David Dittrich – University of Washington Tacoma

THE ACTIVE RESPONSE CONTINUUM

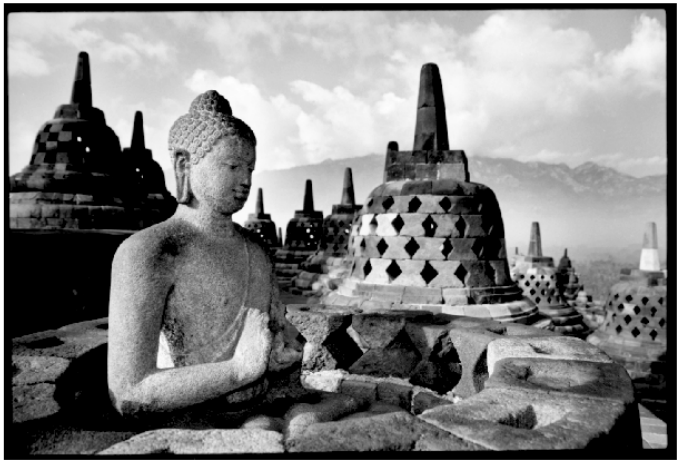
DEBATING THE FUTURE OF "HACKING BACK" IN TERMS OF LANGUAGE, ETHICS, AND LAWS

NCSC One 2017
The Hague, Netherlands
May 17, 2017

Agenda

- The Active Response Continuum
- Ethics and the Law
- Arguments for "hacking back"
- A "Right Action" Framework

Grayscale



Binary

Temple Borobudur, East Java, Indonesia, 1996, David Dittrich.

Google Play's family share pl | Manage your family group - C | Alicia Keys: HERE - Music on | Dave Dittrich

web.archive.org/web/20000815082203/http://www.washington.edu/People/dad/

INTERNET ARCHIVE WayBackMachine

http://www.washington.edu/People/dad/ Go

299 captures
19 Feb 99 - 2 May 16

JUN AUG OCT
1999 15 2001
2000

Close

Help

I'm a Software Engineer and Consultant for the University of Washington's Computing & Communications *Client Services* group, consulting mostly on system security, UNIX system administration, and X Window System related issues.

I used to support World Wide Web services, including the initial prototype and subsequent support of the University's original, now retired, **Weber** web service (and proud father of the Weber Guy).

While I am *not* a professor, I do teach the UW Education & Training course:

- *R870: Unix System Administration - A Survival Course*
  [Search the R870 course notes]

Dave Dittrich

Free Speech Online
Blue Ribbon Campaign

... and occasionally give talks or create Web pages on topics such as:

Talks/Interviews

- Training Ninja at Black Hat '00 [Course notes for Unix forensics class]
- Panelist at the Tomorrow's Technology Today (T3) Conference, Pittsburgh, PN, April 8, 2000
- Panelist on the Diane Rehm show (WAMU radio, NPR affiliate) along with Jeffrey Hunker (coordinator for security, infrastructure protection, and counter-terrorism for the National Security Council), James Adams (CEO of iDefense), and Elias Levy (SecurityFocus.com), February 17, 2000
- Info.sec.radio interview (Originally broadcast March 6, 2000)
- Panelist at Distributed Denial of Service (DDoS) BoF, RSA Conference 2000 (January 17, 2000)
- Panelist at Distributed Denial of Service (DDoS) BoF, NANOG 18 Meeting (February 7, 2000)
- Presentation on Distributed Denial of Service attacks at CERT Distributed-Systems Intruder Tools Workshop (November 2, 1999)
- **Some TCP/IP Vulnerabilities**, Seattle Agora Meeting (December 10, 1999)
- **Unix Security Overview** (1998)
- **Quarterly Departmental Support meeting Security talk** (1999)
  - What can be done with limited time to secure Unix systems?
  - What can be done with limited time to secure Windows NT systems?
- Information Security Management Overview (1999)
- Host and Network Security in the Internet Age: DSL, @Home, ISDN, etc., Seattle Unix User's Group (1998)
- Panelist at SANS '97 technical conference (SA4) Problem Tracking Systems Panel/Workshop (4/97) [Trip report, PowerPoint Slides of talk on QnA, HTML version]
- Web services for the University of Washington (1996)
- Sun's Java langauge (1996)
- Talks on Java and Unix Security at AUUG WET'96 in Darwin, Northern Territory, Australia (4/96)
- An Introduction to WWW (1994)
- Unix System Security (1994 version)

```
================================================================================

  The DoS Project's "trinoo" distributed denial of service attack tool

================================================================================

David Dittrich <dittrich@cac.washington.edu>
University of Washington
Copyright 1999. All rights reserved.
October 21, 1999


Introduction
------------

The following is an analysis of the DoS Project's "trinoo" (a.k.a.
"trin00") master/slave programs, which implement a distributed
network denial of service tool.

Trinoo daemons were originally found in binary form on a number of
Solaris 2.x systems, which were identified as having been compromised
by exploitation of buffer overrun bugs in the RPC services "statd",
"cmsd" and "ttdbserverd".  These attacks are described in CERT
Incident Note 99-04:

        http://www.cert.org/incident_notes/IN-99-04.html

The trinoo daemons were originally believed to be UDP based,
access-restricted remote command shells, possibly used in conjunction
with sniffers to automate recovering sniffer logs.

During investigation of these intrusions, the installation of a trinoo
network was caught in the act and the trinoo source code was obtained
from the account used to cache the intruders' tools and log files.
This analysis was done using this recovered source code.
```

Denial-of-Service Developments

This advisory is being published jointly by the CERT Coordination Center and the Federal Computer Incident Response Capability (FedCIRC).

Original release date: January 3, 2000
Source: CERT/CC and FedCIRC

Systems Affected

- All systems connected to the Internet can be affected by denial-of-service attacks.

I. Description

Continued Reports of Denial-of-Service Problems

We continue to receive reports of new developments in denial-of-service tools. This advisory provides pointers to documents discussing some of the more recent attacks and methods to detect some of the tools currently in use. Many of the denial-of-service tools currently in use depend on the ability of an intruder to compromise systems first. That is, intruders exploit known vulnerabilities to gain access to systems, which they then use to launch further attacks. For information on how to protect your systems, see the solution section below.

…

We thank Dave Dittrich of the University of Washington, Randy Marchany of Virginia Tech, Internet Security systems, UUNet, the Y2K-ICC, the National Infrastructure Protection Center, Alan Paller and Steve Northcutt of The SANS Institute, The MITRE Corporation, Jeff Schiller of The Massachusetts Institute of Technology, Jim Ellis of Sun Microsystems, Vern Paxson of Lawrence Berkeley National Lab, and Richard Forno of Network Solutions.

Active Response Continuum

- First Agora workshop (June 8, 2001)
  - 3 more, funded by Cisco, through 2004

Level	Actor's Posture	Characteristic Actions
4	Non-cooperative	Intelligence collection, unilateral traceback, "cease & desist", retaliatory counterstrike [takedown/ takeover]
3	Cooperative	Joint traceback, collaboration, sharing
2	Interactive	Modify own systems in response to attack
1	Involved	Uses AV, simple firewalls, basic encryption
0	Unaware	None (expect others to protect them)

David Dittrich and Kenneth E. Himma. Active Response to Computer Intrusions. Chapter 182 in Vol. III, Handbook of Information Security, 2005. http://ssrn.com/abstract=790585

"Active Defense"

- Agora workshop defined "Active Defense" to be activity at Level 4
- Level 4 has sub-levels, though
  - Less intrusive to more intrusive
  - Less risky to more risky
  - Less disruptive to more disruptive
- Justification for your actions depends on how responsibly you progress through all Levels

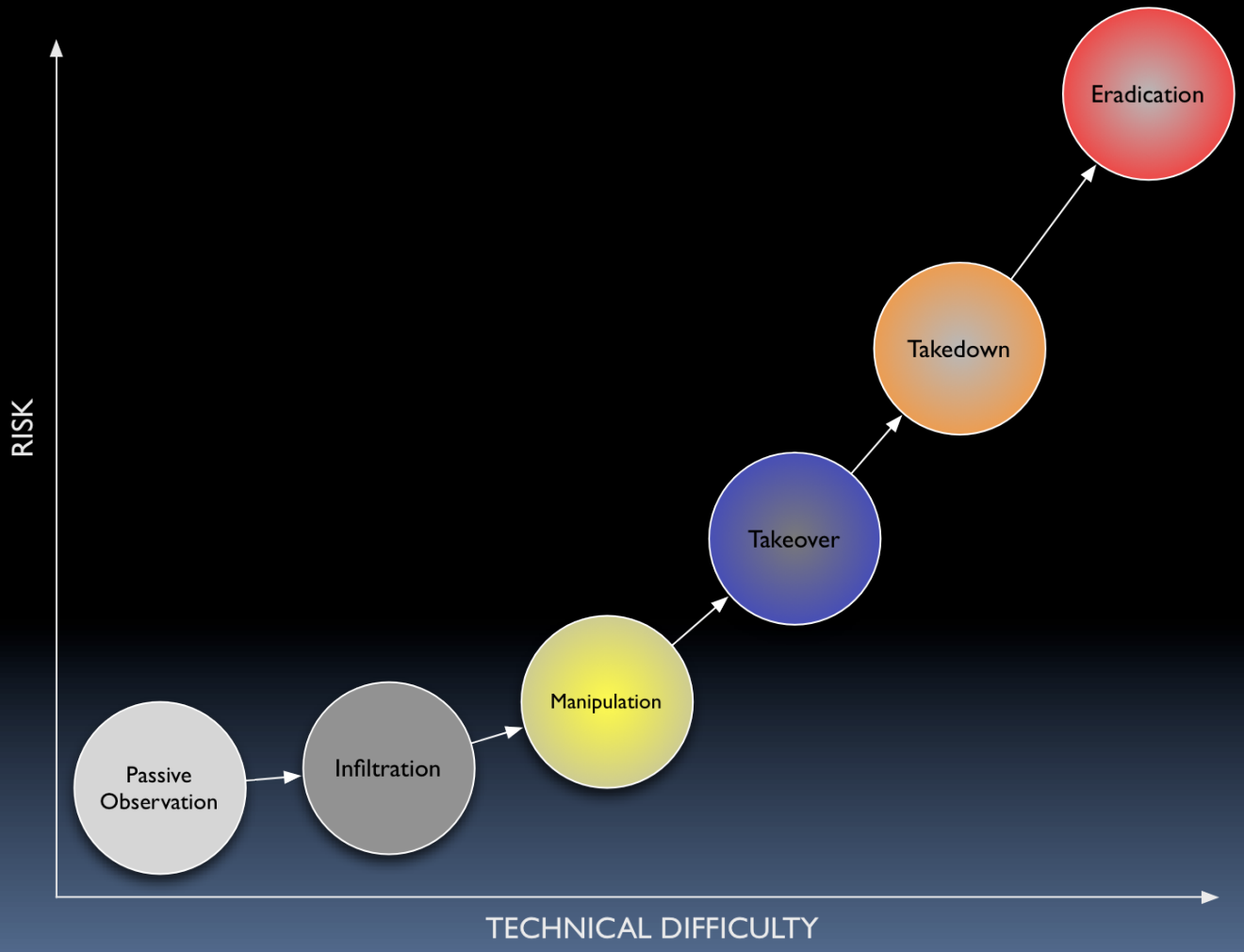
"Active Response Continuum" is a better phrase

Levels of Active Defense

- 4.1 - Non-cooperative 'intelligence' collection
  - External services
  - Back doors/remote exploit to access internal services
- 4.2 - Non-cooperative 'cease & desist'
  - "Interdiction" ala Berman-Coble bill
  - Disabling malware
- 4.3 - Retribution or counter-strike
- 4.4 - Preemptive defense (a.k.a. "offense")

Level 4 involves actions taken *outside your sphere of authority*, *without cooperation* of owners/operators of impacted systems

Levels of Aggressiveness



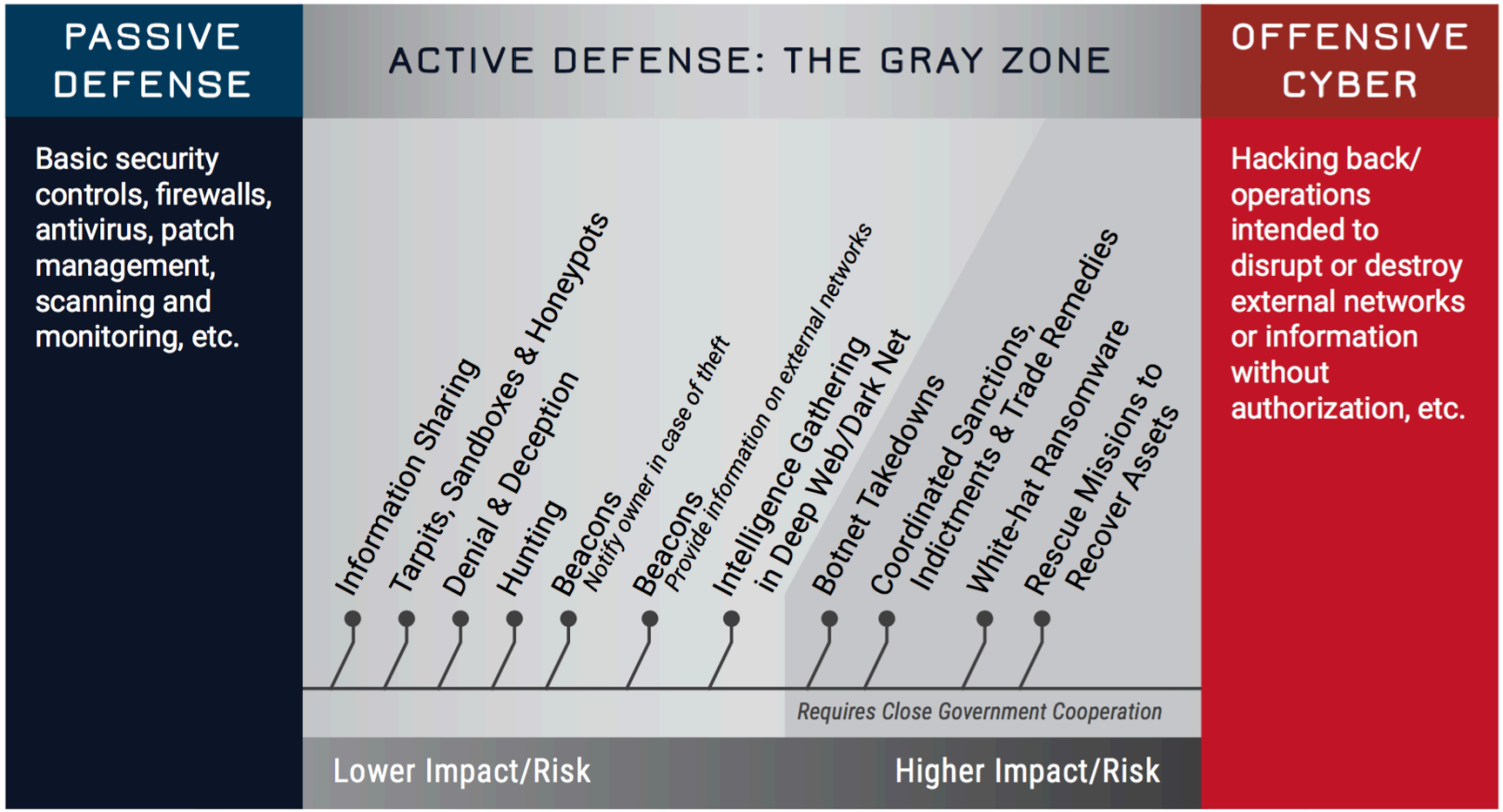
Adapted from: David Dittrich and Kenneth E. Himma. Active Response to Computer Intrusions. Chapter 182 in Vol. III, Handbook of Information Security, 2005. http://ssrn.com/abstract=790585

Active Cyber Defense

- Substitute "Cyber" for "Air and Missile" in DoD "Active Air and Missile Defense" (Joint Publication 3-01)
- "Active" vs. "Passive"
- Four dimensions
  - Scope of effects
  - Degree of cooperation
  - Types of effects
  - Degree of automation
- Justification based on: non-combatant immunity; necessity; proportionality; actions not being retributive or retaliatory

Dorothy E. Denning and Bradley J. Strawser, "Active Cyber Defense: Applying Air Defense to the Cyber Domain," presented at Cyber Analogies Seminar, Department of Defense, U.S. Cyber Command, May 3, 2013.

FIGURE 2. ACTIVE DEFENSE: THE GRAY ZONE



Into the Gray Zone: The Private Sector and Active Defense Against Cyber Attacks, Center for Cyber and Homeland Security, October 2016.
https://www.oodaloop.com/wp-content/uploads/2016/10/CCHS-ActiveDefenseReportFINAL.pdf

Ethics and the (U.S.) Law

Ethical Frameworks

- Deontology (normative)
  - Rules

    Torture is always wrong
- Consequentialism
  - Focus on outcomes
  - "The end justifies the means"

    If it saves `$LIVES`, *torture is acceptable*
- Virtue Ethics
  - Focus on the actor, their history of acting in a virtuous manner

"Integrity, as I❖ define it…"

- Ability to discern right from wrong
- Acting on what you have discerned, even at personal cost
- Saying openly that you are acting on your understanding of right from wrong and how you came to chose the "right action"

❖ Stephen L. Carter. Integrity. BasicBooks – A division of Harper Collins Publishers, 1996. ISBN 0-465-03466-7
http://www.stephencarterbooks.com/books/nonfiction/integrity

"Right Action"

- The Right Agent
- Done to the right person
- At the right time and place
- To the right degree
- In the right way, and
- For the right reason

"Right action is that which a person with practical wisdom, that is, the ability to reason well, would choose in the circumstances."

D. Chan, Beyond Just War: A Virtue Ethics Approach, ISBN 978-1-137-26340-7. Palgrave Macmillan, 2012.

Existing Ethical Norms

	Principle	Question
Societal Code	Defense	Population being protected is identified?
	Defense	Looks like use of *force*?
	Defense	Actions are proportional?
	Defense	Necessary to repel or prevent harm?
	Defense	Benefits of disclosure favor victims over attackers?
	Defense	Actions are appropriately directed?
	Necessity	Greater moral good defined?
	Necessity	No other reasonable options available?
	Necessity	Otherwise respectful of rights?
	Punishment	Avoids punitive motives?
	Retribution	Avoids retributive motives?
	Evidentiary	Adequate reason to think preconditions of applying other principles are met?
Professional Code	Do Good	Positively impacts human well-being?
	Avoid Harm	Harms users, public, employees, or employers?
	Avoid Harm	Efforts made to mitigate or undo negative consequences?
	Be Honest	Honors property rights?
	Be Honest	Gives proper credit?
	Be Honest	Honors confidentiality?
	Be Fair	Discriminates on basis of race, sex, religion, age, disability, or nationality?
	Be Fair	Inequities exist between groups?
	Privacy	Minimal information collected?
	Privacy	Protected from unauthorized access?
	Privacy	Data used only for intended purposes?
Academic Code	Respect for Persons	Individuals treated as autonomous agents?
	Respect for Persons	Individuals (or their providers) informed and allowed to consent?
	Respect for Persons	Individuals with diminished autonomy protected?
	Respect for Persons	Identities of innocents are protected?
	Beneficence	Low potential to inflict harm?
	Beneficence	Maximize possible benefits and minimize harms
	Beneficence	Risks and benefits systematically evaluated
	Justice	Who benefits?
	Justice	Fairness (neutrality) of procedures

D. Dittrich, M. Bailey, and S. Dietrich. Building An Active Computer Security Ethics Community. *Security Privacy, IEEE, 9(4):32–40, July/August 2011.*

DHS S&T and the Menlo Report

- DHS Working Group on Ethics in ICTR
  - Inaugural workshop May 26th-27th, 2009 in Washington, DC
  - Lawyers, Computer Scientists, IRB Members, Ethicists
- Goal: Create an updated Belmont report for the field of ICTR
- Published in Federal Register, Dec. 2011
  - Revision based on comments delivered May 2012
  - Engaging Industry, other USG, IRB community

Stakeholder Analysis

- **Primary** Stakeholders

  "Those ultimately affected [either positively or negatively]"

- **Secondary** Stakeholders

  "Intermediaries in delivery [of the benefits or harms]"

- **Key** Stakeholders

  "Those who can significantly influence, or are important to the success [or failure] of the project"

Stakeholder Analysis by Example

- D. Dittrich. The Ethics of Social Honeypots. Research Ethics, May 2015. doi: 10.1177/1747016115583380. http://rea.sagepub.com/content/early/2015/05/19/1747016115583380.abstract.
- Honeynet Project. FAQ on Kelihos.B/Hlux.B sinkholing, March 2012. http://www.honeynet.org/node/836
- D. Dittrich, F. Leder, and T. Werner. A Case Study in Ethical Decision Making Regarding Remote Mitigation of Botnets. In Proceedings of the 14th International Conference on Financial Cryptograpy and Data Security, FC'10, pages 216–230, Berlin, Heidelberg, 2010. Springer-Verlag. http://staff.washington.edu/dittrich/papers/wecsr2010-botethics-dlw.pdf

Evidentiary Standards

System	Authority	Standard
Criminal	Title 18 U.S.C.	Beyond a reasonable doubt, probable cause, reasonable belief/suspicion, credible
Civil	Common Law	Preponderance of the evidence, clear and convincing, substantial
Military	Title 10 U.S.C.	"A high threshold of certainty." *
Intelligence	Title 50 U.S.C.	Not oriented towards prosecution
Threat intelligence companies	None (see Title 18 U.S.C.)	No standards (also no accepted ethics guidelines or code of conduct)

* J. Carr. Responsible Attribution: A Prerequisite for Accountability. The Tallinn Papers, a NATO CCD COE publication on Strategic Cyber Security, 2014.
https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%20%206%20Carr.pdf

The Arguments for Hacking Back

"Hacking back"

- J. Rabkin and A. Rabkin. Hacking Back Without Cracking Up, June 2016. Series Paper No. 1606. https://drive.google.com/file/d/0B_PclSuEzVCVYU01bE5fUjFEMHM/view
- S. Baker, Steptoe Cyberlaw Podcast: An Interview with Jeremy and Ariel Rabkin, July 2016. https://www.lawfareblog.com/steptoe-cyberlaw-podcast-interview-jeremy-and-ariel-rabkin

Rabkin Argument in Normal Form

Since organizations have been compromised repeatedly over the past two decades,
and these compromises are an attack on victimized organizations,
and these attacks constitute the largest transfer of wealth in human history,
and these compromises are likely to increase as time goes on,
and the most clever & determined hackers manage to work around almost all defensive measures,
and defenders in victimized organizations are frustrated,
and law enforcement is unable to protect these organizations from becoming victims,
and the federal government is incapable or disinclined to deal with the threat,
and these victims can identify who is attacking them from their system logs,
and they can accurately trace back and attribute who is attacking them,
and industry will likely develop a greater capacity to handle this threat than will the government,
and industry already successfully uses a model of private investigators to protect themselves
and new law authorizing private sector strike back would take a long time to write and be difficult
and new laws or regulations are long-term commitments (withdrawal f/w is awkward or difficult) ,
and experimenting with private sector strike back may be effective/may not cause harm,
therefore it is feasible and advisable to begin experimenting with authorizing private hack-back.

Core Elements

- These attacks constitute the largest transfer of wealth in human history
- These compromises are likely to increase as time goes on
- Law enforcement is unable to protect these organizations from becoming victims
- The federal government is incapable or disinclined to deal with the threat

∴ We can trust the private sector to safely use "Active Defense" to defend themselves

Greatest Transfer of Wealth

"The annual losses are likely to be comparable to the current annual level of U.S. exports to Asia - over $300 billion. The exact figure is unknowable, but private and governmental studies tend to understate the impacts due to inadequacies in data or scope. The members of the Commission agree [with…] General Keith Alexander, that the ongoing theft of IP is `the greatest transfer of wealth in history.' "

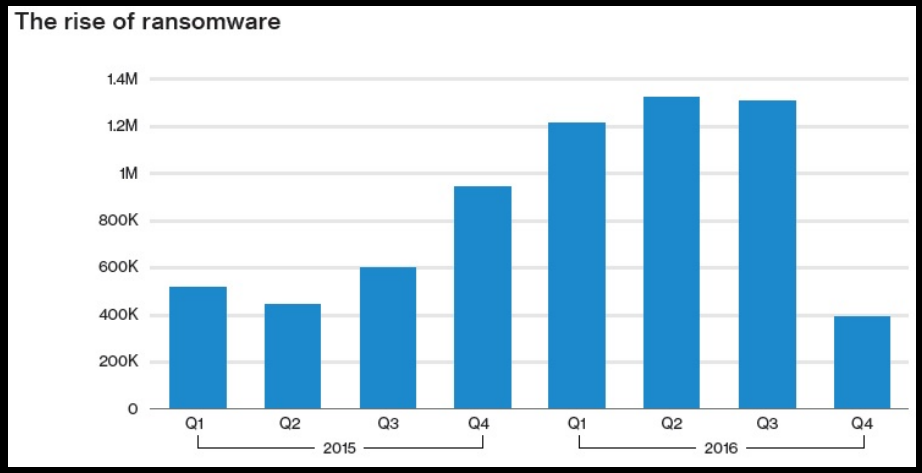
The National Bureau of Asian Research. The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property, May 2013. http://ipcommission.org/report/IP_Commission_Report_052213.pdf

"Calculating US losses from the technology outflow is difficult. Private estimates put the combined costs of foreign and domestic economic espionage [by all methods], including the the of intellectual property, as high as $300 billion per year and rising."

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2002, Office of the National Counterintelligence Executive, NCIX 2003-10006, 2003.
https://fas.org/irp/ops/ci/docs/2002.pdf

"Fewer than 1 percent of the firms surveyed were willing to attach figures to their losses of intellectual property, but the totals from those who made estimates amounted to $151 million in 2001, up from only about $67 million the previous year and $20 million in 1997."

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2002, Office of the National Counterintelligence Executive, NCIX 2003-10006, 2003.
https://fas.org/irp/ops/ci/docs/2002.pdf



"Compared to last year's DBIR report, ransomware attacks are up 50 percent. Still, Verizon suspects the true number of ransomware attacks and victims is likely going under reported. […] 'Organized criminal groups continue to utilize ransomware to extort money from their victims, and since a data disclosure in these incidents is often not confirmed, they are not reflected in statistical data,' Verizon wrote."

T. Spring. Ransomware, Cyberespionage Dominate Verizon DBIR, April 2017. https://threatpost.com/ransomware-cyberespionage-dominate-verizon-dbir/125261/.

"The majority of errors in our corpus come from the government organizations that contributed to the report, not because they are more prone to mistakes than the rest of us, but because they have more stringent reporting requirements than most other industries."

Verizon. 2017 Data Breach Investigations Report, April 2017. http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf

Efficacy and Risks

See also:

D. Dittrich. So You Want to Take Over a Botnet… In LEET'12: Fifth USENIX Workshop on Large-Scale Exploits and Emergent Threats, April 2012. https://www.usenix.org/conference/leet12/so-you-want-take-over-botnet

D. Dittrich. So You Want to Take Over a Botnet… Presentation to Microsoft Digital Crimes Consortium 2013 meeting, February 2013. http://staff.washington.edu/dittrich/talks/dcc2013_dittrich_botnets.pdf

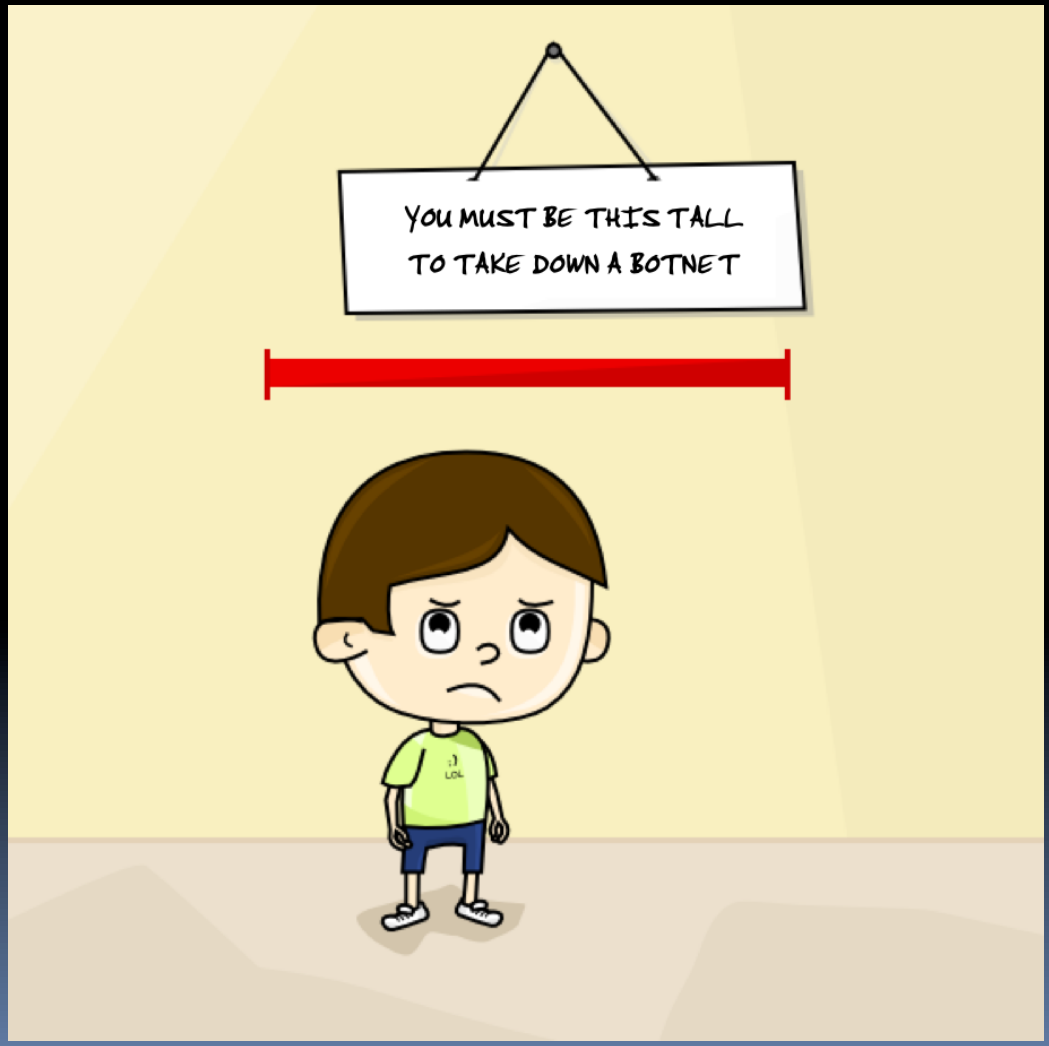
Botnet takedown

"It's very risky [if] you don't combine a legal operation with a technical operation. We've seen in the [past that when they suspect they have been discovered] they try to destroy evidence. [We] assumed that if this legal operation was started, they would probably try to [issue the `os_kill` or `user_destroy` commands] to destroy some machines."

Tillmann Werner

E. Peterson, M. Sandee, and T. Werner. GameOver Zeus: Badguys And Backends, BlackHat USA 2015, August 2015. https://youtu.be/KkEVwswqIBs

How to do it “right”



Prioritize Law Enforcement

"If we don't know about it and no one keeps track of it, then no one cares. [It's] incumbent on everyone in the information security industry to communicate how businesses are affected [by ransomware]. [We] don't get better as police officers without help from the community."

Detective Frank McLaughlin
Boston Police Department

C. Brook. Lack of Communication Achilles' Heel for Ransomeware Fighters. SOURCE Boston 2017, April 2017. https://threatpost.com/lack-of-communication-achilles-heel-for-ransomware-fighters/125264/.

Prioritize Spending

"[Depending] on the study, the U.S. is spending 2.5 to 4 times as much on cyber offense research and development as we are cyber defense. […] Pentagon spending on cybersecurity is essentially around 10 times as large as Homeland Security spending (it kind of depends on how you add up the different lines)."

Dr. Peter Singer on his new book, Cybersecurity and Cyberwar, International Affairs Forum interview. http://www.ia-forum.org/Content/ViewInternalDocument.cfm?ContentID=8089

“Right Action” Framework

- Follow virtue ethics (Integrity + “Right Action” justification)
- Handle deconfliction
- Provide before- and after-action review
- Favor government over private sector action at the extreme end of the ARC
- Favor civil/criminal process over extrajudicial private sector action

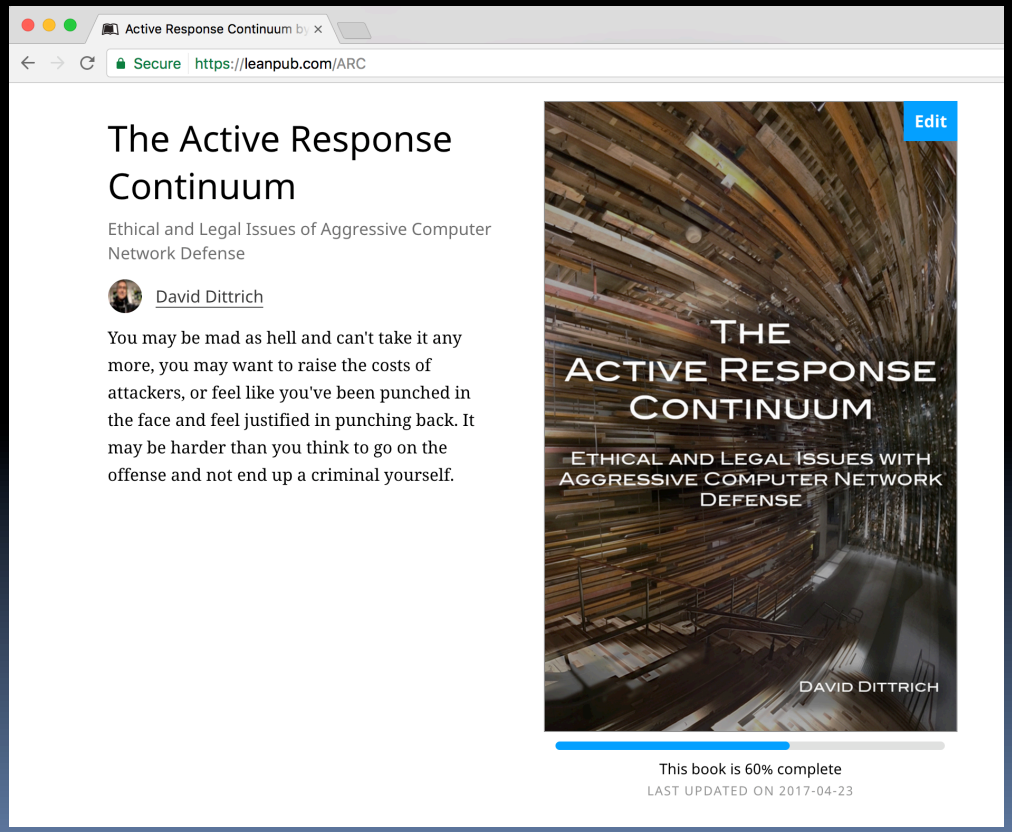
Contact

Dave Dittrich

dave.dittrich *at* gmail *dot* com

@davedittrich / @TheARCBook

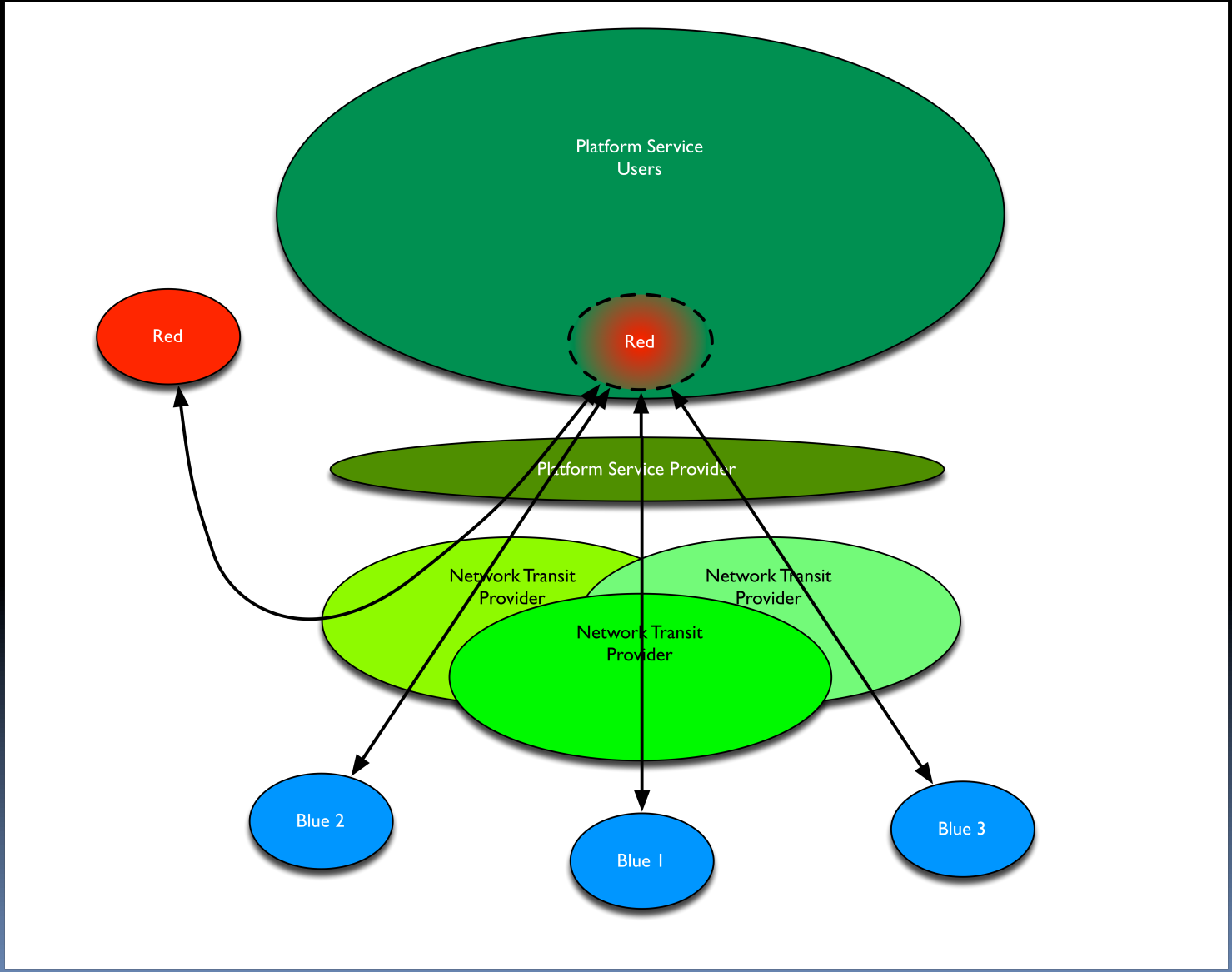
http://staff.washington.edu/dittrich/



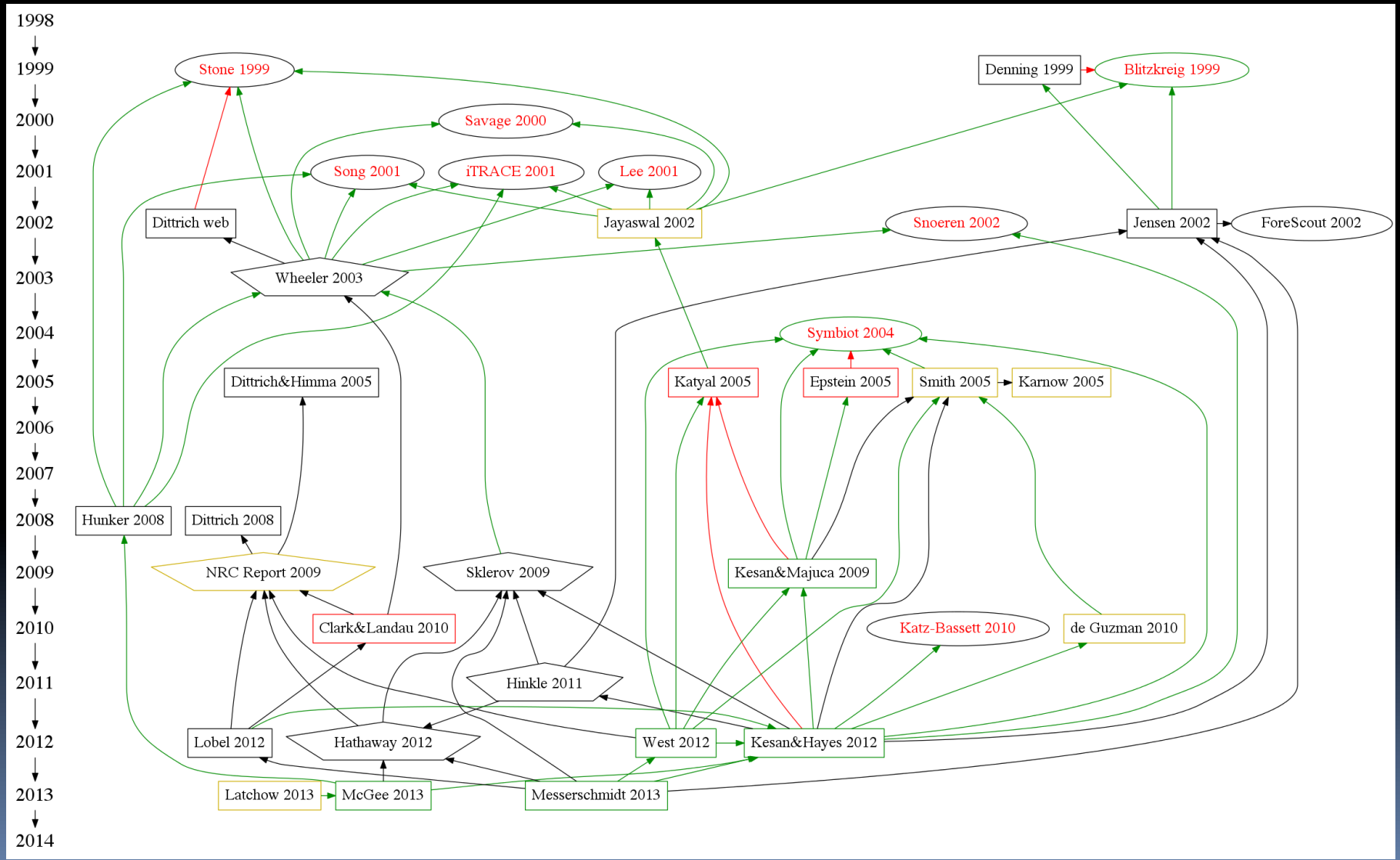
Thanks to Michael Bailey, Erin Kenneally, Sven Dietrich, Katherine Carpenter, Ken Himma, Kirk Bailey and members of Seattle's Agora, who contributed to the development of some of the concepts, content, and/or publications cited herein.

Extra slides

Relationships and “Distance”



Published Literature



Achieving the Desired Outcome

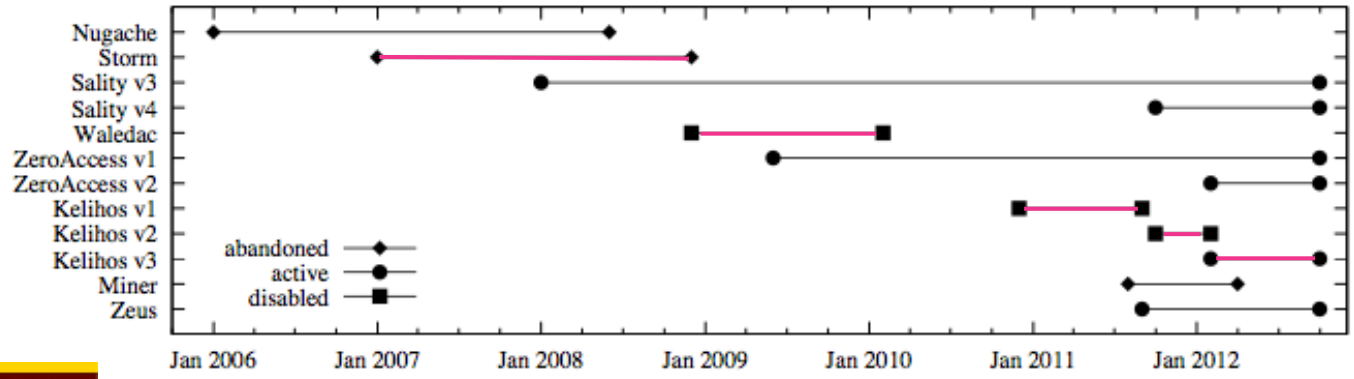
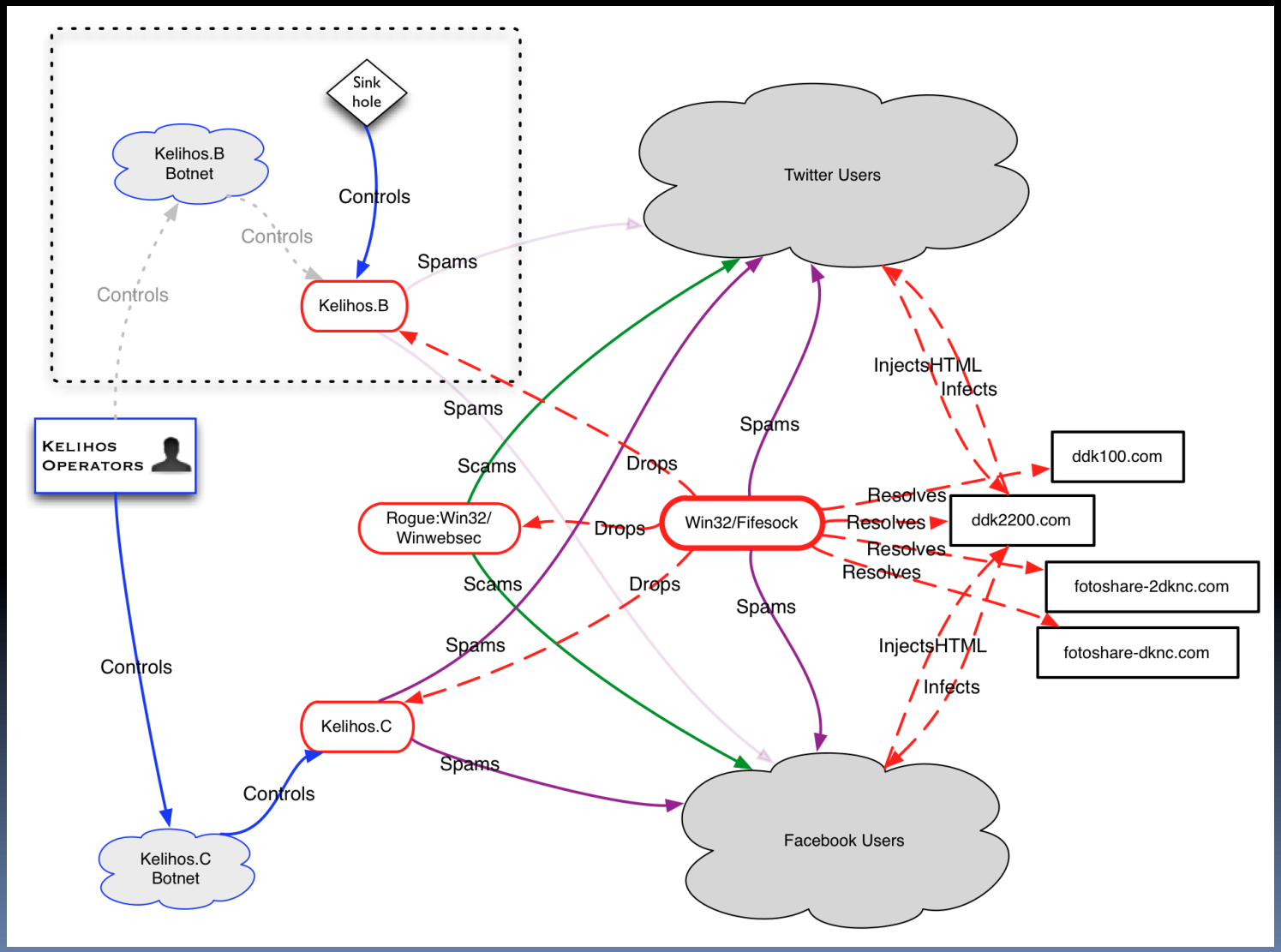


Figure 2: Lifespans of P2P botnet variants.

C. Rossow, D. Andriesse, T. Werner, B. Stone-Gross, D. Plohmann, C. J. Dietrich, and H. Bos. SoK: P2PWNED — Modeling and Evaluating the Resilience of Peer-to-Peer Botnets. In Proceedings of the IEEE Symposium on Security and Privacy, May 2013.

T. Werner. P2P Botnet Kelihos.B with 100.000 Nodes Sinkholed, March 2012. http://www.crowdstrike.com/blog/p2p-botnet-kelihosb-100000-nodes-sinkholed/index.html

Kelihos.B Sinkholing



Botnet takedown

"'We were actually a little surprised that it worked so well, even better than for Kelihos.A, where it took a few minutes for the poison to propagate,' [said Werner.] Within an hour they'd collected 50,000 machines — 10,000 more than they'd expected the entire botnet to contain. Marco Preuss at Kaspersky Lab had begun a coordinated poisoning effort and saw similar results; soon the number of sinkholed machines topped 100,000."

J. Hicks. Down the sinkhole: inside the Kelihos.B takedown. The Verge, April 2012. http://www.theverge.com/2012/4/30/2971958/kelihos-b-botnet-takedown-crowdstrike.

Botnet takedown

"But it was impossible to eliminate every uncertainty. 'You don't really know how good it's gonna work,' says Werner, 'as you cannot test it with the real botnet, obviously, and lab tests might miss something or the botmaster might take counteractions of some sort.' A savvy botmaster might notice his dwindling control and try to fight back."

J. Hicks. Down the sinkhole: inside the Kelihos.B takedown. The Verge, April 2012. http://www.theverge.com/2012/4/30/2971958/kelihos-b-botnet-takedown-crowdstrike.

Botnet takedown

"GameOver Zeus was designed [in] response to previous law enforcement investigations. [It] was designed to make it impossible for us to end up taking it over."

S.A. Elliot Peterson, FBI

E. Peterson, M. Sandee, and T. Werner. GameOver Zeus: Badguys And Backends, BlackHat USA 2015, August 2015. https://youtu.be/KkEVwswqIBs.

Botnet takedown

"They were running way behind—Werner's code wasn't close to being ready. Over the rest of the week, as Werner and Stone-Gross raced to finish writing, another teams [prepared to help] to take GameOver Zeus down. The White House had been briefed on the plan and was waiting for results. [The] team had known for months that the GameOver botnet was controlled by a server in Canada. But then, just days before the attack, they discovered that there was a second command server in Ukraine. The realization made hearts drop. 'If you're not even aware of the second box,' Werner says, 'how sure are you that there's not a third box?'"

G. M. Graff. Inside the Hunt for Russia's Most Notorious Hacker. Wired, March 2017. https://www.wired.com/2017/03/russian-hacker-spy-botnet/.

Case studies and Observations

Torpig

- A.k.a., Sinowal, Anserin
- First reported Feb. 2006
- Central C&C for rootkit (Mebroot) and keylog deposition
- UCSB takeover in Jan. 2009
  - 182,800 bot IDs (1,247,642 unique IPs)
  - 8310 accounts, 140 institutions
  - 8.7GB of Apache log files and 69GB of pcap data collected
- Attackers regained control after 10 days and patched bugs

Ozdok

- A.k.a., Mega-D
- First reported 2008
- Not well recognized by AV industry
- FTC gets court ordered shutdown of network in 2008 (back up < 1 year later)
- FireEye (cooperative) takedown initiated Nov. 2009
  - Notification of involved ISPs
  - Working w/registrars to cooperatively take down C&C domains
  - Registration of as-yet unused domains

Mariposa

- A.k.a., Rimecud, Krap, Pilleuz, Zbot
- First reported in 2009 by Defense Intelligence (zero to "largest botnet in the world" in months?!?)
- Central C&C on "bulletproof" hosting provider
  - Access concealed by VPN
  - Commands are binary+encrypted (not readable)
- Mariposa Working Group established
  - Takedown initiated Dec. 2009
  - 900+Mbps DDoS counter-attack against WG members
  - Attacker accidentally logs in w/o VPN, exposing IP
  - Spanish police given intel; arrests follow

Waledac

- First reported April 2008
- Hybrid central/proxy/P2P C&C hierarchy
  - 1024-bit RSA self-signed certificates
  - XML+bzip2+AES-128+Base64
- Microsoft *Operation b49* initiated Feb. 2010
  - First of its kind ex parte TRO to take 277 domains
  - All bots sinkholed; botnet abandoned
  - Microsoft given ownership of domains under default judgment in Oct. 2010

Bredolab

- A.k.a., Harnig (possibly)
- First reported mid-2009
- Dropper framework for installing other malware
  - Zbot (a.k.a., Zeus), SpyEye, TDSS, HareBot, Blakken (a.k.a., Black Energy 2)
  - Uses fast-flux DNS to spread infected machines across many C&C servers
- Dutch federal police take over 143 controllers on Oct. 25, 2010
  - Used infrastructure to push warning program
  - Over 100,000 followed link; 55 complaints filed
  - Infrastructure active again within months

Pushdo/Cutwail

- A.k.a., Pandex
- First reported Jan. 2007
- Advanced dropper (Pushdo) with modules (e.g., Cutwail spam module)
- No self-propagation: Loaded by frameworks like Bredolab along with other malware (e.g., Storm, Srizbi, Rustock, AntispywareXP2009)
- LLoD initiates cooperative takedown Aug. 2010
  - Acknowledged they were unlikely to succeed fully
  - Botnet back to full strength within days

Rustock

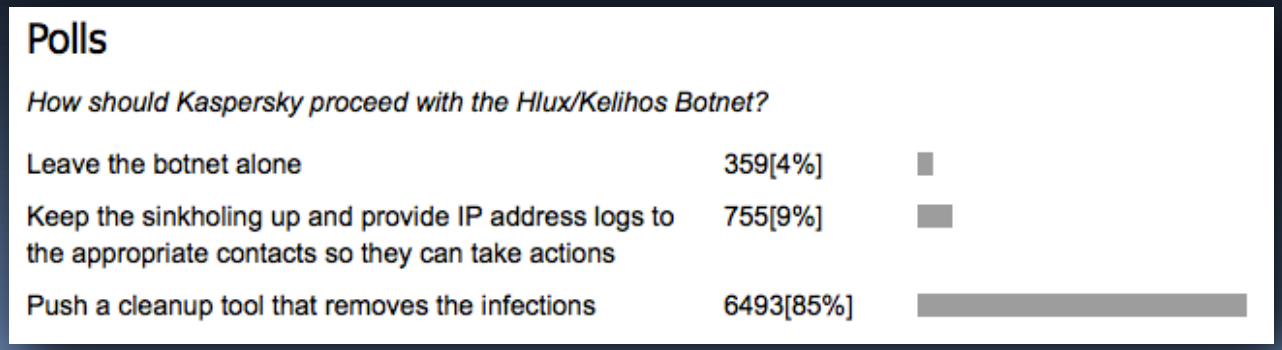
- A.k.a., Spam-Mailbot.c
- First reported early 2006
- First detailed RE reports early 2007
- Central C&C servers hosted on non-cooperative "bullet-proof" hosting companies
- Microsoft *Operation b107* on March 6, 2011
  - Involves ex parte TRO, search warrants, US Marshall assistance, taking out core servers
  - AV companies note Harnig goes down, too, due to shared infrastructure disruption

Coreflood

- First reported 2001
- Low-profile and low-aggressiveness kept botnet under industry radar
  - Researchers got cooperative ISP to provide copy of a C&C server
- April 2011, U.S. Federal court grants DoJ ex parte TRO for ISC to sinkhole bots
  - FBI allowed to issue "stop" command
  - Can clean up with "remove" command iff permission granted by system owners' signing ***Authorization to Delete Coreflood from Infected Computer(s)*** form

Kelihos

- A.k.a., Hlux, Darlev
- First reported Dec. 2010
- Re-write of Waledac
- Kaspersky Labs developed sinkhole capability, bypassing C&C protections
- Sep. 26, 2011, Microsoft *Operation b79* initiated
  - Again, ex parte TRO takes out domains
  - Kaspersky sinkholes all infected bots



Virut

- A.k.a., Virtob
- First reported 2006
- PE infector, IRC for C&C (later also HTML infection)
- Symantec ("300,000 in 24 hours")
- CERT Polska
  - Quoted in news as "860,000 in 2012"
  - Sinkhole shows ~330,000 (and slightly growing)
- Symantec reports "Waledac" dropped
  - At least third method: Conficker (2009), Fifesock (2012)
- Jan. 2013, NASK (Polish registrar)/CERT Polska, removes 43 domains
  - They sinkhole all .pl Virut domains
  - Registrars in .ru and .at notified (again), but Austria registrar refuses to remove domain without court order
  - Half of bots had DGA for .com fallback domains

Summary of Selected Takedowns

Botnet	Peak Size (est)	First Seen	Take Down	Time Elapsed	Success on 1st try	Used Legal Process
Torpig	180,000	Feb 2006	Jan 2009	3 years	No	No
Ozdok	264,784 [1]	Early 2008	Nov 2009	2 years	No	No
Mariposa	12 million [2]	May 2009	Dec 2009	7 months	No	No [3]
Waledac	6,600+ [4]	Apr 2008	Feb 2010	3 years	Yes [9]	Yes
Pushdo	1.5-2 million	Jan 2007	Aug 2010	3.5 years	No	No
Bredolab	30 million [5]	Mid-2009	Oct 2010	1.5 years	No	Yes [6]
Coreflood	378,758 [7]	2001	Apr 2011	10 years	Yes	Yes
Rustock	1.6 million [8]	2006	Mar 2011	5 years	Yes	Yes
Kelihos.A	41,000	Dec 2010	Sep 2011	8 months	Yes [9]	Yes
Kelihos.B	110,000	Jan 2012	Mar 2012	3 months	Yes [9]	No
Zeus	13 million [10]	Jul 2007	Mar 2012	5 years	Yes [11]	Yes
Virut	308,000 [12]	2006	Jan 2013	7 years	No [13]	No

Table 2: Botnets subject to highly publicized takedown efforts (by takedown date)

[1] *Unique IPs connecting to FireEye's sinkhole in 24 hrs. The 2008 estimate of 35,000 by Marshal Software [78, 81] provided no time frame or counting methodology.*

[2] *Unique IP addresses over an unspecified time period [20]. Other estimates show no more than 1.5M per day.*

[3] *The Mariposa Working Group did not use legal process in their botnet takedown attempts, but information they obtained was provided to law enforcement who eventually made arrests.*

[4] *Count of actively spamming nodes in 24 hr period.*

[5] *Count of total infections, not to be considered a single monolithic botnet of 30M computers. Also, counting method and time period used to establish count was not specified.*

[6] *Criminal procedures were used to seize control of C&C servers.*

[7] *Unique IP addresses seen over a six month period.*

[8] *Size estimated by Microsoft immediately after court-ordered takedown.*

[9] *While the botnets were abandonded, facts in [64, 96, 49] suggest the "success" is qualified.*

[10] *Total infections observed by Microsoft since 2007. Damaballa listed the largest single botnet seen in 2009 at 600,000.*

[11] *Only the Zeus activity related to a limited number of servers seized by Microsoft was affected, not all Zeus botnets (there are many more).*

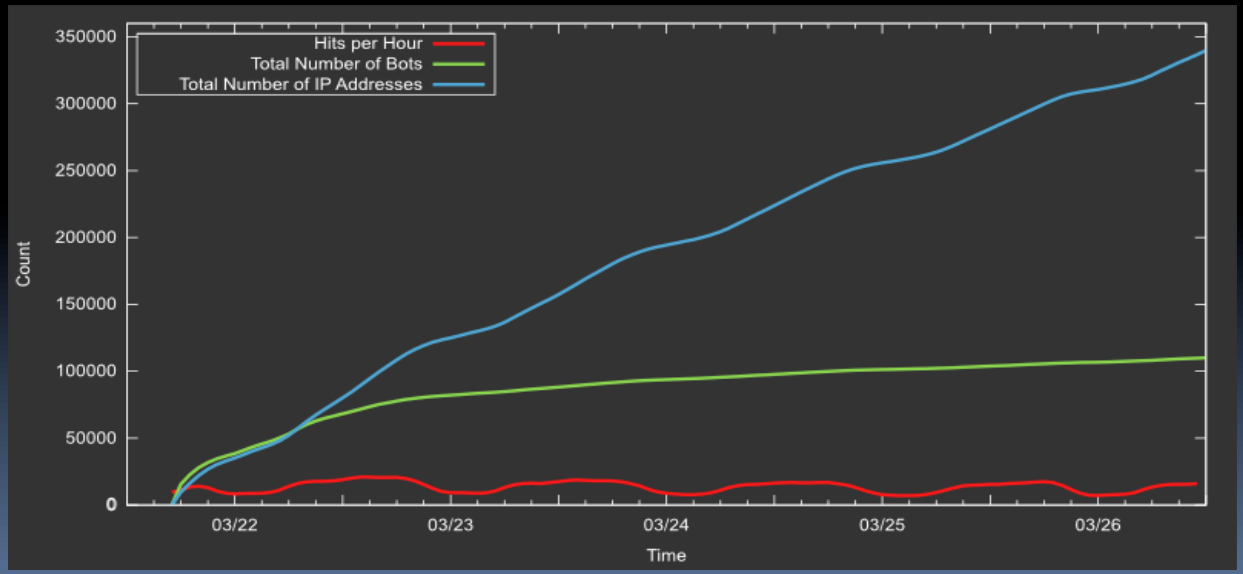
[12] *CERT Polska noted "870,000 unique IPs [50]" in all of 2012.*

[13] *All Polish domains taken out; Registrars in Austria and Russia had been notified multiple times.*

David Dittrich. So You Want to Take Over a Botnet… Unpublished manuscript, February, 2013.

Observations

- Size estimates vary by orders of magnitude
  - Incentive to inflate numbers
  - Easy to exploit IP over-counting and conflate with "infections"



Tillmann Werner. P2P Botnet Kelihos.B with 100.000 Nodes Sinkholed, March 2012. http://blog.crowdstrike.com/2012/03/p2p-botnet-kelihosb-with-100000-nodes.html

Observations (continued)

- Naming is inconsistent
- Taxonomy rarely used

Observations (continued)

- All(?) takedowns combining legal process and technical methods succeeded on first try
- (…or did they really *all fail*?)
  - Those using *only* technical means, or relying on *cooperation* of all parties involved, did not
  - It's not always about taking the botnet down
  - Today's most sophisticated botnets require this combination of **legal + technical** measures

Observations (continued)

- Mariposa takedown caused harm to innocent third parties; succeeded by luck (or risky gamble?)
- Takedowns using legal process effectively describe *ethics as by-product*
  - Defined stakeholders
  - Detailed harms/benefits
  - Likelihood
  - Intention for requested actions
  - External review (by the court)