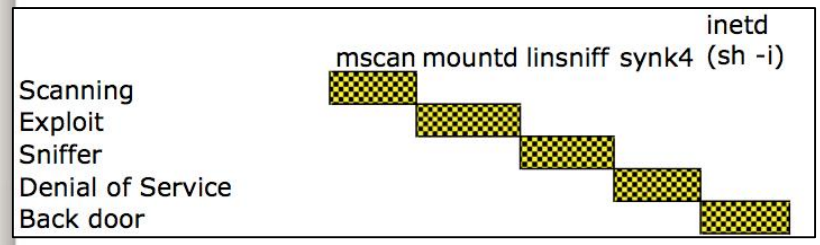
David Dittrich
The Information School
University of Washington

Outline

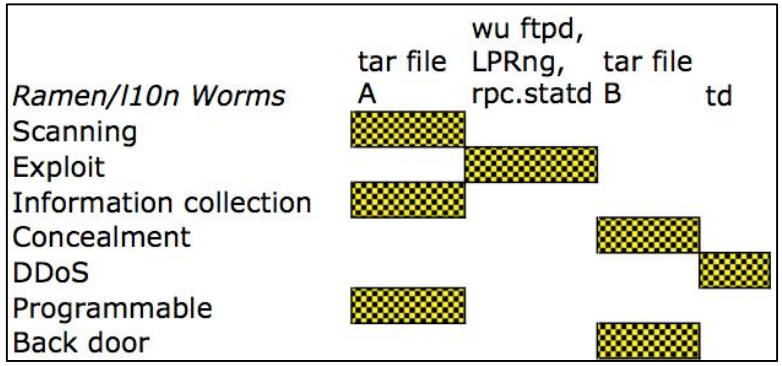
- Advances in distributed attack tools/methods
  - Case studies of recent attacks
- Rethinking your defense strategy
- Is “Strike-back” an option?
  - Case study: “Make Love, not Spam.”
- Conclusions

Converging Features

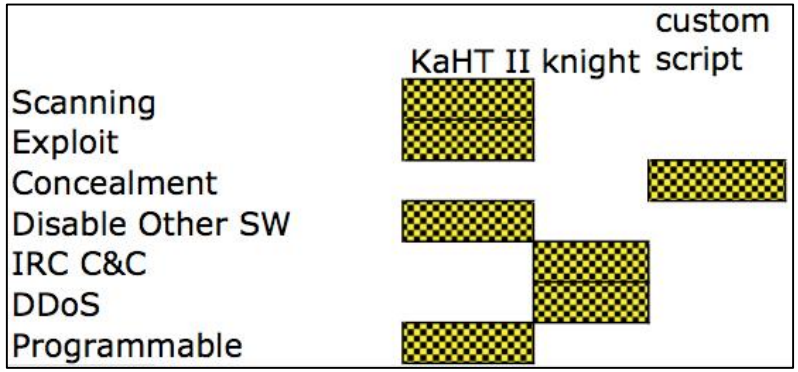
1999 Custom Linux kit



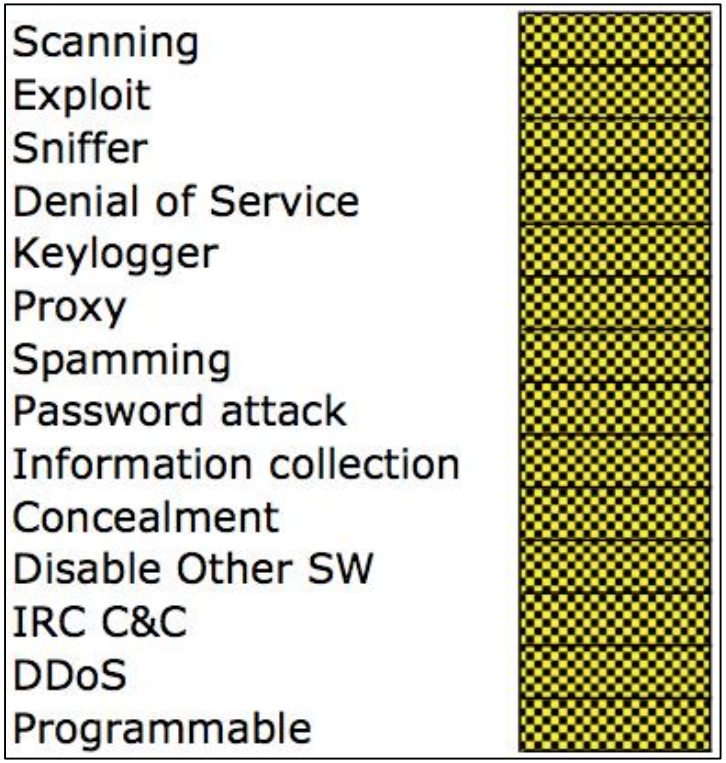
2001 Ramen/l10n worms

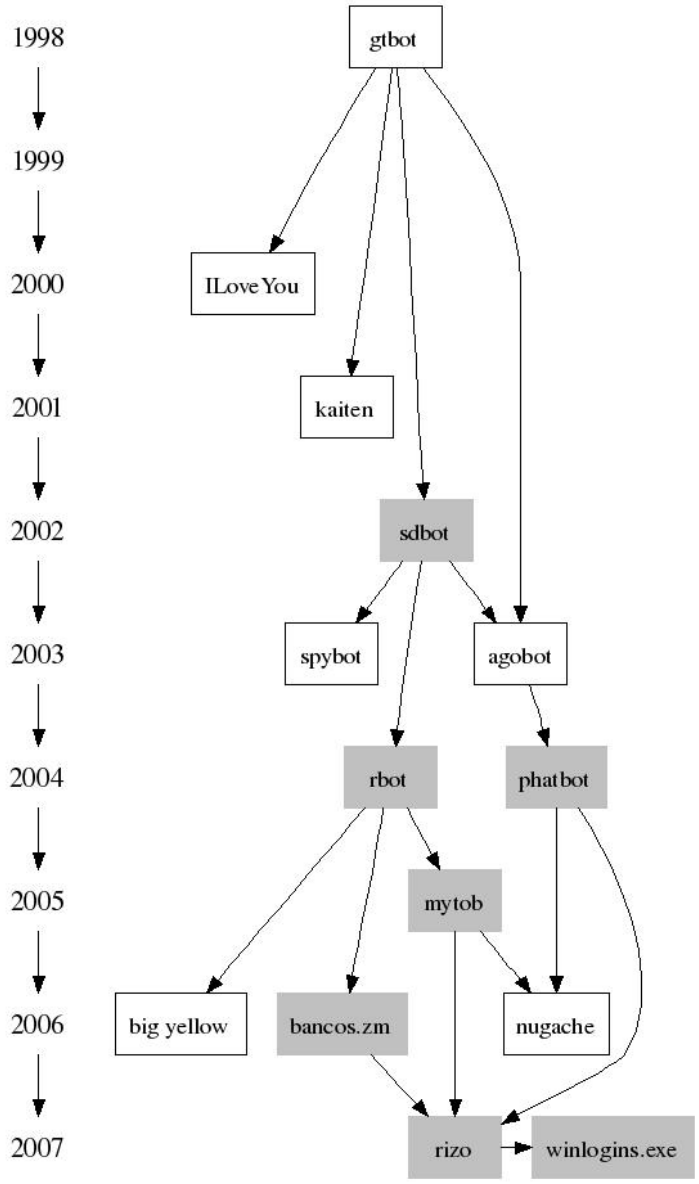


2003 Custom Windows kit



2004 Agobot/Phatbot



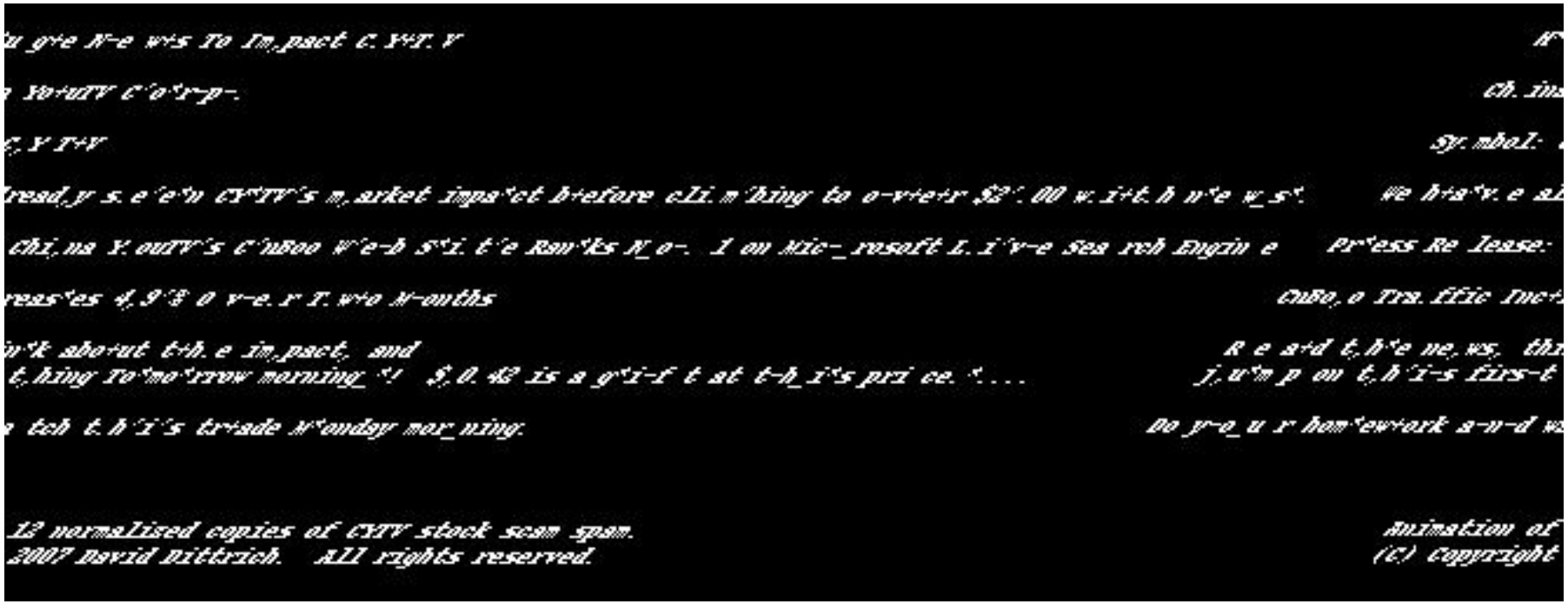


IRC Bot Feature Lineage

- Attackers
  - Can steal code…
  - Or steal ideas/features
  - Easy to stay under the radar
- Defenders
  - Attacker tools & tactics getting better
  - AV industry helps with detection (sometimes) but not so much reaction

Version 00x010x31	Version 00x010x34
A----U_S_A	A____USA
|Vir	|Virt
exw_trella_m	exwtrellam
Who_a{m}_I	WhoamI
BaR-MaN^22	
Gina}{-	Gina_
deepthr__t	deepthrt
KaJ|aRa`[F]	KaJlaRaF
nIcOs^m_away	nIcOsmaway
. . .	. . .

Similar tactic in spam



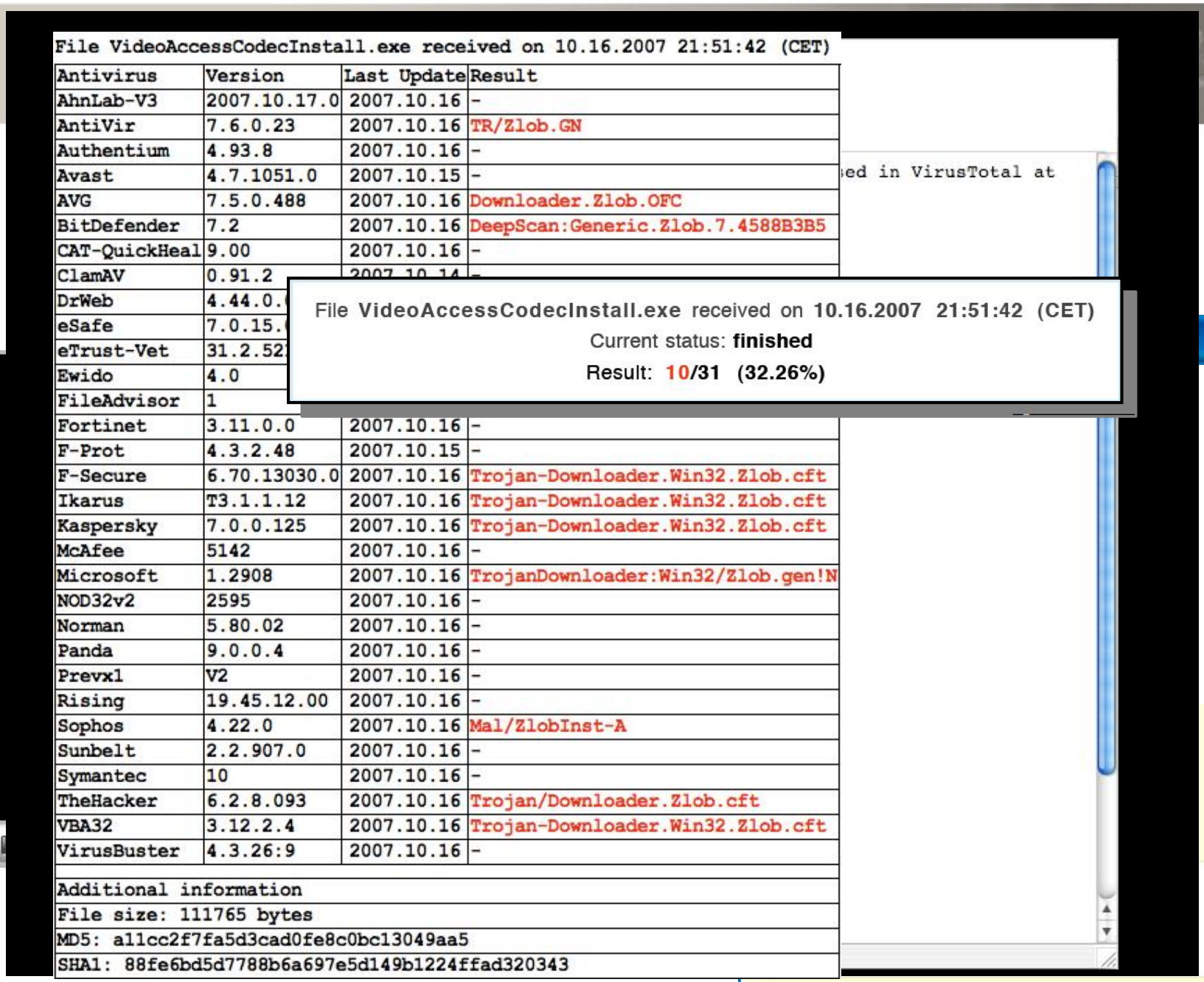
http://staff.washington.edu/dittrich/misc/spamanimation.gif

Propagation mechanisms

1. Exploitation of remotely accessible vulnerabilities in the Windows LSASS (139/tcp) and RPC-DCOM

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		
DrWeb	4.44.0.		
eSafe	7.0.15.		
eTrust-Vet	31.2.52		
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

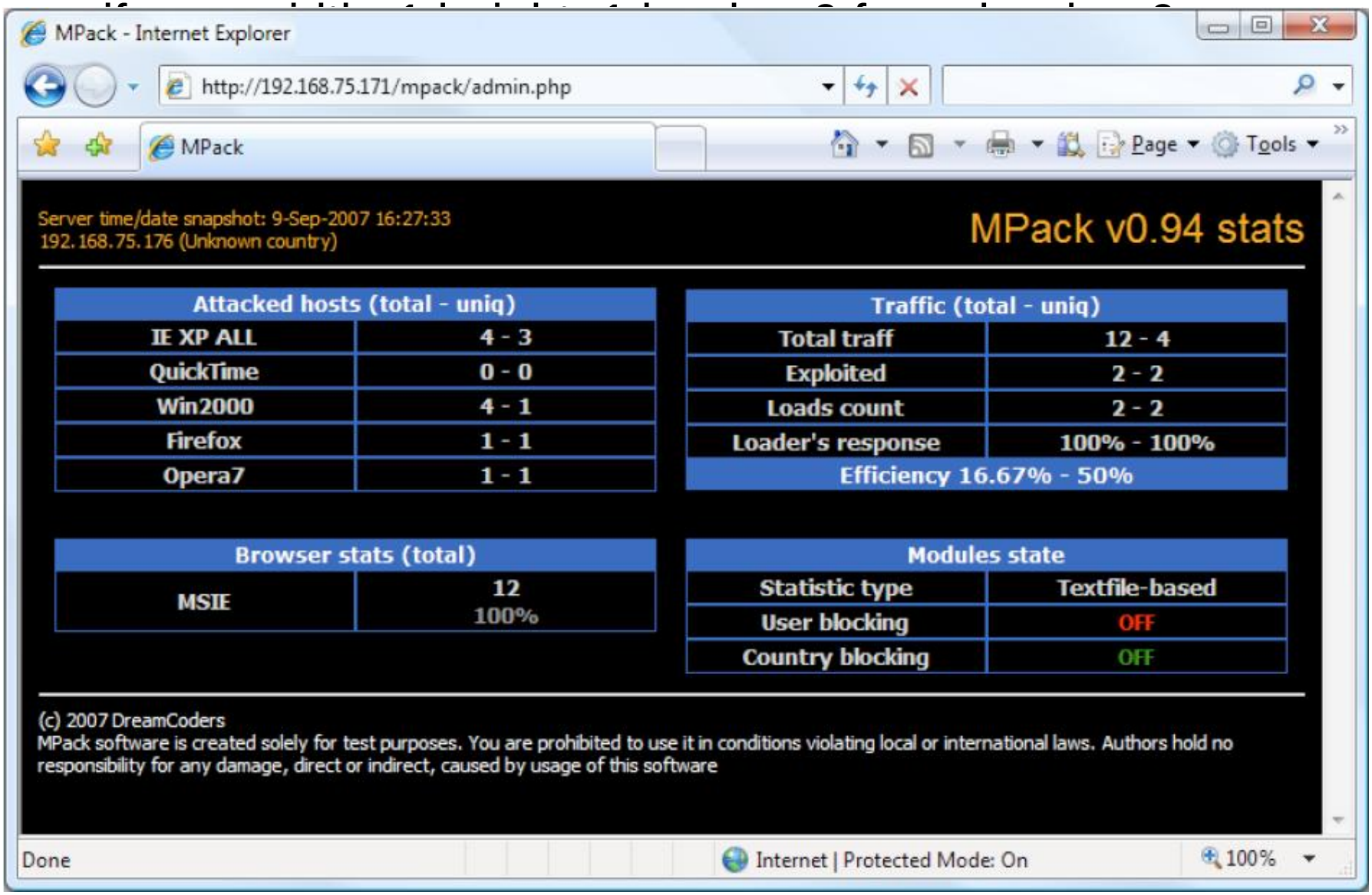
SHA1: 88fe6bd5d7788b6a697e5d149b1224ffad320343

ed in VirusTotal at

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

Current status: **finished**

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

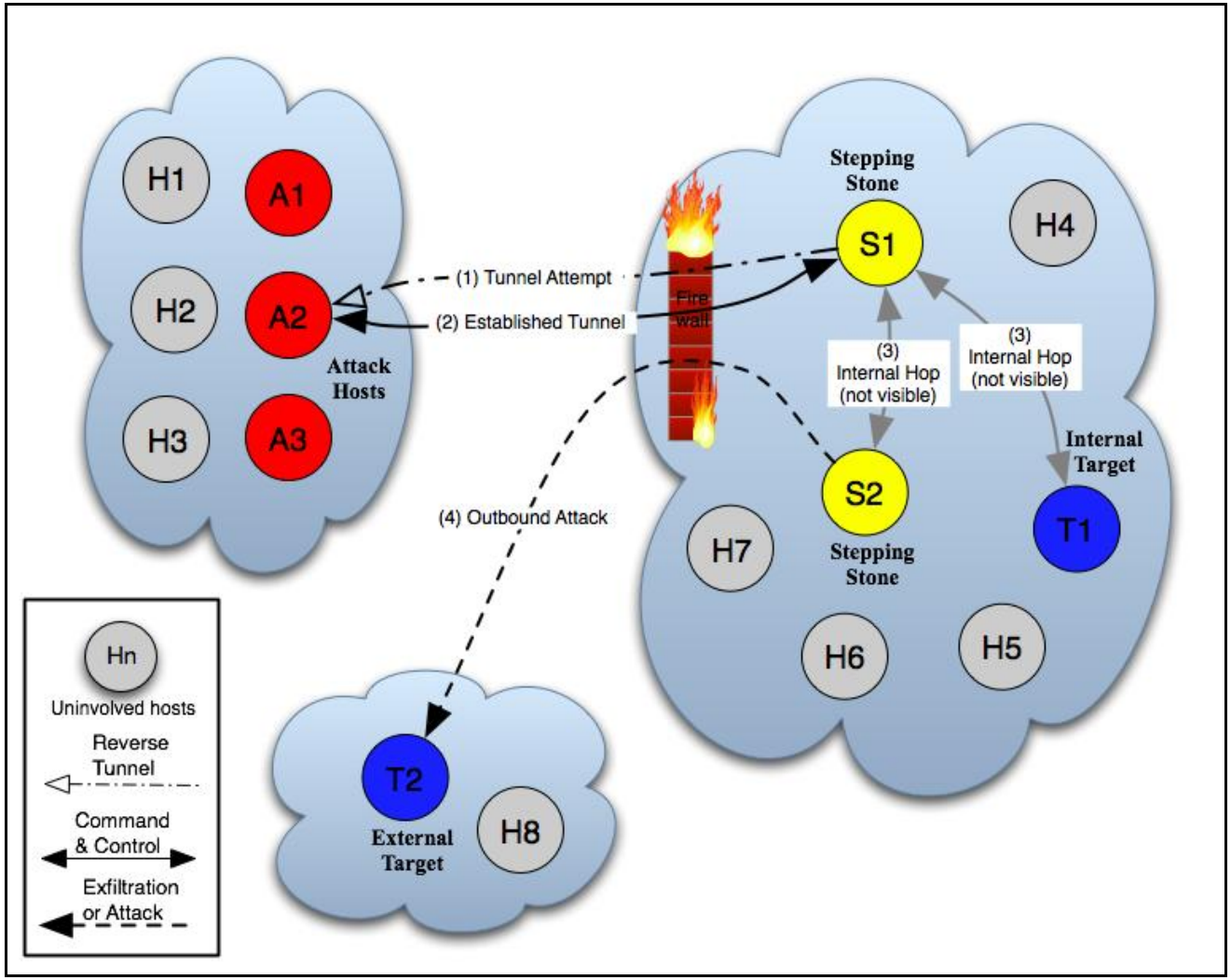

MPack - Internet Explorer
http://192.168.75.171/mpack/admin.php
MPack
Page
Tools
Server time/date snapshot: 9-Sep-2007 16:27:33
192.168.75.176 (Unknown country)
MPack v0.94 stats
Attacked hosts (total - uniq)
IE XP ALL 4 - 3
QuickTime 0 - 0
Win2000 4 - 1
Firefox 1 - 1
Opera7 1 - 1
Traffic (total - uniq)
Total traff 12 - 4
Exploited 2 - 2
Loads count 2 - 2
Loader's response 100% - 100%
Efficiency 16.67% - 50%
Browser stats (total)
MSIE 12 100%
Modules state
Statistic type Textfile-based
User blocking OFF
Country blocking OFF
(c) 2007 DreamCoders
MPack software is created solely for test purposes. You are prohibited to use it in conditions violating local or international laws. Authors hold no responsibility for any damage, direct or indirect, caused by usage of this software
Done
Internet | Protected Mode: On
100%

Automatic tasking

```
T 2007/10/11 18:21:42.932316 10.1.1.102:1097 -> [redacted]:80 [AP]
join #[redacted],#[redacted],#[redacted].

T 2007/10/11 18:21:43.238910 [redacted]:80 -> 10.1.1.102:1097 [AP]
:[00][XP][SP2][USA]-131615421![redacted]@[redacted].net JOIN :#[redacted].
:[redacted] 332 [00][XP][SP2][USA]-131615421 #[redacted] :!advscanall 70 . -l -w -s.
:[redacted] 333 [00][XP][SP2][USA]-131615421 #[redacted] {XP}-5187341 1191757621.
:[redacted] 353 [00][XP][SP2][USA]-131615421 @ #[redacted] :[00][XP][SP2][USA]-131615421 .
:[redacted] 366 [00][XP][SP2][USA]-131615421 #[redacted] :End of /NAMES list..
:[00][XP][SP2][USA]-131615421![redacted]@[redacted].net JOIN :#[redacted].
:[redacted] 332 [00][XP][SP2][USA]-131615421 #[redacted] :!secure -s.
:[redacted] 333 [00][XP][SP2][USA]-131615421 #[redacted] {XP}-5187341 1191757621.
:[redacted] 353 [00][XP][SP2][USA]-131615421 @ #[redacted] :[00][XP][SP2][USA]-131615421 .
:[redacted] 366 [00][XP][SP2][USA]-131615421 #[redacted] :End of /NAMES list..
:[00][XP][SP2][USA]-131615421![redacted]@[redacted].net JOIN :#[redacted].
:[redacted] 353 [00][XP][SP2][USA]-131615421 @ #[redacted] :[00][XP][SP2][USA]-131615421 .
:[redacted] 366 [00][XP][SP2][USA]-131615421 #[redacted] :End of /NAMES list..
```

Reverse Tunnel



Networks on Many Levels

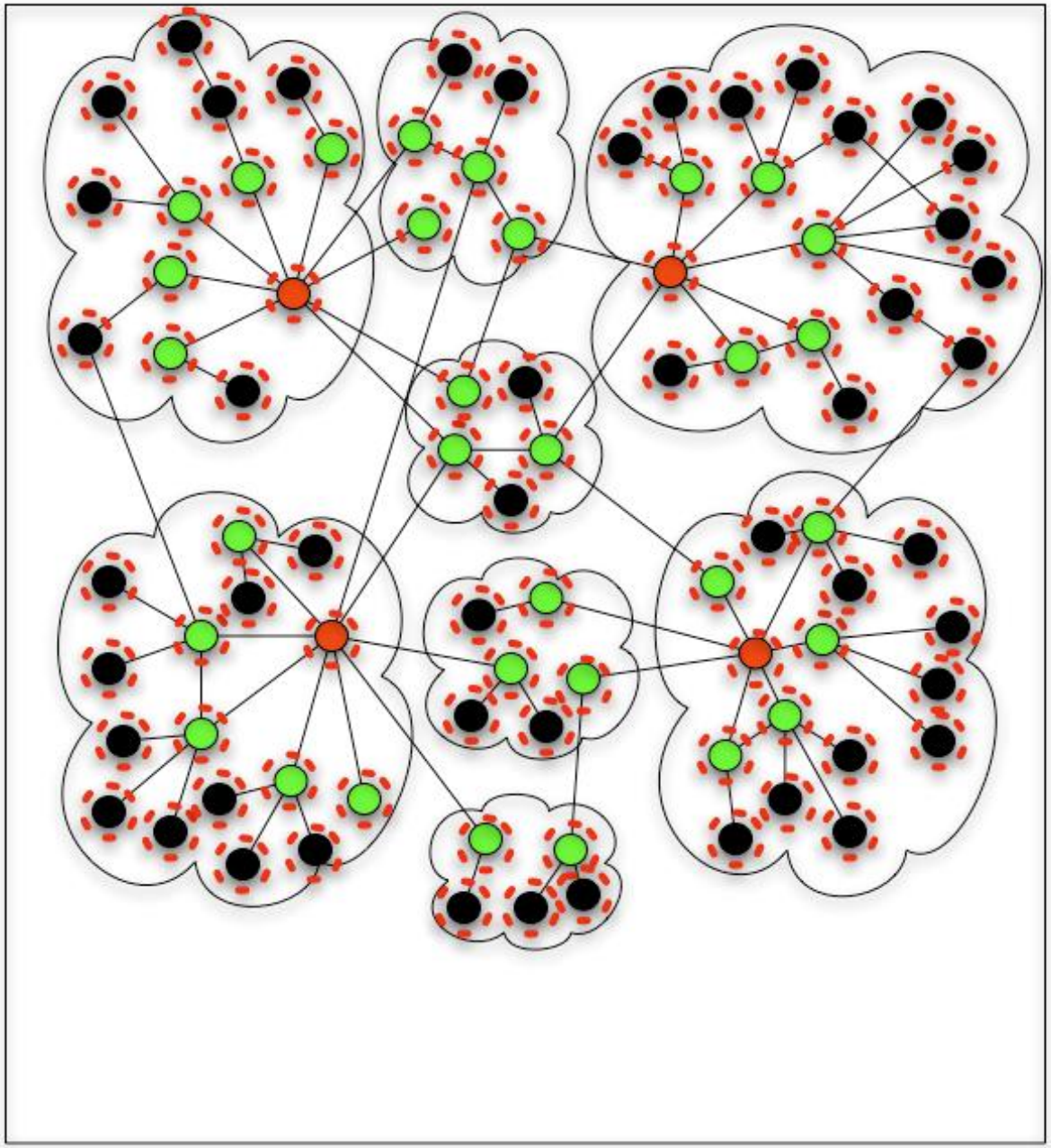
Physical (routers, switches, wires…)

Logical (domains, subnets…)

Political (enterprises, organizations, departments…)

Social (Employment, collaborations, affiliations…)

All are attacked: at the same time!



Case Studies

Operation “Cyberslam” (2003-04)

Israeli “Trojan Horse” (2005)

Storm Trojan (2006-07)

Operation “ ” (2003-04)

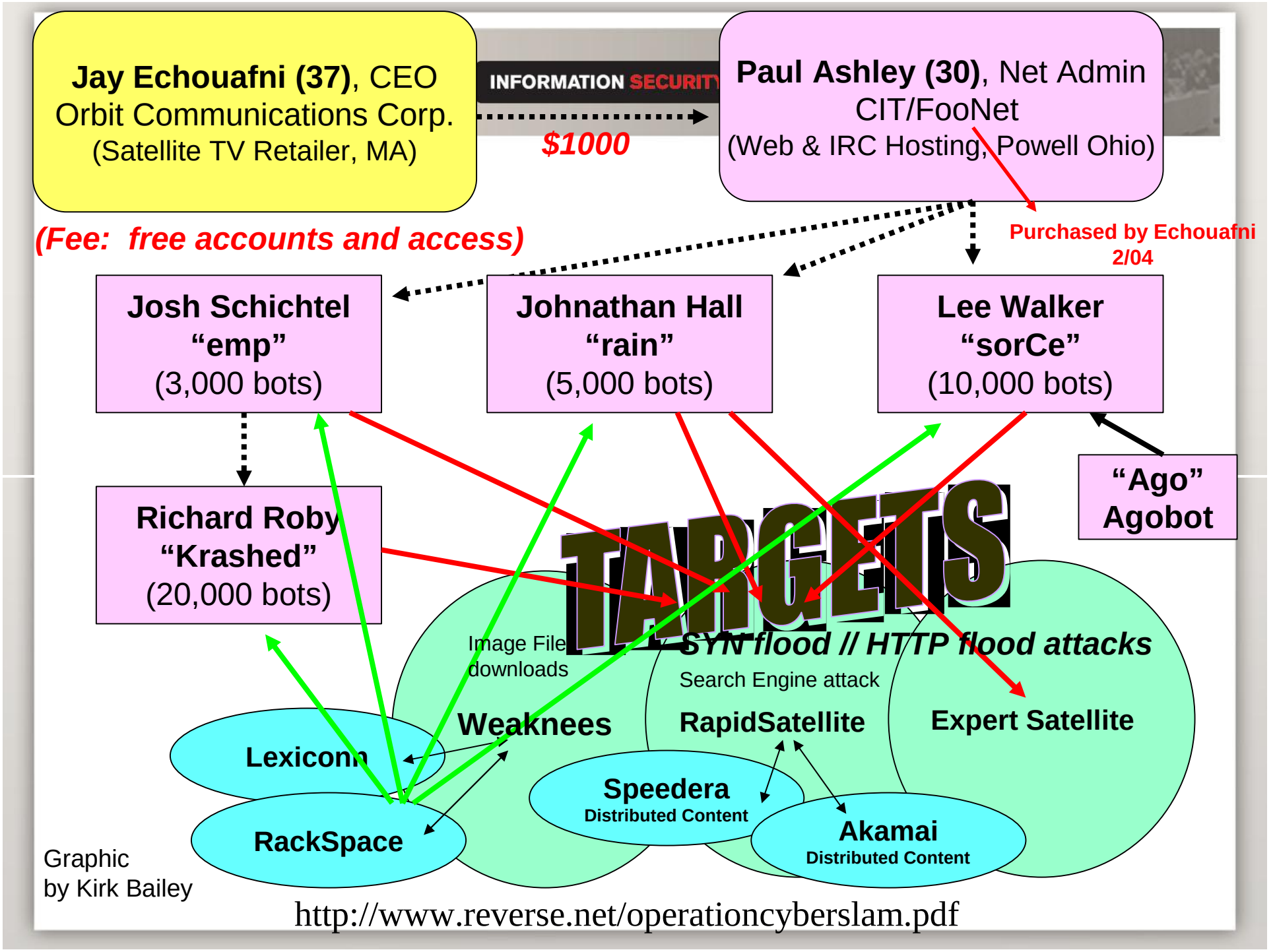
“*The first case of its kind involving a DDoS for commercial advantage or for hire*”

- 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]
- -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



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

- Custom Trojan Horse Key Logger, installed and run for PI firms in Israel
  - One year+ operation
  - US$4000/host

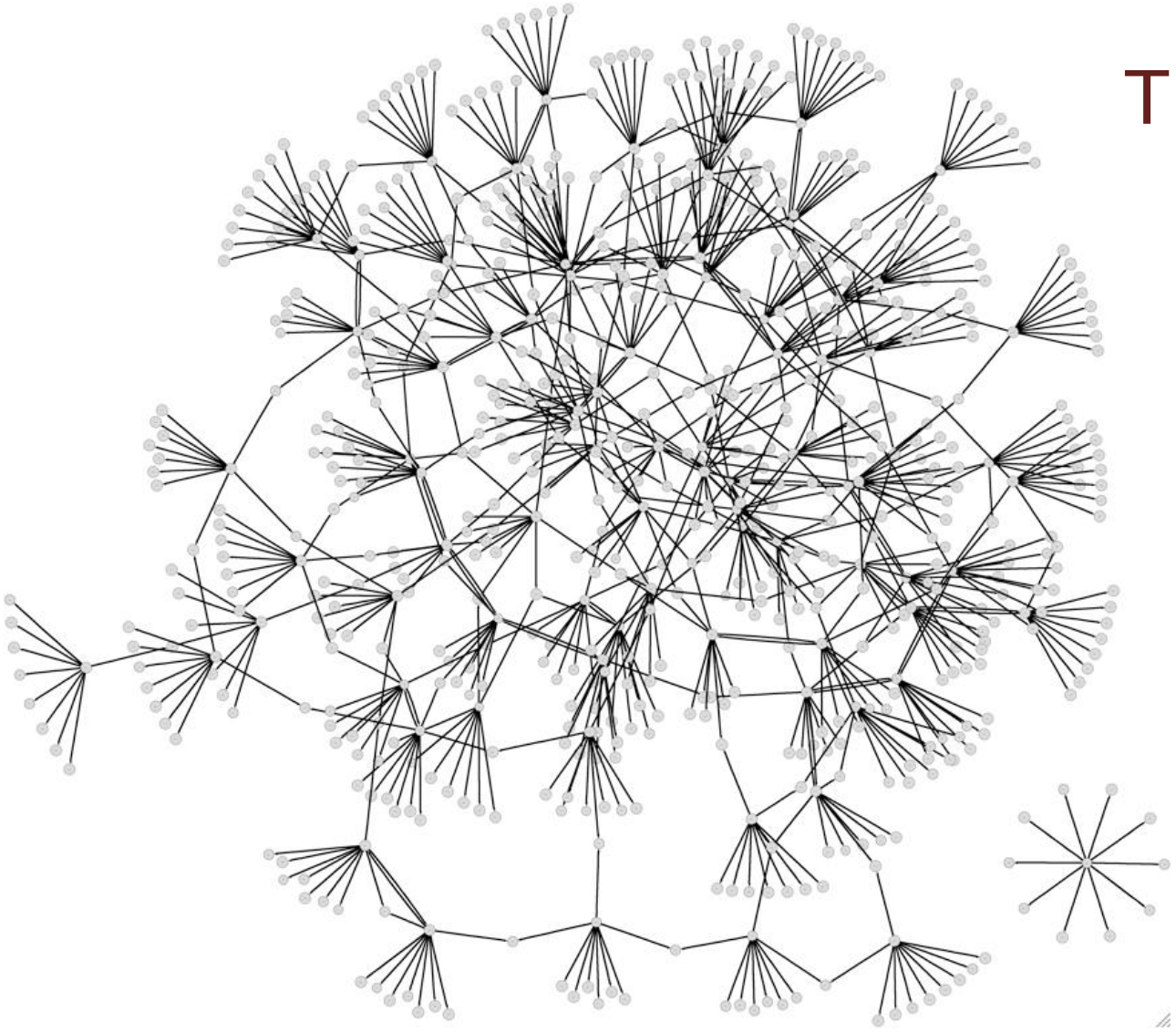
17 year old son)

100+ pieces of computer equipment seized

Caught because of mistake, not detection

Storm Trojan (2007)

- Storm is NOT a worm
- Population estimates are highly exaggerated
  - Wikipedia states 1-50 Million!
  - Microsoft MSRT (Sept. 11 release) cleaned ~300,000 infections (Win32/Nuwar)
- Multi-part malware kit
- Uses a “pull” model of C&C after finding server via eDonkey/Overnet P2P protocol
- Very prolific spam engine



The Shape to Come?

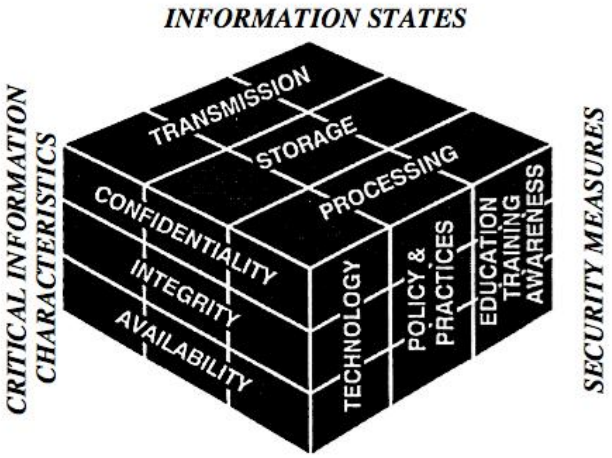
So what do we do?

- Layered and complementary defenses
- Do all: Protect, Detect, and React
- Not all solutions are technical
- Support those tackling the hard problems

- 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



Can we strike back?

“I’m mad as hell, and I’m not going to take this anymore!”
Network

Strike back

Possible mechanisms include

- Launching counter attacks (perhaps DDoS)
- Attempting to compromise the attacking host to remove the attack engine or disable the host
- Isolating the attacker from the net by reconfiguring its upstream router

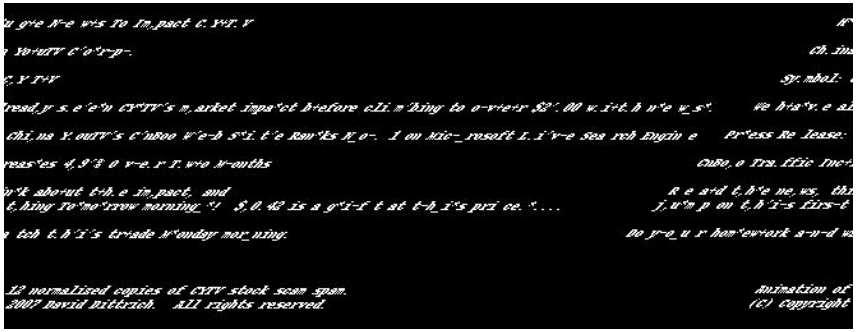
Who is easier to catch: The good guy who doesn't hide, or the bad guy who does?

Option	Opinion
Fight DDoS with DDoS	Are you *serious*?
Pre-emption	Highly unlikely
Retribution	High risk
Back-tracking through systems of 3rd parties	Moderate Risk
Information gathering	Low risk
Ambiguity/dynamism	Low risk

How bad an idea was “ ”

(Let me ways.)

In case there is *any* doubt…



…even if they do come up with some cool tactics!

Over 100,000 downloads of the screen saver

Activates in standby mode

Gets XML list of targets (URL Blacklist)

```
<target id="TVRnMA;;" domain="www.artofsense.com" hits="2251"
bytes="6436860" percentage="96.5" responsetime01="410.0”
responsetime02="410.0" location="US"
url="http://www.artofsense.com/english/" />
```

Sends mal-

```
<makeLOVEnotSPAM>
5?l[?ojMlm(Ngjm?_?vp+*xz4l(C5>
</makeLOVEnotSPAM>
```

Stated motives - Molte Pollman

"I have to be very clear that it's *not a denial-of-service attack…that would be illegal*, but we can *send a strong signal that spam is unacceptable*."

"We *slow the remaining bandwidth to 5 percent.* It wouldn't be in our interests to [carry out DDoS attacks]. It is to *increase the cost of spamming*. We have an interest to make this, economically, not more attractive."

"[We decided we] should *attack the flow of money and make it harder to profit* from [spamming]."

Web site: *"Annoy* a spammer now!"

EFFECTS OF THE CAMPAIGN

The sites that are targeted from the Make LOVE not SPAM screensaver aren't making money from getting more requests, it is actually the opposite. These sites don't sell advertising space (banners), they are just trying to sell their products at the lowest cost possible. They have to pay for their bandwidth, therefore more requests means higher bills.

The numbers below show how response times have decreased.

DOMAIN NAME	%	Traffic
www.bokwhdok.com	-85%	1,93 Gb
www.rxmedherbals.info	-41%	2,16 Gb
blundering.subbvbvf.com	-21%	8,45 Gb
m39.computergearplus.com	-15%	1,99 Gb
www.artofsense.com	-10%	4,68 Gb
www.fingermygirlfriend.com	-5%	3,41 Gb
printmediaprofits.biz	-64%	7,04 Gb

Netcraft detects two Chinese sites are completely unavailable

Relevant Ethical Principles

The Defense Principle

The Necessity Principle

The Evidentiary Principle

Punitive actions not ethical/legal

Ethics - The Defense Principle

Use “force” to protect self/others

- Response is proportional
- Necessary to cease harm
- Directed only at those responsible

Ethics -

Morally acceptable to infringe a right if and only if:

- Infringing results in greater moral value
- Good of protecting << Result of infringing
- There is no other option besides infringing

Ethics - The Evidentiary Principle

Morally permissible to take action under principle P if you have adequate reason to believe all preconditions of applying P are satisfied

- Defense Principle
  - Is the force proportional?
    - N spam emails == X Gb?
  - Is it targeted properly?
    - Customers of spammers, not spammers
    - Innocent third parties?
- Necessity Principle
  - Does it achieve a greater moral value? (i.e., costing spammers $$$)
  - Is there any other way to raise spammers' costs?
  - Is this a greater moral value than unimpeded use of purchased network resources?
- Evidentiary Principle
  - Is there adequate reason to believe *all* preconditions are satisfied?

Verdict on MLNS

was justifiable

They may have used excessive, indiscriminate "force"

They clearly had a punitive motive

- Violation of CFAA (or similar) laws?
- Informed consent/misrepresentation?
- Liability for damages to innocent parties?
- What if miscreants trick MLNS into attacking .mil sites, or innocent .com sites?

In Conclusion…

We are *way* beyond “just patch, buy AV, install a firewall and an IDS, and you’ll be OK.”

Attacks are going to keep getting more subtle, more sophisticated, and more complex

Defenses had better follow suit, or we’re in trouble

Lots of opportunities for more collaborative response…

…but risk if actions go too far

HUGE need for more research funding

Thanks

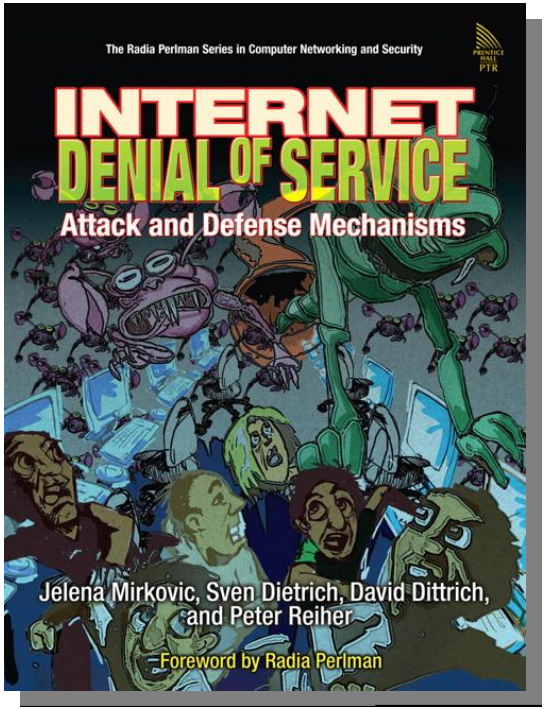
Kirk Bailey & The Agora
Mike Eisenberg/David Notkin
Harry Bruce/Bob Mason/iSchool staff
Sven Dietrich, Sam Stover &
Christian Seifert

Questions?

Dave Dittrich

Senior Security Engineer/
Affiliate InfoSec Researcher
The Information School
University of Washington

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



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