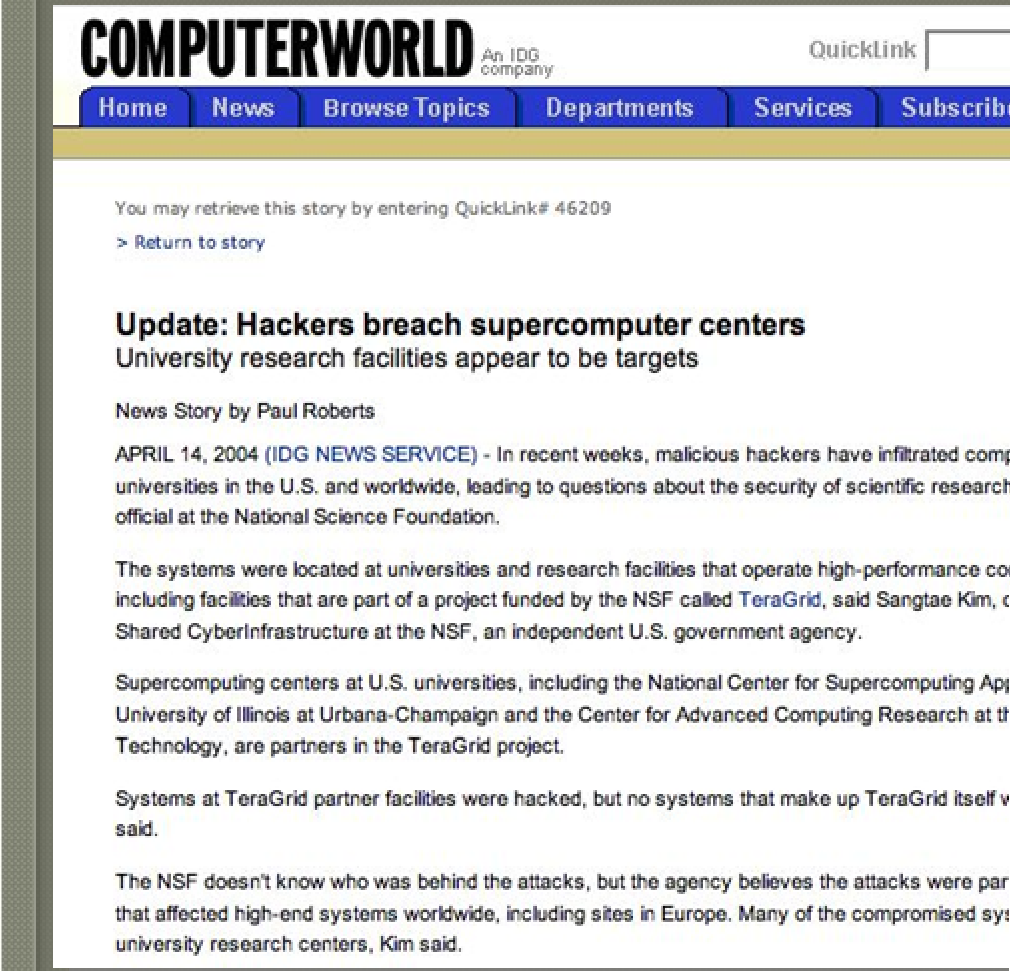
Threat Briefing

David Dittrich
University of Washington

UNOLS RVTEC Meeting, November 19, 2009

Attacks on supercomputer Centers



Update: Hackers breach supercomputer centers

University research facilities appear to be targets

News Story by Paul Roberts

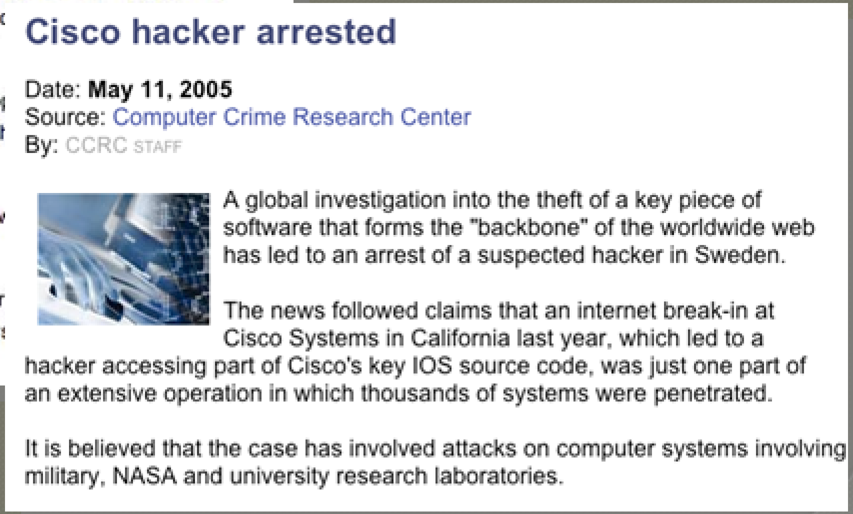
APRIL 14, 2004 (IDG NEWS SERVICE) - In recent weeks, malicious hackers have infiltrated computer systems at universities in the U.S. and worldwide, leading to questions about the security of scientific research data, according to an official at the National Science Foundation.

The systems were located at universities and research facilities that operate high-performance computer centers, including facilities that are part of a project funded by the NSF called TeraGrid, said Sangtae Kim, c Shared CyberInfrastructure at the NSF, an independent U.S. government agency.

Supercomputing centers at U.S. universities, including the National Center for Supercomputing Ap University of Illinois at Urbana-Champaign and the Center for Advanced Computing Research at tl Technology, are partners in the TeraGrid project.

Systems at TeraGrid partner facilities were hacked, but no systems that make up TeraGrid itself v said.

The NSF doesn't know who was behind the attacks, but the agency believes the attacks were par that affected high-end systems worldwide, including sites in Europe. Many of the compromised sy: university research centers, Kim said.



Cisco hacker arrested

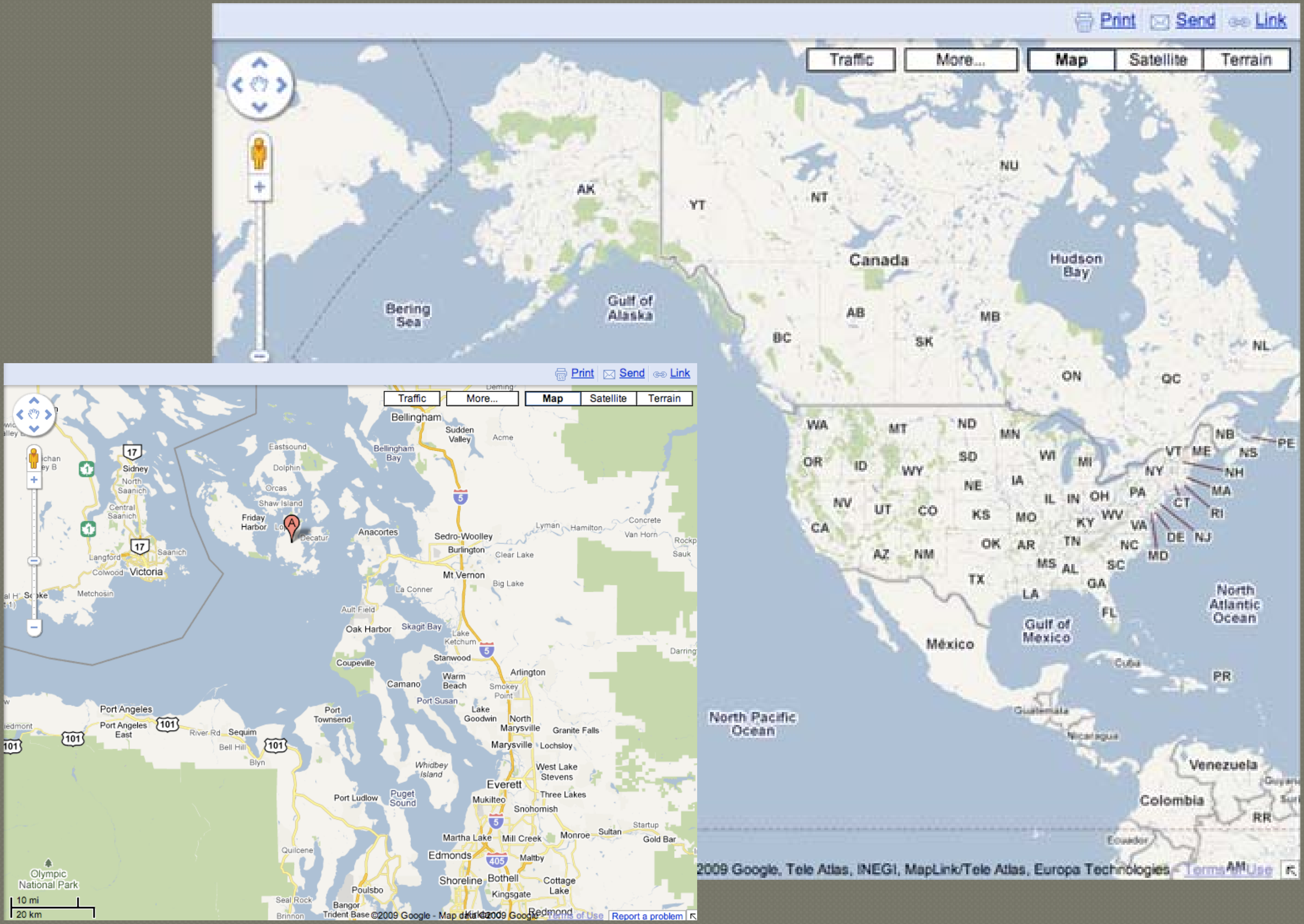
Date: **May 11, 2005**
Source: Computer Crime Research Center
By: CCRC STAFF

A global investigation into the theft of a key piece of software that forms the "backbone" of the worldwide web has led to an arrest of a suspected hacker in Sweden.

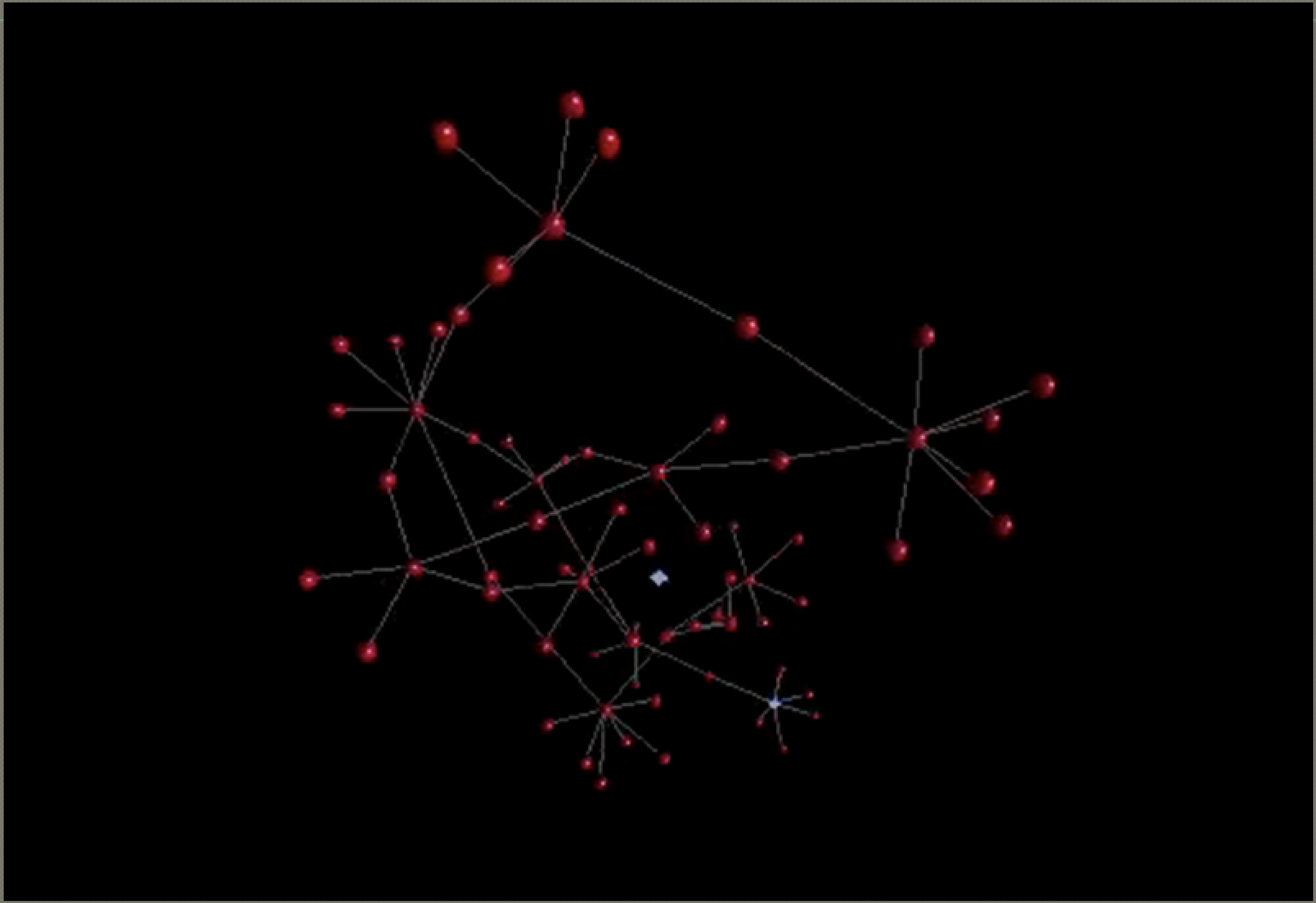
The news followed claims that an internet break-in at Cisco Systems in California last year, which led to a hacker accessing part of Cisco's key IOS source code, was just one part of an extensive operation in which thousands of systems were penetrated.

It is believed that the case has involved attacks on computer systems involving military, NASA and university research laboratories.

Where is…


Print Send Link
Traffic
More...
Map
Satellite
Terrain
AK
YT
NT
NU
Canada
Hudson Bay
Bering Sea
Gulf of Alaska
BC
AB
SK
MB
ON
QC
NL
NB
PE
NS
WA
MT
ND
MN
OR
ID
WY
SD
WI
MI
NY
VT
ME
NH
MA
CT
RI
NE
IA
IL
IN
OH
PA
NV
UT
CO
KS
MO
KY
WV
VA
NJ
DE
MD
CA
AZ
NM
OK
AR
TN
NC
SC
MS
AL
GA
TX
LA
FL
México
Gulf of Mexico
Cuba
PR
North Atlantic Ocean
North Pacific Ocean
Guatemala
Nicaragua
Venezuela
Colombia
Ecuador
RR
©2009 Google, Tele Atlas, INEGI, MapLink/Tele Atlas, Europa Technologies - Terms of Use
Bellingham
Sudden Valley
Acme
Bellingham Bay
Eastsound
Dolphin
Orcas
Shaw Island
Friday Harbor
Decatur
Anacortes
Sedro-Woolley
Burlington
Lyman
Hamilton
Concrete
Van Horn
Clear Lake
Mt Vernon
Big Lake
La Conner
Sidney
North Saanich
Central Saanich
Saanich
Langford
Colwood
Victoria
Metchosin
Sooke
Ault Field
Oak Harbor
Skagit Bay
Lake Ketchum
Stanwood
Coupeville
Camano
Warm Beach
Arlington
Smokey Point
Port Susan
Port Angeles
Port Angeles East
Sequim
River Rd
Bell Hill
Blyn
Port Townsend
Lake Goodwin
North Marysville
Granite Falls
Marysville
Lochsloy
Whidbey Island
West Lake Stevens
Everett
Port Ludlow
Puget Sound
Mukilteo
Three Lakes
Snohomish
Quilcene
Martha Lake
Mill Creek
Monroe
Sultan
Startup
Gold Bar
Edmonds
Maltby
Shoreline
Bothell
Cottage Lake
Kingsgate
Poulsbo
Seal Rock
Bangor
Trident Base
Brinnon
Redmond
Olympic National Park
Darring
Rockp
Sauk
5
17
101
405
10 mi
20 km
©2009 Google - Map data ©2009 Google - Terms of Use
Report a problem

Now where is…?



Stages of Attack (simple view)

1. *Reconnaissance* (gather information about the target system or network)
2. *Probe and attack* (probe the system for weaknesses and deploy the tools)
3. *Toehold* (exploit security weakness and gain entry into the system)
4. *Advancement* (advance from an unprivileged account to a privileged account)
5. *Stealth* (hide tracks; install a backdoor)
6. *Listening post* (establish a listening post)
7. *Takeover* (expand control from a single host to other hosts on network)

"Catapults and grappling hooks: The tools and techniques of information warfare," IBM Systems Journal, Vol. 37, No. 1, 1998
http://www.research.ibm.com/journal/sj/371/boulanger.html

Principal Threat Categories

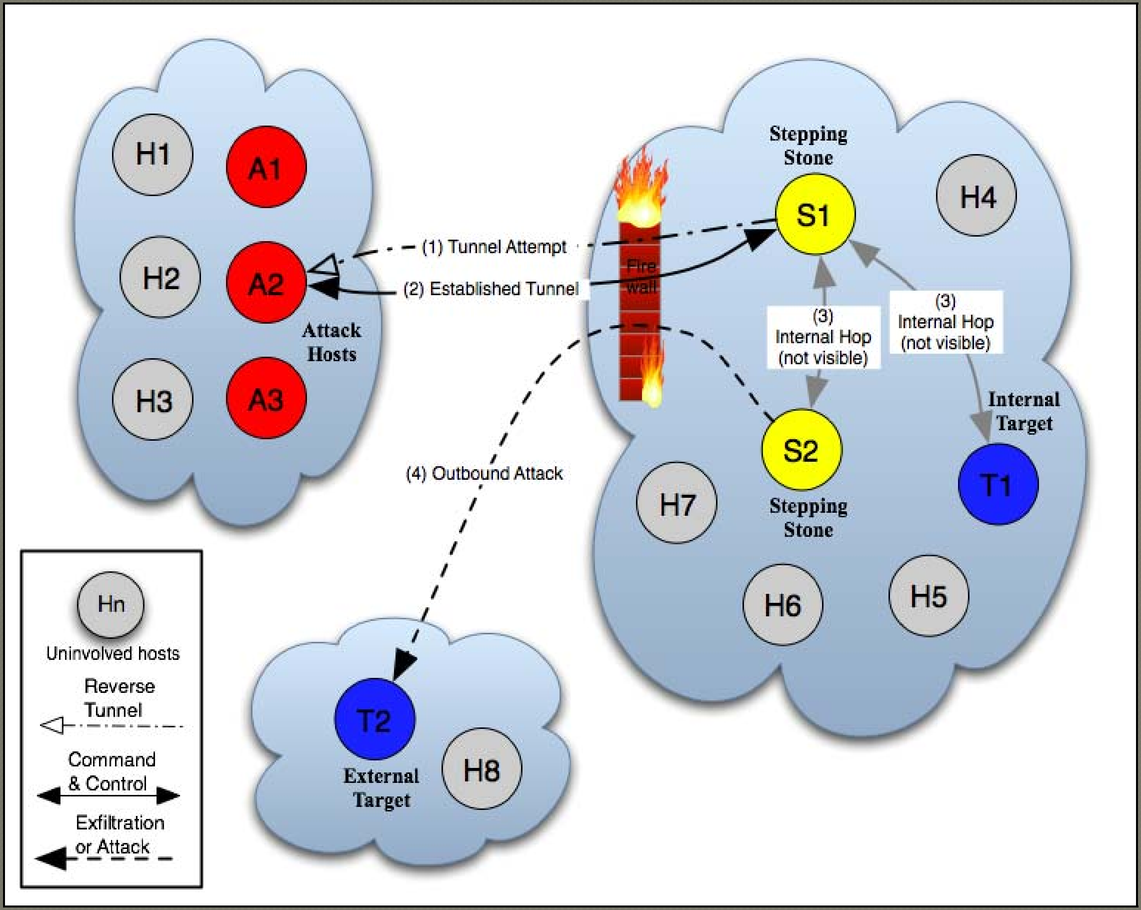
- Data Theft and Espionage (Industrial and National Security)
- Fraud
- Disruption of Operations
- Extortion

Espionage/Data Theft

- Targeted “spam” with trojan horse, “lost” USB thumb drives in parking lots, etc.
  - Executable attachments
  - Media files, documents, embedded content
  - Key loggers or “root kits” installed
  - Data exfiltrated by POST or reverse tunnel through firewall
- Surplused equipment!

  http://www.computer.org/portal/cms_docs_security/security/v1n1/garfinkel.pdf

Reverse Tunnel



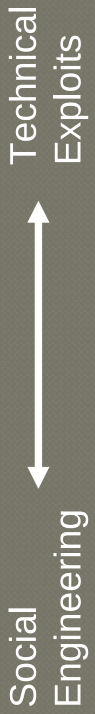
Fraud

- Unauthorized access to steal data, media
- Phishing (social engineering via email)
- Key logging, or screen capture (attack virtual keyboards)
- HTTP `POST` interception

Attack Mechanisms

- Social engineering and exploiting trust
- Bypassing technical defenses
- Eluding capture through concealment
- Avoiding detection for long periods of time

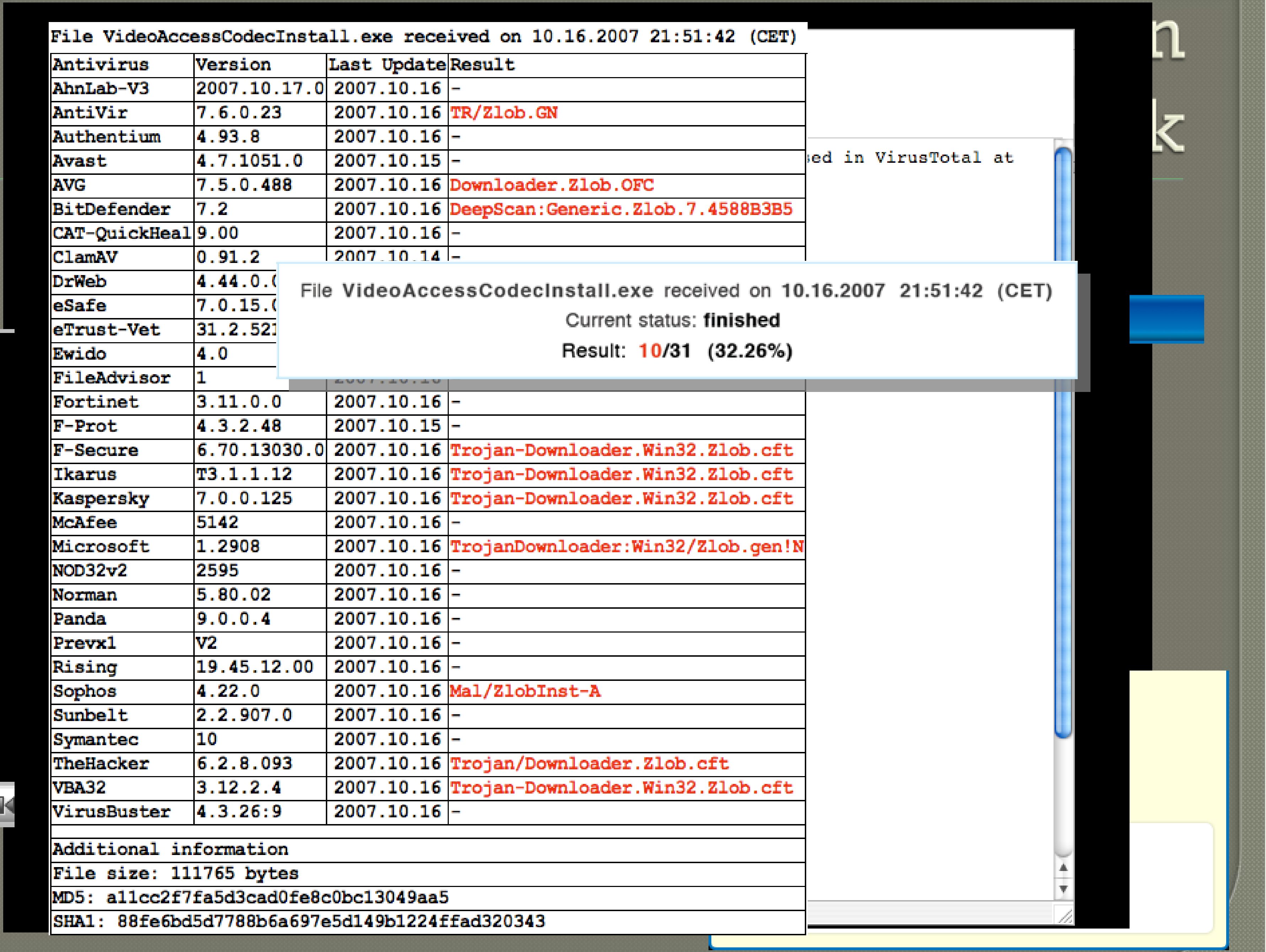
Propagation mechanisms



Technical Exploits

Social Engineering

1. Exploitation of remotely accessible vulnerabilities in the Windows LSASS (139/tcp) and RPC-DCOM (445/tcp) services
2. Email to targets obtained from WAB except those containing specific substrings (e.g., “icrosof”, “ecur” , “.mil”, etc.)
3. Messaging AIM and MSN buddy list members with randomly formed sentence and URL
4. Trojan Horse `SETUP.EXE` on free download site
5. Trojan Horse *dropper* associated with “celebrity video clips”



File VideoAccessCodecInstall.exe received on 10.16.2007 21:51:42 (CET)

Antivirus	Version	Last Update	Result
AhnLab-V3	2007.10.17.0	2007.10.16	-
AntiVir	7.6.0.23	2007.10.16	TR/Zlob.GN
Authentium	4.93.8	2007.10.16	-
Avast	4.7.1051.0	2007.10.15	-
AVG	7.5.0.488	2007.10.16	Downloader.Zlob.OFC
BitDefender	7.2	2007.10.16	DeepScan:Generic.Zlob.7.4588B3B5
CAT-QuickHeal	9.00	2007.10.16	-
ClamAV	0.91.2	2007.10.14	-
DrWeb	4.44.0.(		
eSafe	7.0.15.(		
eTrust-Vet	31.2.521		
Ewido	4.0		
FileAdvisor	1		
Fortinet	3.11.0.0	2007.10.16	-
F-Prot	4.3.2.48	2007.10.15	-
F-Secure	6.70.13030.0	2007.10.16	Trojan-Downloader.Win32.Zlob.cft
Ikarus	T3.1.1.12	2007.10.16	Trojan-Downloader.Win32.Zlob.cft
Kaspersky	7.0.0.125	2007.10.16	Trojan-Downloader.Win32.Zlob.cft
McAfee	5142	2007.10.16	-
Microsoft	1.2908	2007.10.16	TrojanDownloader:Win32/Zlob.gen!N
NOD32v2	2595	2007.10.16	-
Norman	5.80.02	2007.10.16	-
Panda	9.0.0.4	2007.10.16	-
Prevx1	V2	2007.10.16	-
Rising	19.45.12.00	2007.10.16	-
Sophos	4.22.0	2007.10.16	Mal/ZlobInst-A
Sunbelt	2.2.907.0	2007.10.16	-
Symantec	10	2007.10.16	-
TheHacker	6.2.8.093	2007.10.16	Trojan/Downloader.Zlob.cft
VBA32	3.12.2.4	2007.10.16	Trojan-Downloader.Win32.Zlob.cft
VirusBuster	4.3.26:9	2007.10.16	-

Additional information

File size: 111765 bytes

MD5: a11cc2f7fa5d3cad0fe8c0bc13049aa5

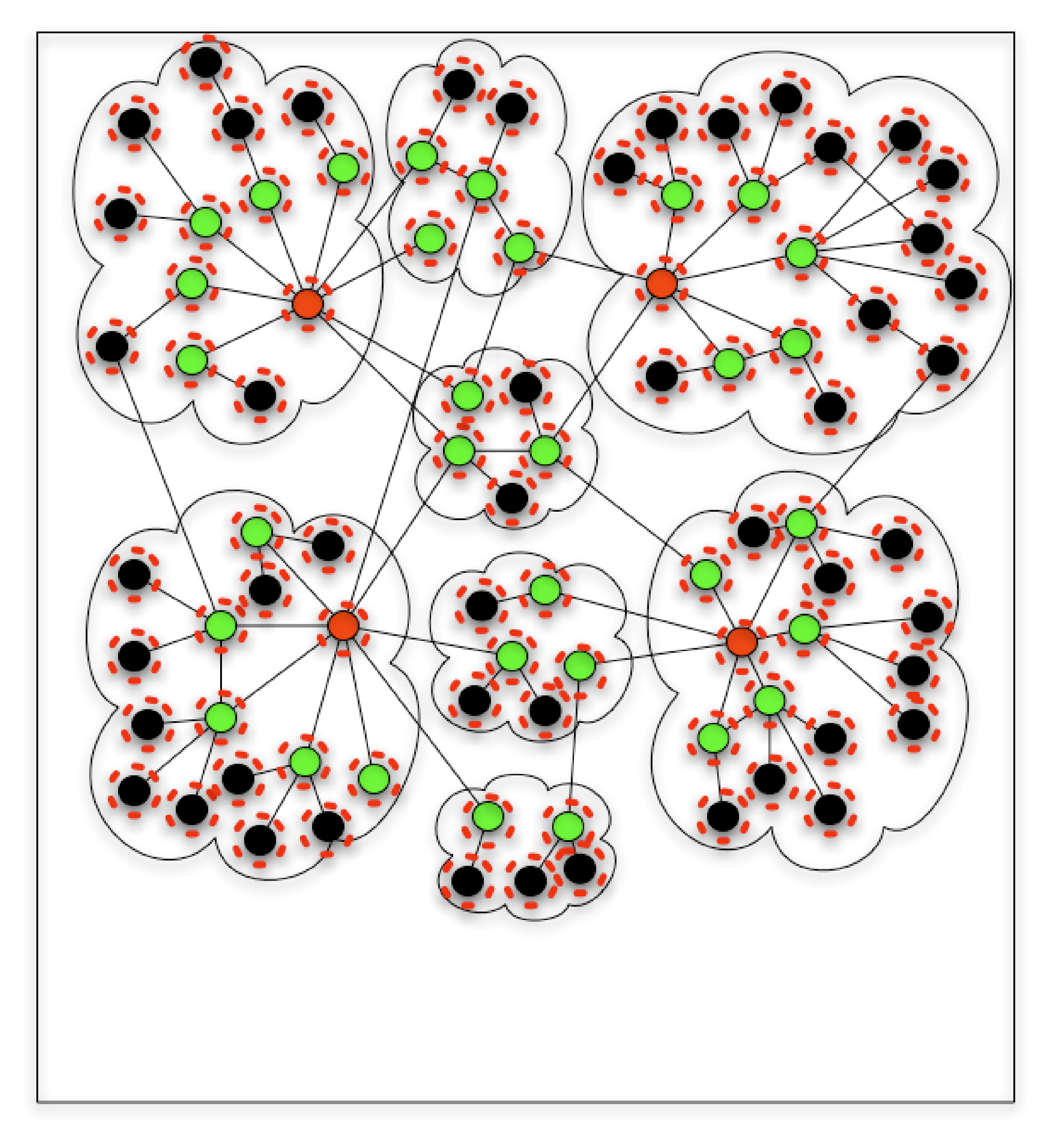
SHA1: 88fe6bd5d7788b6a697e5d149b1224ffad320343

sed in VirusTotal at

File VideoAccessCodecInstall.exe received on 10.16.2007 21:51:42 (CET)

Current status: **finished**

Result: **10/31 (32.26%)**

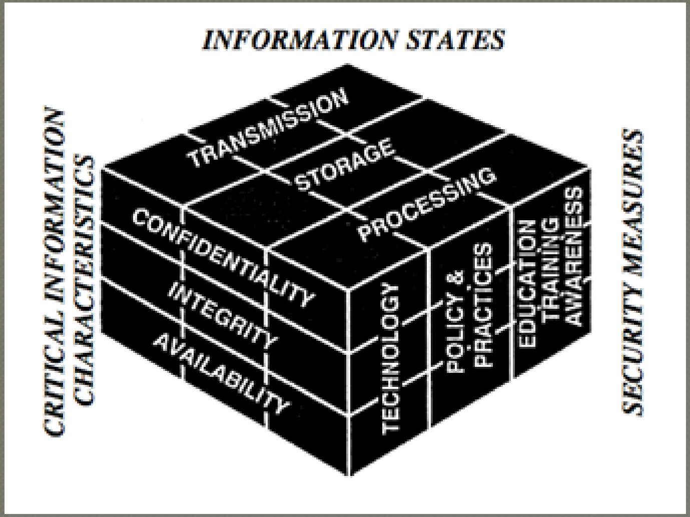


Rethinking Defensive Posture

- Information Assurance (IA) is defined to be, "measures that protect and defend information and information systems by ensuring their *availability*, *integrity*, *authentication*, *confidentiality*, and *non-repudiation*."

- "These measures include providing for restoration of information systems by incorporating *protection*, *detection*, and *reaction* capabilities."

Source: National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, Revised 2003



So what do we do?

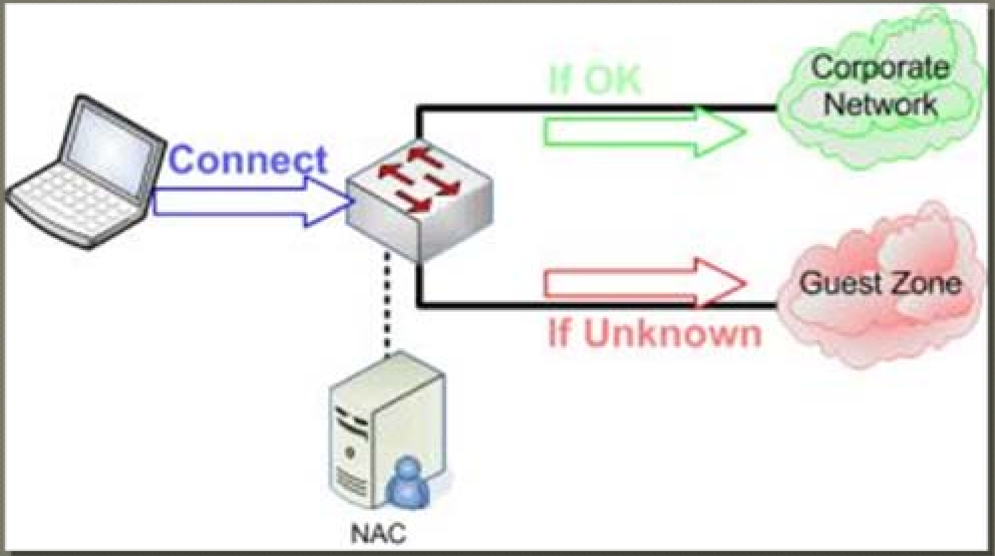
- Apply layered & complementary defenses
- Do all: Protect, Detect, and React
- Not all solutions are technical
- Support those tackling the hard problems with policy and resources

Isolation of untrusted devices

- Trusted devices on secured AP
- Un-trusted devices on open AP (outside firewall: can only talk to the internet)
- Alt: Use PPTP, IPSec or other VPN to tunnel *in* to trusted network
- Constantly scan hosts (nmap) and analyze traffic (ntop, Snort, etc.)

"*Trust, but verify,*" Ronald Reagan

Network Access Control & Quarantine



Source: "*How FreeNAC Works*"
http://freenac.net/en/products/solution

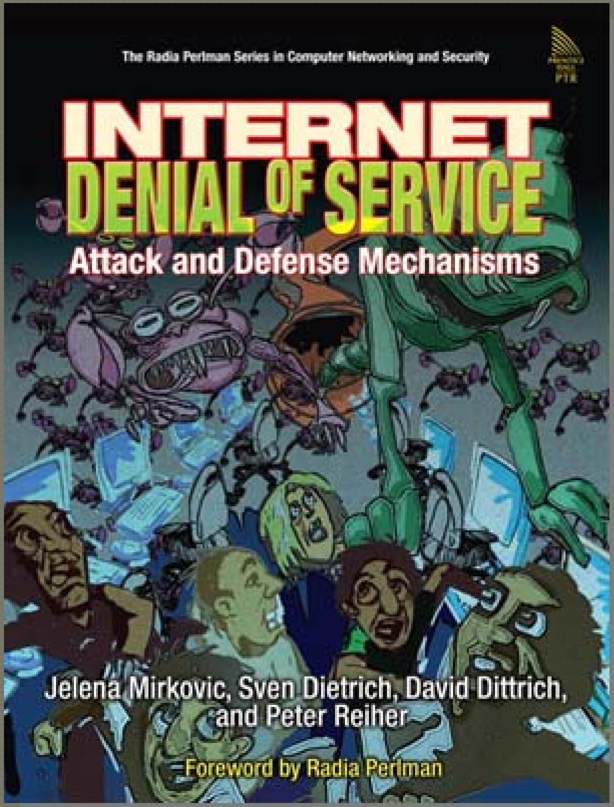
Thank You and Questions

- *Contact:*

  Dave Dittrich

  Affiliate Principal Scientist
  Applied Physics Laboratory
  University of Washington

  dittrich(at)u.washington.edu
  http://staff.washington.edu/dittrich/


The Radia Perlman Series in Computer Networking and Security
INTERNET DENIAL OF SERVICE
Attack and Defense Mechanisms
Jelena Mirkovic, Sven Dietrich, David Dittrich, and Peter Reiher
Foreword by Radia Perlman

http://vig.prenhall.com/catalog/academic/product/0,1144,0131475738,00.html

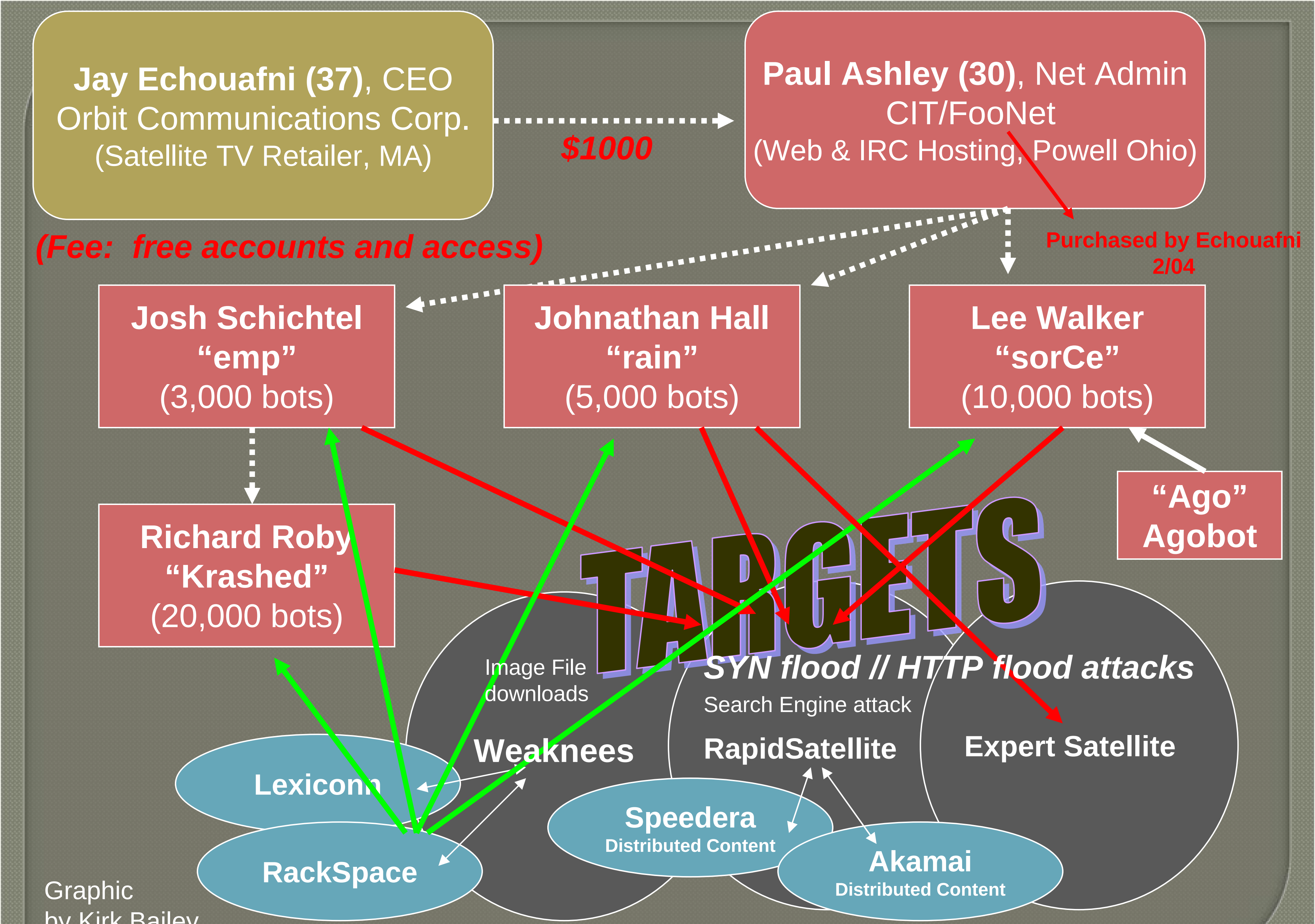
Case Studies

Operation “Cyberslam” (2003-04)
Israeli “Trojan Horse” (2005)
“GhostNet” (2008-09)

Operation "Cyberslam" (2003-04)

- "*The first case of its kind involving a DDoS for commercial advantage or for hire*"
  - 1 directing, 1 managing, 4 "consulting"
  - DDoS for cash, free server, free shell account
  - Purchase of ISP, hired "consultant" ($120K/yr)
  - " *u gotta keep ane eye on it...cuz they could null route the ip and change the dns...and it would be back up.*" [sic]
- 5,000-10,000 custom "Agobot" hosts (1 person)
  - Special web attack methods to avoid DDoS mitigation
  - Special DNS attack to defeat distributed DNS service
- Over 20,000 more bots (3 other individuals)
- Reported US$2M in damages to targets & their NSPs

http://www.reverse.net/operationcyberslam.pdf



Jay Echouafni (37), CEO
Orbit Communications Corp.
(Satellite TV Retailer, MA)

$1000

Paul Ashley (30), Net Admin
CIT/FooNet
(Web & IRC Hosting, Powell Ohio)

Purchased by Echouafni
2/04

(Fee: free accounts and access)

Josh Schichtel
“emp”
(3,000 bots)

Johnathan Hall
“rain”
(5,000 bots)

Lee Walker
“sorCe”
(10,000 bots)

“Ago”
Agobot

Richard Roby
“Krashed”
(20,000 bots)

TARGETS

SYN flood // HTTP flood attacks

Image File downloads

Search Engine attack

Weaknees

RapidSatellite

Expert Satellite

Lexiconn

RackSpace

Speedera
Distributed Content

Akamai
Distributed Content

Graphic
by Kirk Bailey

http://www.reverse.net/operationcyberslam.pdf

Israeli Industrial Espionage (2005)

- Custom Trojan Horse Key Logger, installed and run for PI firms in Israel
  - One year+ operation
  - US$4000/host
  - Bypassed all AV and IPS
- 18 arrests (primary suspects a couple and their 17 year old son)
- 100+ pieces of computer equipment seized
- Caught because of mistake, not detection

"Tracking GhostNet"

- SecDevGroup & Monk Centre, U. Toronto, Canada
- June 2008 – March 2009
- Victims: Foreign embassies, Tibetan government in exile, development banks, media orgs, student orgs, NGOs, multi-national consulting agencies, etc.
- 1,295 infected computers in 103 countries
- Took control of botnet to observe use

http://www.infowar-monitor.net/ghostnet