec)
- Nigerian Money Scams
- DDoS extortion: sport bet sites etc.
- ... and many more

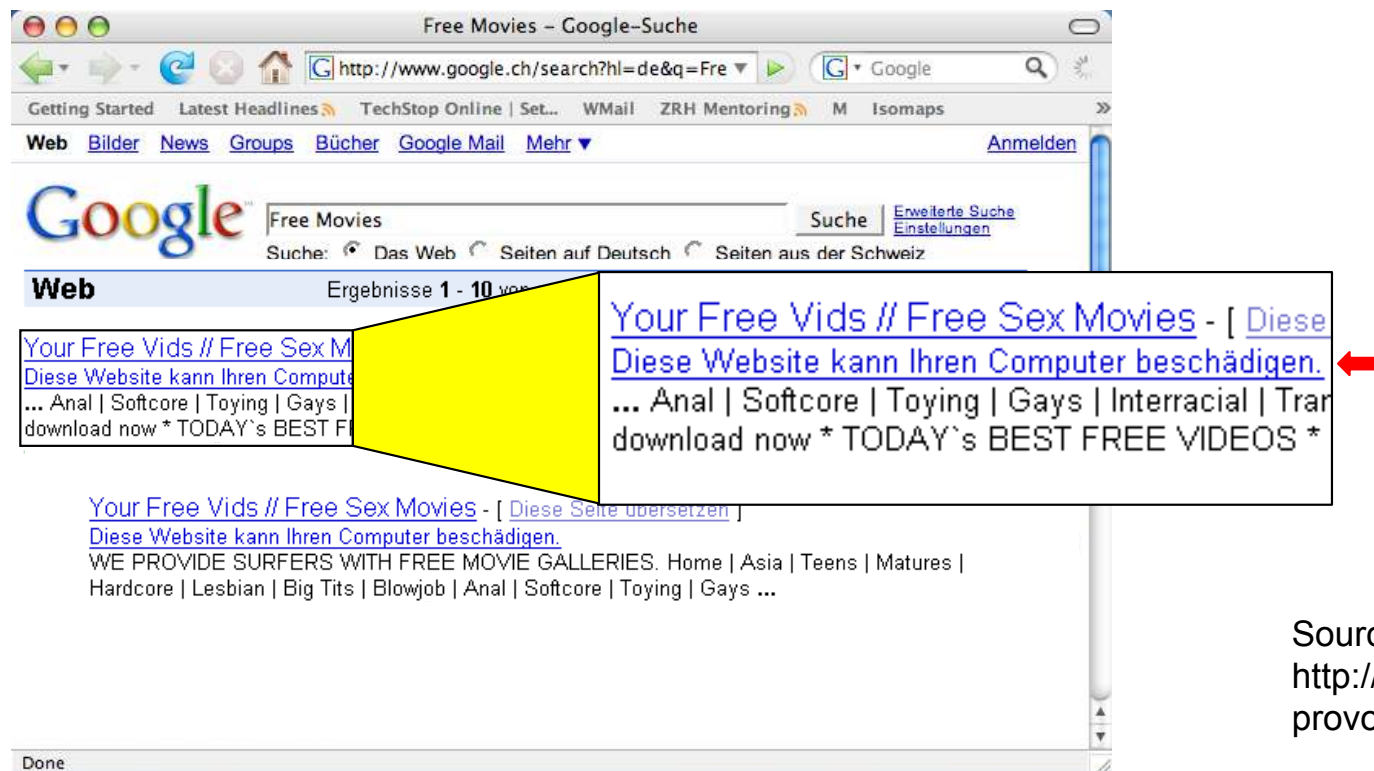


Information
Security Society
Switzerland
> *vormals FGSec*

Drive-By Downloads (Web Browser Exploits)

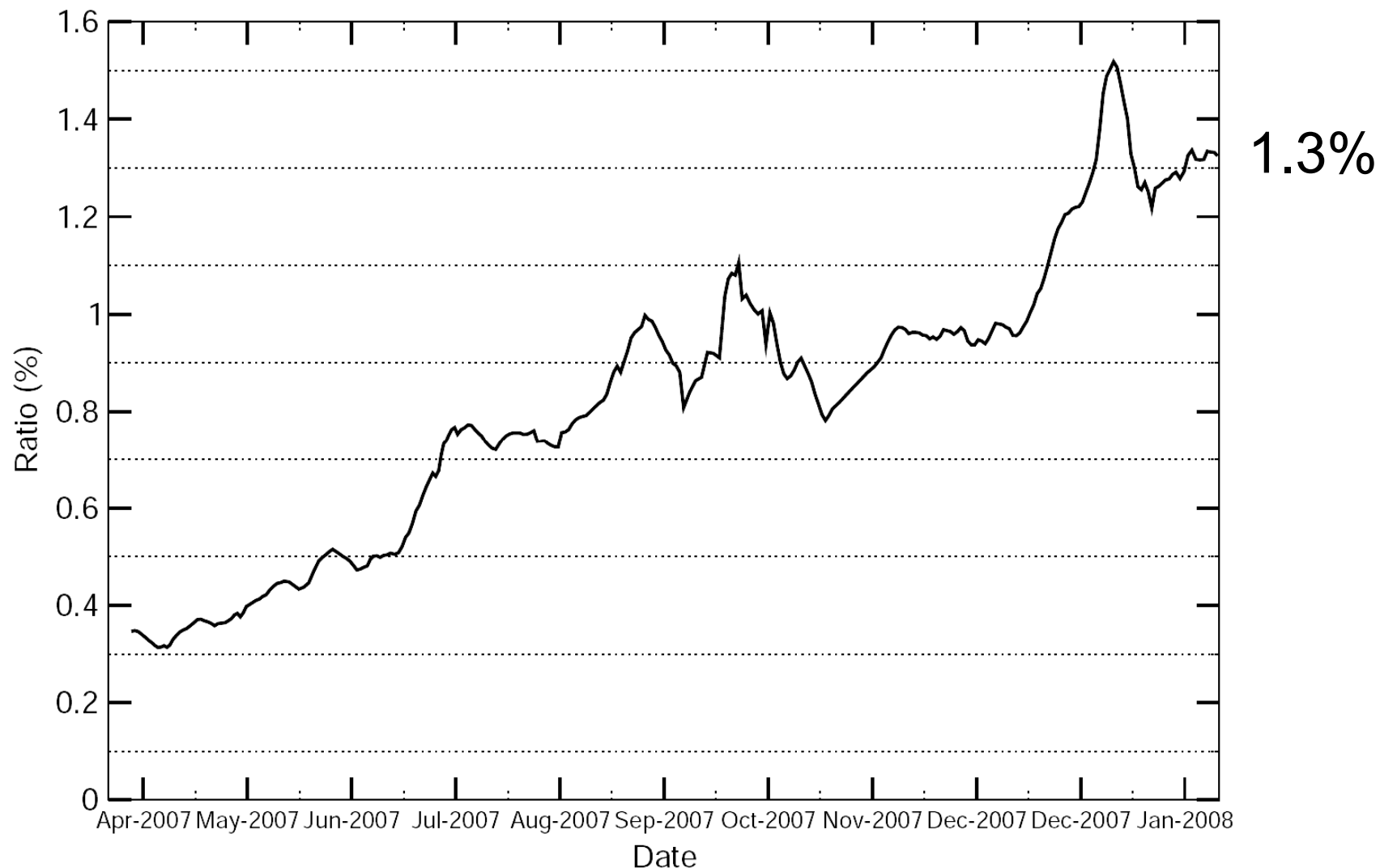
Malicious Web Sites

- >3 million web sites are known to be malicious
- Popular exploits are linked from >10,000 web sites
- Domains with malicious URLs marked „may harm your computer“ on Google's search result page.



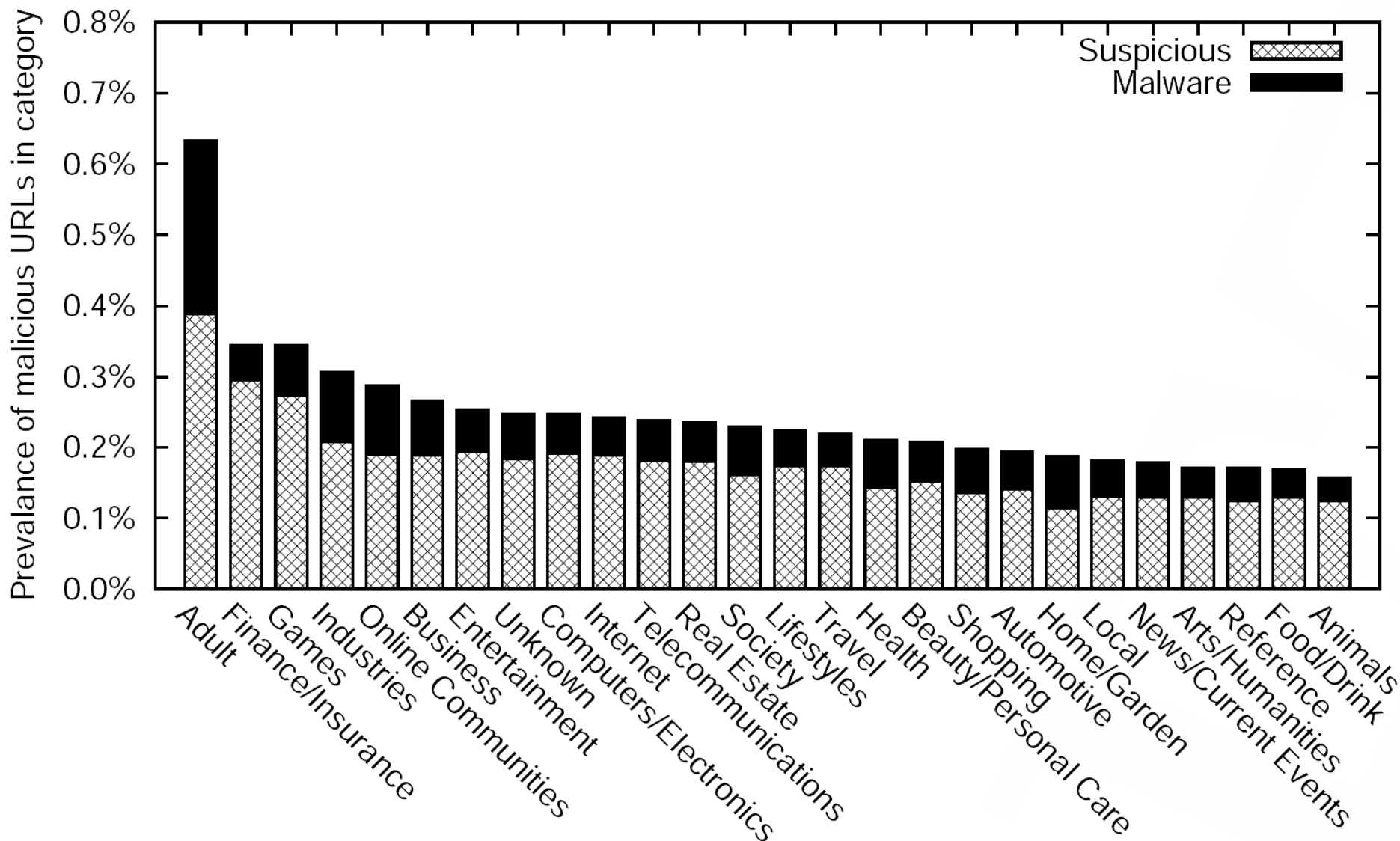
Source: Google 2008,
<http://research.google.com/archive/provos-2008a.pdf>

Ratio of Google Search Queries Containing At Least One Malicious URL in Search Results



Source: Google 2008, <http://research.google.com/archive/provos-2008a.pdf>

Ratio of Malicious URLs by Content Category



Source: Google 2008, <http://research.google.com/archive/provos-2008a.pdf>

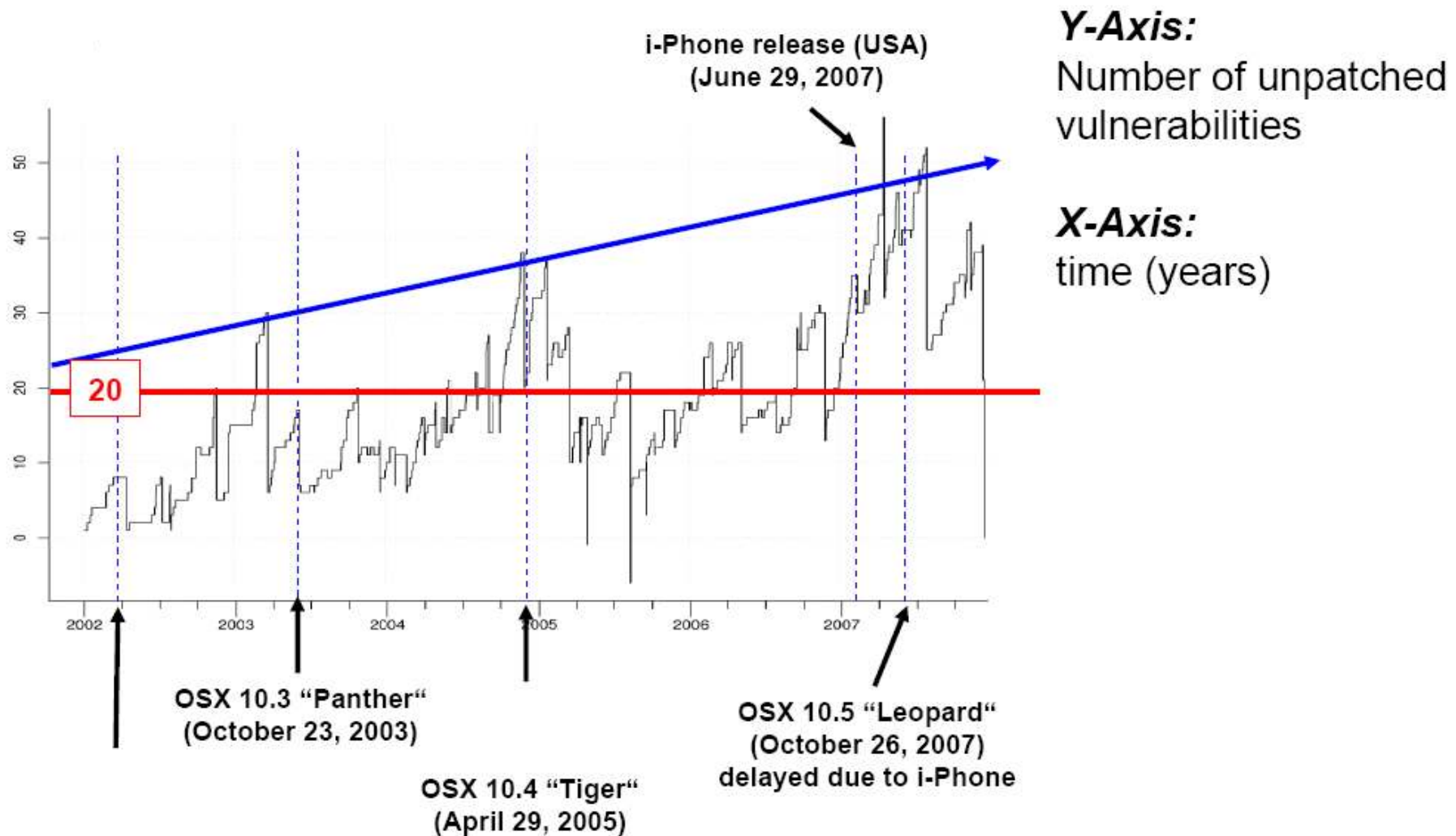


Information
Security Society
Switzerland
> *vormals FGSec*

Slower Patching and Faster Exploits

Apple less secure than Windows

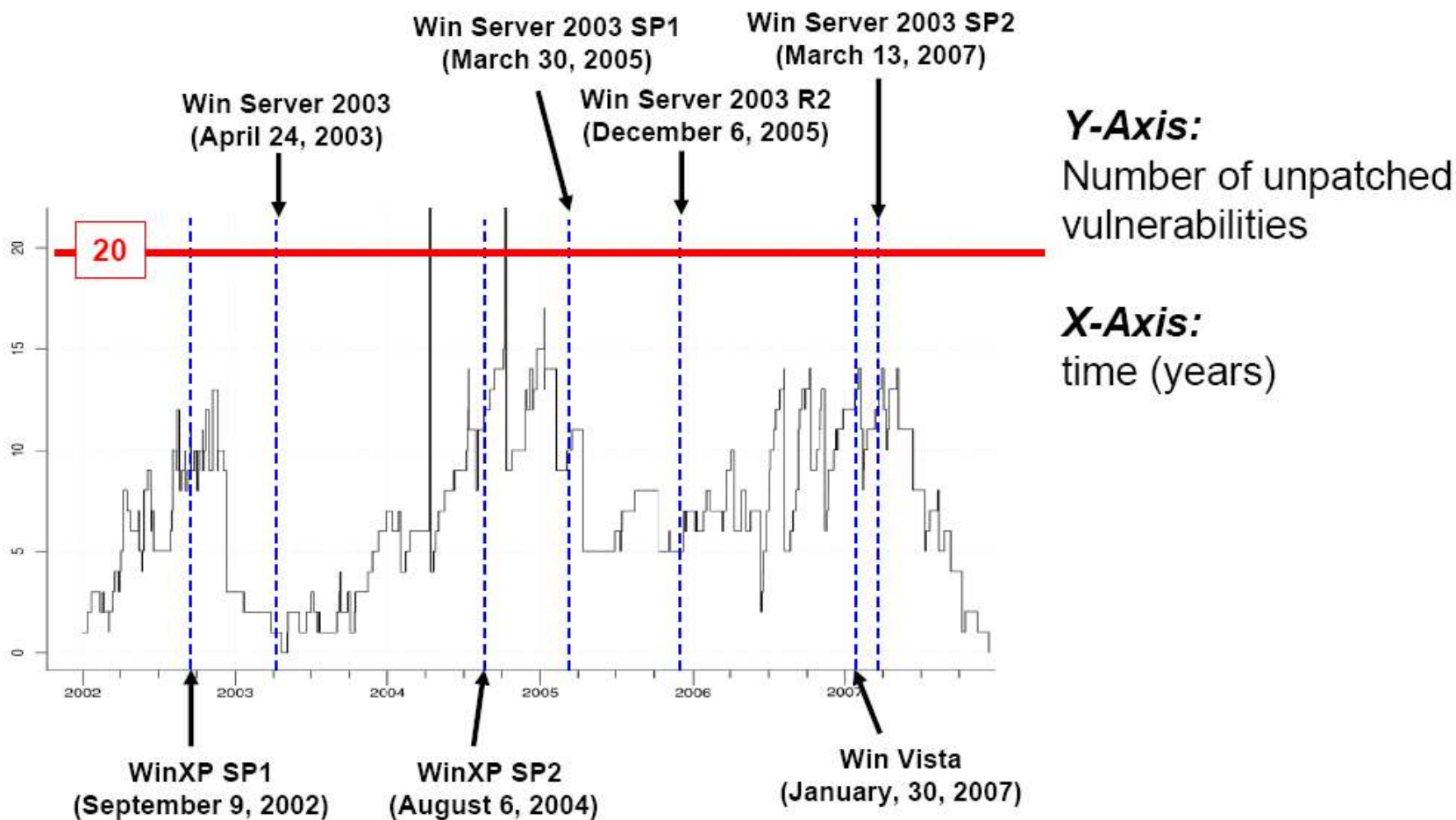
Apple: Number of unpatched critical vulnerabilities



Source: „0-Day Patch - Exposing Vendors (In)security Performance“, BlackHat 2008,
<http://www.techzoom.net/publications/papers.en>

Apple less secure than Windows

Microsoft: Number of unpatched critical vulnerabilities



Source: „0-Day Patch - Exposing Vendors (In)security Performance“, BlackHat 2008,
<http://www.techzoom.net/publications/papers.en>

Zotob Worm (2005)

- August 2005: Zotob worm (Rbot worm variant) appeared 5 (!) days after Microsoft released a patch for a Windows plug'n'play component.
- Rbot can force an infected computer to continuously restart
- Its outbreak on Aug 16th, 2005 was covered "live" on CNN television, as the network's own computers got infected.
- Clean-up per company affected:
 - Average cost of US\$ 97,000
 - 80 hours of cleanup

Source: [http://en.wikipedia.org/wiki/Zotob_\(computer_worm\)](http://en.wikipedia.org/wiki/Zotob_(computer_worm))

Exploit Generator (2008)

- Given:
 - Buggy program with an unknown vulnerability
 - Corresponding Security Patch
- An exploit generator developed at Carnegie Mellon University can automatically create an exploit for unpatched systems **within a few minutes**.
- Shown for several Windows vulnerabilities and patches.

Source: <http://www.cs.cmu.edu/~dbrumley/pubs/apeg.pdf>
To appear in May 2008 at [IEEE Security and Privacy Symposium](#)



Information
Security Society
Switzerland
> *vormals FGSec*

Vulnerable Internet End Points

Internet Clients are Most Vulnerable

- but also servers



Image Source: <http://www.webpchelp.com/antivirus/antivirus.html>

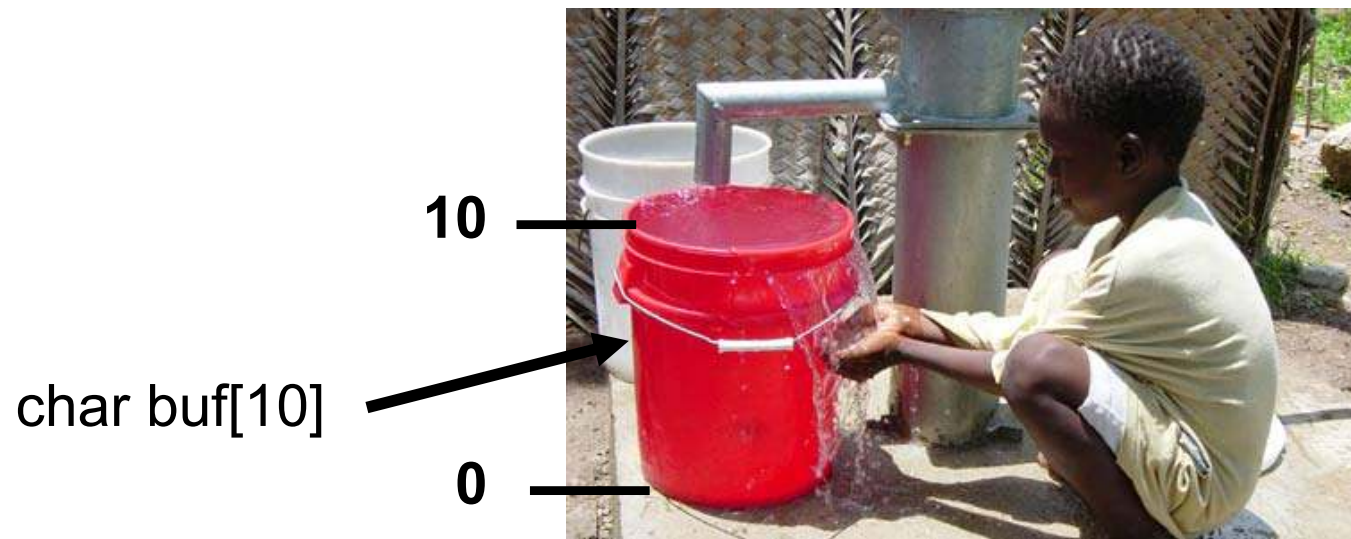


Information
Security Society
Switzerland
> *vormals FGSec*

Lack of Security Aware Software Developers

Buffer Overflow

- Buffer: memory used to store user input
- Buffer overflow: a condition that occurs when more user input is provided than can fit in the buffer; this can lead to code injection and execution



- Known since 1972; first exploit 1988 (Morris worm)
- 50% of CERT advisories in 1998!
- Jan 2008: Two Buffer Overflows in Apple Quicktime

Summary – Top 10 Security Trends

- Economic Value of Information
- Critical Infrastructure Outages
- Bot Networks
- Third Parties Controlling Information
- Complexity
- Criminals
- Drive-By Downloads
- Slower Patching and Faster Exploits
- Vulnerable Internet End Points
- Lack of Security Aware Software Developers

Thanks for your attention!