Beyond the Range of the Moment: Ethical Response to Cybercrime

David Dittrich Katherine Carpenter

NANOG 63 | San Antonio, TX | 3 Feb 2015

This material includes research sponsored by the Department of Homeland Security (DHS) Science and Technology Directorate, Homeland Security Advanced Research Projects Agency, Cyber Security Division (DHS S&T/ HSARPA/CSD), BAA 11-01 and Air Force Research Laboratory, Information Directorate under agreement number FA8750-12-2-0329. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of Department of Homeland Security, Air Force Research Laboratory or the U.S. Government.

Objectives

- Enlist the community in defining the parameters for effective and safe counter-criminal actions
- Produce a healthy and open debate of all aspects of previous botnet takedown actions
- Elicit comments from NANOG members about interacting with an advisory body helping guide risky network operations before & after action

ACTING ON THE *RANGE OF THE MOMENT*

"a lot of people … are frustrated and angry and they want to kick some bad-guy ass. that in itself is great, unless it leads us to range-of-the-moment thought and action, such as taking down botnets. can we uplevel this discussion -- talk about strategic teamwork that would have a lasting impact on bad-guy profits?"

Paul Vixie

FRUSTRATION AND LOATHING

"We will continue to fight the threat of botnets and the criminals behind them," says Davis. "We'll start by dismantling their infrastructure and won't stop until they're standing in front of a judge."
Chris Davis, CEO for Defence Intelligence (re: Mariposa Botnet)
http://security.ulitzer.com/node/1305941

- "Law enforcement is not doing their job."
- "I found a cache of stolen documents and reported it to LE. It's been months and nothing has happened and they haven't told me anything."
- "What's the result of most botnet takedowns? The botnets are mostly still up and running and not a single person is in jail."

Domestic Justice Systems

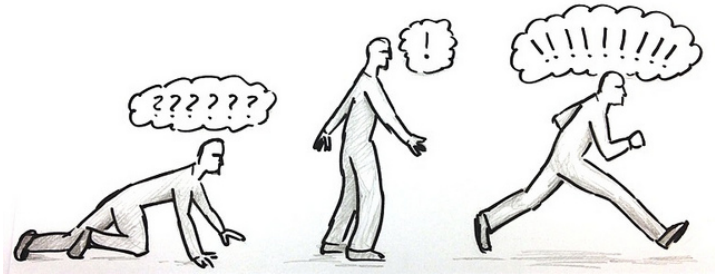
- Civil and/or Criminal Process
- Codified Law vs. Common Law
- Justice is a "deliberative" process
  - Constitutional protections
  - The Grand Jury
  - MLAT system for trans-national criminal investigations

Discrimination, collateral harm

Active Response Continuum

First Agora workshop (June 8, 2001)

3 more, funded by Cisco, through 2004



http://www.flickr.com/photos/69839732@N08/8010796716/

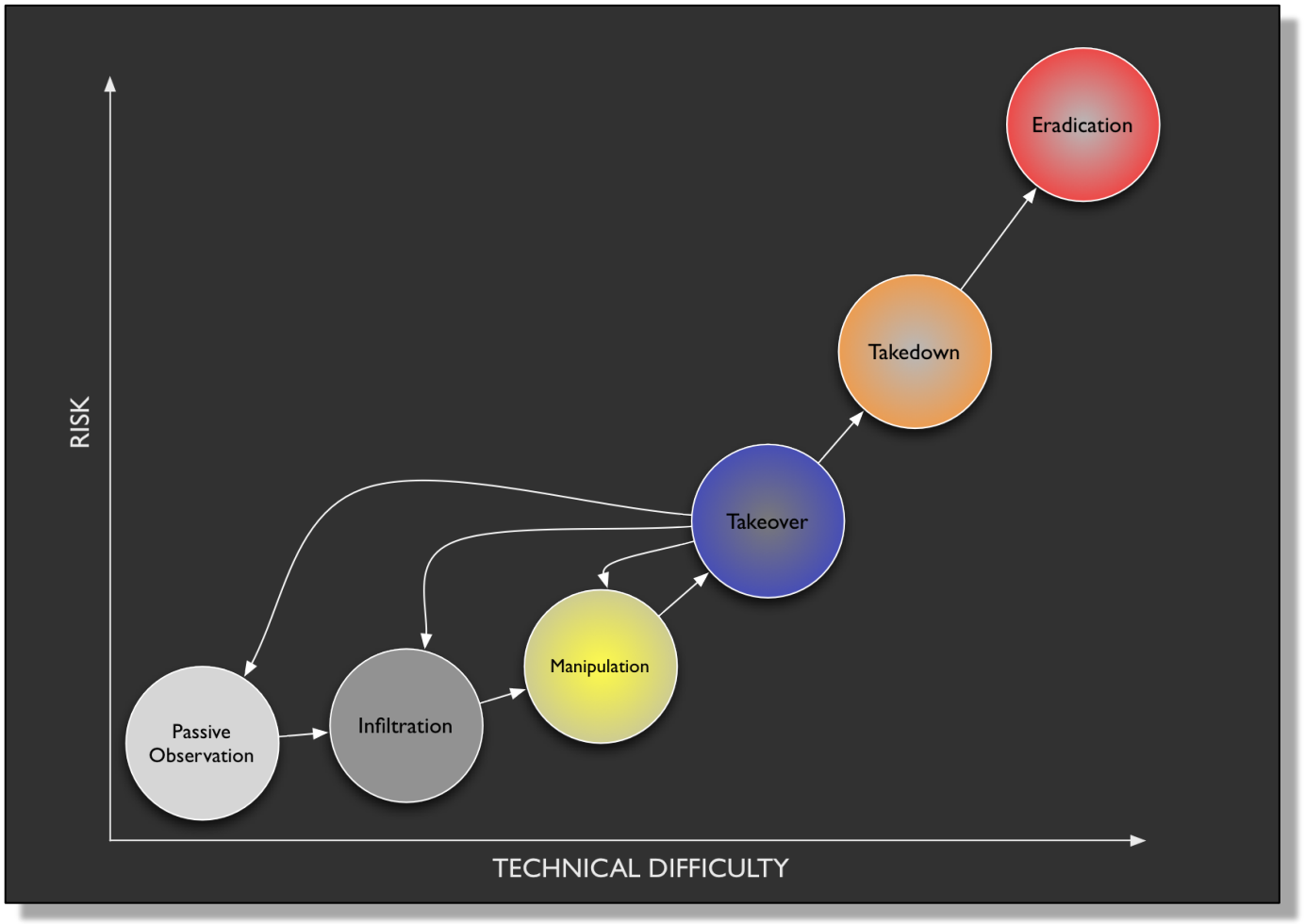
Level	Actor's Posture	Characteristic Actions
4	Non-cooperative	Intelligence collection, tracebacks, cease & desist, *takedown/takeover*, retaliatory counterstrike
3	Cooperative	Joint traceback, collaboration, sharing
2	Interactive	Modify own systems in response to attack
1	Involved	Uses AV, simple firewalls,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

Level 4 of the Active Response Continuum

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

Involves things ***outside your sphere of authority***, ***without cooperation*** of their owners/operators

Levels of Action



ETHICS AND THE PRIVATE SECTOR

EXHIBITING INTEGRITY

- *"Integrity, as I define it…"**
  1. *Able to discern right from wrong*
  2. *Acting on what you have discerned, even at personal cost*
  3. *Saying openly that you are acting on your understanding of right from wrong*

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

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

Virtuous Choice

- 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.

Reflect Ethics

- What is [your] intent in [your proposed action]?
- Who is the stakeholder being served?
- How would this stakeholder view my actions and interpret my intent?
- Would they feel grateful, neutral or resentful?

"When engaged [in] `world-fixing,' one needs to `[derive their methods] through constant, critical reflection on the goals of research and the research questions,' understanding not only the problems to be solved, but the potential effects on all parties involved." - Annette Markham

A. Markham. Method as Ethic, Ethic as Method: A Case for Reflexivity in Qualitative ICT Research. Journal of Information Ethics, 15(2):37–55, 2006.

DHS S&T AND THE MENLO REPORT

- DHS Working Group on Ethics in ICTR
  - Inaugural mtg - May 26th-27th, 2009, Washington, DC
  - Lawyers, Computer Scientists, IRB Members, Ethicists
- Report published in Federal Register, Dec. 2011
  - Revision based on comments delivered May 2012
  - "Companion to the Menlo Report" published in 2012

Belmont Principle	Menlo Application
Respect for Persons	➢Identify stakeholders ➢Informed consent
Beneficence	➢Identify potential benefits and harms ➢Balance risks and benefits ➢Mitigate realized harms
Justice	➢Fairness and equity
Additional Menlo Principle: Respect for the Law and Public Interest	➢Compliance ➢Transparency and accountability

STAKEHOLDER ANALYSIS

- **Primary** Stakeholders

  "Those ultimately affected [either positively or negatively]"

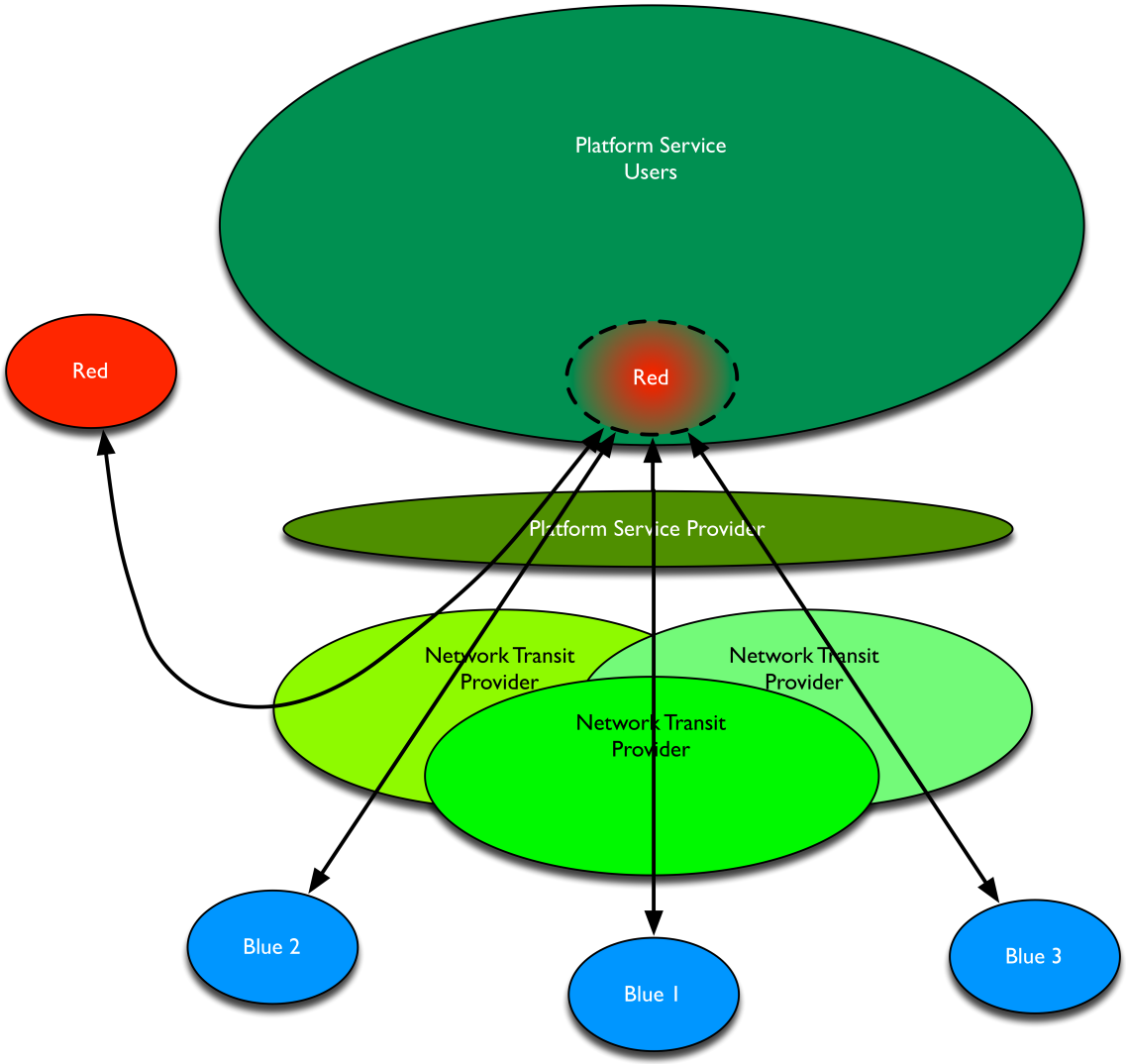
- **Secondary** Stakeholders

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

- **Key** Stakeholders

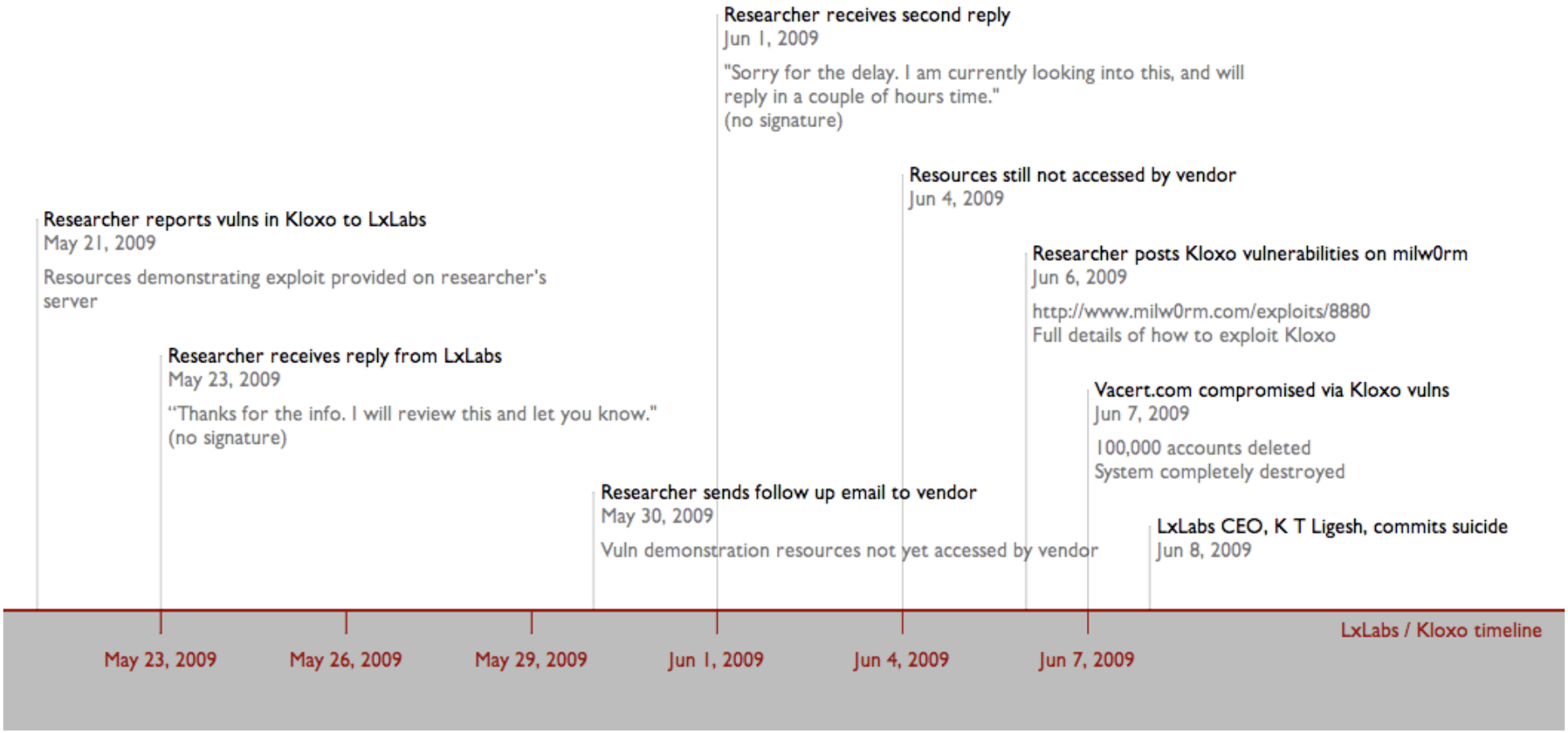
  "Those who can significantly influence, or are important to the success [or failure] of the project"

Relationships and “Distance”



CASE STUDY: HYPERVM/KLOXO (2009)

Timeline of events



Stakeholders

Entity	Activity	Type	Risk/Benefit
Researcher	Discovered vulnerabilities	Key	Reputation, altruism, personal safety
Programmers	Write and maintain software	Key	Jobs
Vendor	Control programmers' activities	Key	Reputation, lost revenue
Svc. Providers	Customers of vendor; provide service to clients	Secondary	Lost revenue
Clients	Create/run virtual storefronts	Primary	Lost revenue
Customers	Buy from online stores	Primary	DoS, fraud
Criminals and attackers	Exploit services	Key	Booty, LOLZ, Arrest

CASE STUDY: KELIHOS TAKEDOWN (2012)

Raise the Costs of the Attacker

ACTIVE DEFENSE

What is Active Defense?

Passive Security vs. Active Defense

Determined attackers will go to almost any level of expense, time, and effort to penetrate a victim's network. The traditional passive defense security model that focuses on castle-building and development of better detection systems is failing. The only option this strategy offers organizations is continuously escalating spending on additional passive defensive measures that do nothing more than slightly delay the inevitable compromise by a targeted attacker. Meanwhile, adversaries are able to overcome these passive countermeasures at a fraction of the cost.

The reality is that existing security solutions focus merely on improving detection rates and attempting to swat away adversary intrusions and do not fundamentally raise the cost and risk to the attackers. Basic statistics tells us that even if these solutions are able to achieve a rate of 99% effectiveness, all that means is that a persistent attacker has to attempt to compromise the network just 250 times before he has an over 90% chance of success (Aside Statistics 101 refresher: $1 - 0.99^{250} = 91.9\%$ chance of success).

The time has come for us to adopt an Active Defense strategy that instead focuses on raising costs and risks to the adversary and attempts to deter their activities.

Achieving the Desired Outcome

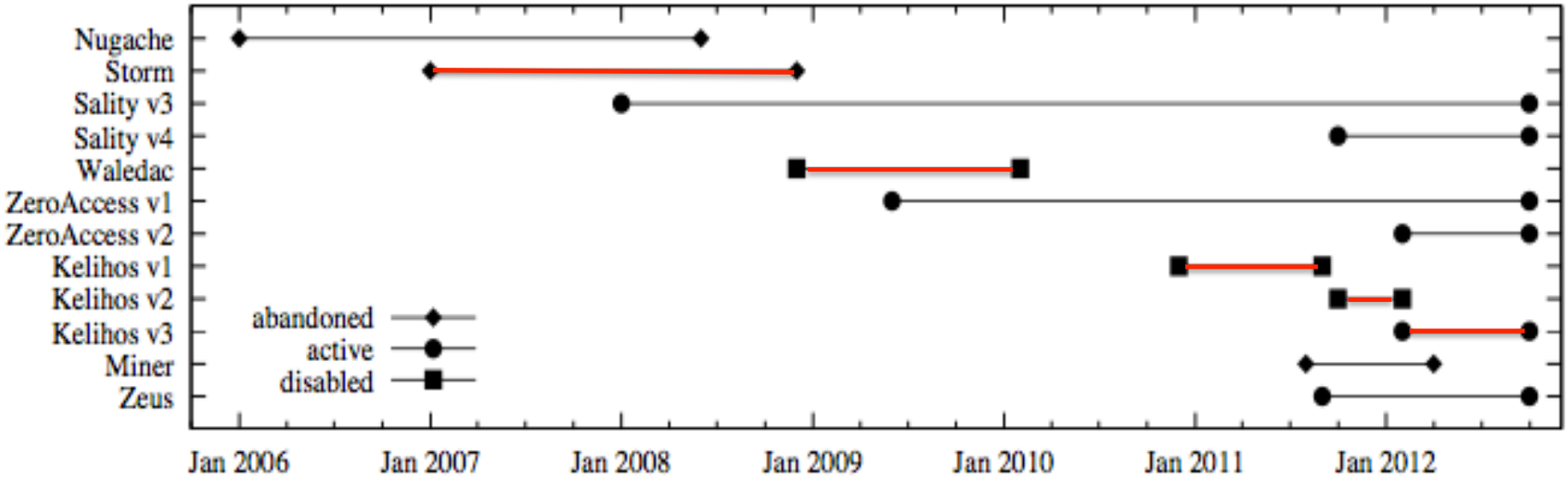


Figure 2: Lifespans of P2P botnet variants.

Back of the Envelope

How much does it cost to buy 10,000 U.S.-based malware-infected hosts?

Posted on February 28, 2013 by ddanchev

5 Votes

By Dancho Danchev

Earlier this month, we profiled and exposed **a newly launched underground service offering access to tens of thousands of malware-infected hosts**, with an emphasis on the fact that U.S.-based hosts were relatively more expensive to acquire, largely due to the fact that U.S.-based users are known to have a higher online purchasing power. How much does it cost to buy 10,000 U.S.-based malware-infected hosts? Let's find out.

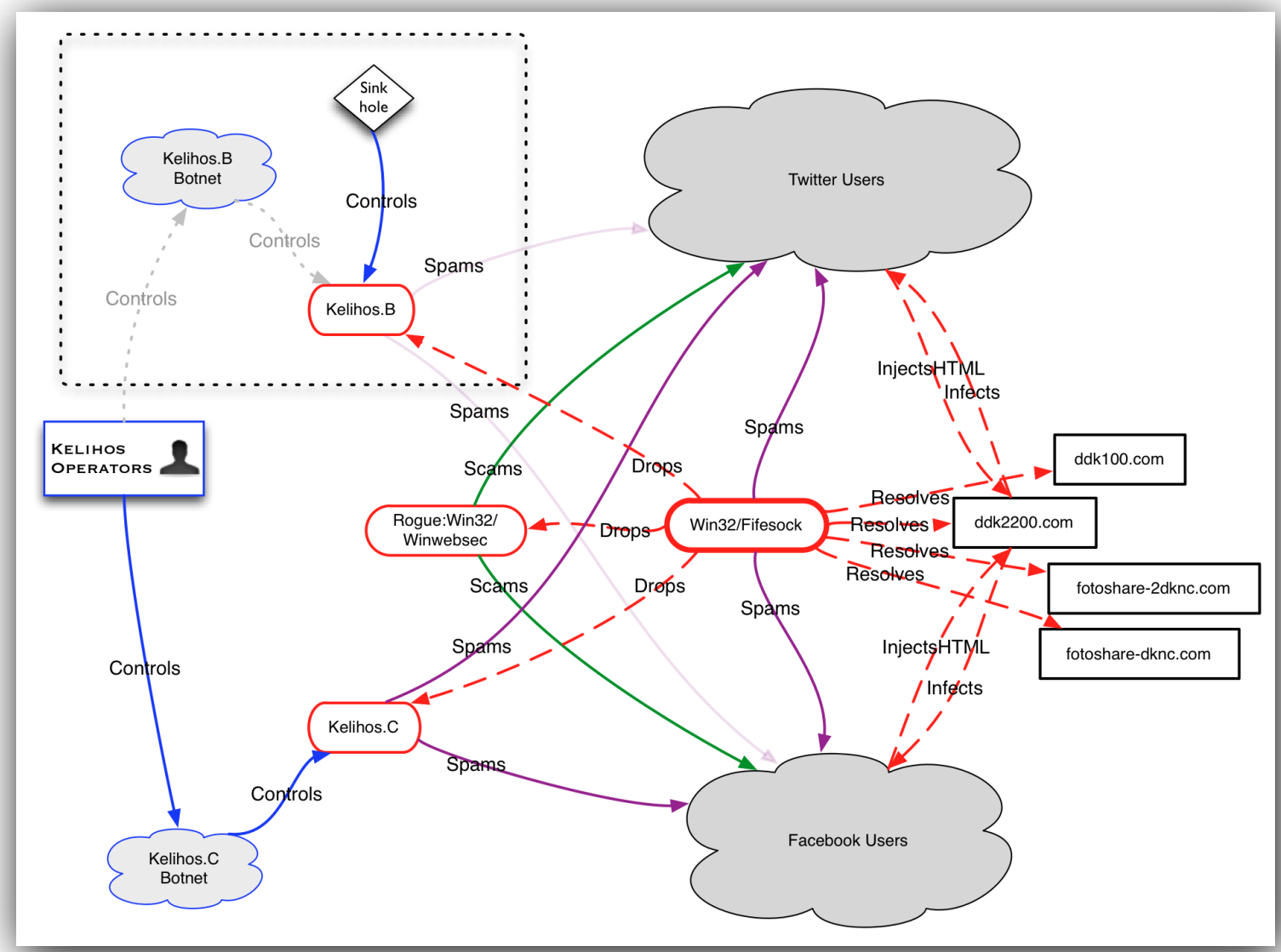
Cost to *replace* Kelihos in 24 hours

Bots	Rate	Cost
110,000	$200/10K	$2,200
110,000	$400/10K	$4,400
110,000	$1K/10K	$11,000

Comparative cost to *initiate* sinkhole

Hours	Rate	Cost
37	$300/hr	$11,000
73	$150/hr	$11,000
110	$100/hr	$11,000

Roles & Relationships



ELEMENTS OF A VIABLE FRAMEWORK FOR ARC

Attributes of a Viable (Ethical) Framework

- Should handle deconfliction (in more than the military sense)
- Should provide before- and after-action review
- Should favor government over private sector action at the extreme end of the ARC
- Should favor civil/criminal process over extrajudicial private sector action
- Should follow virtue ethics (Integrity + "Right Action" justification)

How do NANOG members fit in?

- How should your organization be involved?
  - Active, or secondary?
- What influence does your organization have in terms of botnet mitigation operations?
- What limits your organization's ability to be actively involved?
- How should your organization express its concerns in botnet mitigation operations?

CONTACT

- Dave Dittrich
  University of Washington
  dittrich @ uw.edu
  https://staff.washington.edu/dittrich/

- Katherine Carpenter
  carpenter.katherinej @ gmail.com

Questions? Discussion…

References

- Active Response Continuum
  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
- Levels of Action
  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
- DHS "Menlo Report"
  D. Dittrich and E. Kenneally (editors). The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research, December 2012. http://www.cyber.st.dhs.gov/wp-content/uploads/2012/09/MenloPrinciplesCORE-20120803.pdf
- Achieving the desire outcome
  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
- Relationships and "Distance"
  Adapted from: Katherine Carpenter and David Dittrich. Bridging the Distance: Removing the Technology Buffer and Seeking Consistent Ethical Analysis in Computer Security Research. In 1st International Digital Ethics Symposium. Loyola University Chicago Center for Digital Ethics and Policy, October 2011. http://staff.washington.edu/dittrich/papers/loyola-2011/
- Stakeholder analysis
  D. Dittrich. FAQ on Kelihos.B/Hlux.B sinkholing, March 2012. http://www.honeynet.org/node/836
  Dittrich, Leder, and 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.
  Dittrich, Bailey, and Dietrich. Towards Community Standards for Ethical Behavior in Computer Security Research. Stevens CS Technical Report 2009-1, 20 April 2009
  Dittrich, Bailey, and Dietrich. Have we Crossed the Line? The Growing Ethical Debate in Modern Computer Security Research. In (Poster at) Proceedings of the 16th ACM Conference on Computer and Communication Security (CCS '09), Chicago, Illinois USA, November 2009

KELIHOS SINKHOLE FAQ

The Honeynet Project

Home › Blogs › david.dittrich's blog

Navigation

- About us
- Blogs
  - Honeynet Project Blog
- Funding/Donations
- Challenges
- Chapters
- Papers
- Projects
- Code of Conduct
- Google SoC 2009

FAQ on Kelihos.B/Hlux.B sinkholing

Sun, 04/01/2012 - 23:26 — david.dittrich

On March 31, 2012, the Honeynet Project published a draft Code of Conduct and a statement about Ethics in Computer Security Research: Kelihos.B/Hlux.B botnet takedown.

The initial draft of the Code of Conduct was drawn from concepts described in the The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research that was published in the United States Federal Register on December 28, 2011 for public comment. The Code of Conduct was refined through discussion within the Legal and Ethics Committee and volunteer Honeynet Project members to help make it workable within the structure of the Honeynet Project membership for evaluating the ethics of future research activities.

The following FAQ reflects how the Menlo Report principles and proposed Honeynet Project Code of Conduct can be used to analyze and explain an action like the Kelihos/Hlux sinkholing operation.

KELIHOS SINKHOLE FAQ

Question: Who are all the stakeholders involved in the Kelihos.B/Hlux.B botnet?
Answer: The set of stakeholders can be divided up into three categories based on: (1) their ability to directly affect the botnet operation (for good or bad), (2) their involvement in delivery of services affected by the botnet (for good or bad), and (3) the end-users and individuals in society who are generally impacted by the botnet operation (for good or bad).

Those (key) stakeholders who have an directly affecting role:

- The Honeynet Project in general, and those researchers in specific who have been reverse engineering this malware.
- The organizations involved in the sinkholing (Kaspersky, CrowdStrike, Dell SecureWorks)
- The individual or group who is operating the botnet.
- Law enforcement who may be investigating crime and who learn how to investigate crime through reading our research publications.

Those (secondary) stakeholders who are involved as intermediaries:

- The owners/providers of hosts being used for the top-level C&C infrastructure.
- The owners/providers of network services that are receiving spam emails.
- Malware distribution ("pay per install" or dropper) services used to spread the bot.

Those (primary) stakeholders/end-users who are affected:

- People whose computers are infected with the malware and anyone using or relying upon those computers.
- Those individuals who recieve spam emails and/or are defrauded by spam selling fake drugs, etc.
- Any persons who benefit from computer crime activity (e.g., spammers, people purchasing/using stolen credit cards or Bitcoin wallets for financial fraud, etc.)
- The general public, who reads our research papers and blog posts.

Kelihos

SECURITY dark READING
Protect The Business Enable Access

It's (Already) Baaack: Kelihos Botnet Rebounds With New Variant

Botnet hunters debate whether Kelihos/Hlux operators can reclaim rescued bots

By Kelly Jackson Higgins, Dark Reading
March 29, 2012
URL: http://www.darkreading.com/attacks-breaches/its-already-baaack-kelihos-botnet-reboun/232700540

Less than one day after botnet hunters announced they had crippled the Kelihos.B/Hlux.B botnet, a new version of the tenacious botnet is now back up and running today.

Researchers at Seculert were the first to point out the Kelihos/Hlux botnet was in action: Aviv Raff, co-founder and CTO at Seculert, late yesterday confirmed that his firm had seen the botnet spreading via a Facebook worm despite the announcement yesterday by Kaspersky, CrowdStrike, Dell SecureWorks, and The Honeynet Project that they had knocked the botnet offline. Raff says there's still communication under way via its command-and-control (C&C) servers.

"We still see infected Kelihos.B machines, even new ones, sending spam and communicating with the C&C server," Seculert's Raff says.

But researchers from Kaspersky Lab, CrowdStrike, Fortinet, and Unveillance contend that this is a *new* variant of Kelihos/Hlux, not the same botnet that was taken down over the past few days. That one, KelihosB/HluxB -- which was built for spamming, information-stealing, DDoSing, as well as for pilfering Bitcoins and electronic wallets -- was sunk when the team poisoned it with their own code in order to redirect some 110,000 bots to their sinkhole server and away from the operator's control. It was about three times as large as the first Hlux/Kelihos botnet, which was crippled last fall by a team led by Microsoft and that included Kaspersky.