The Legal and Ethical Challenges With Aggressive Computer Security Research and Operations Actions

David Dittrich Katherine Carpenter

DCC 2014 Singapore, March 4, 2014

AGENDA

- Why we are speaking to you today
- Legal Issues
- Ethical Issues (and The Menlo Report)
- Case studies
- Conclusions

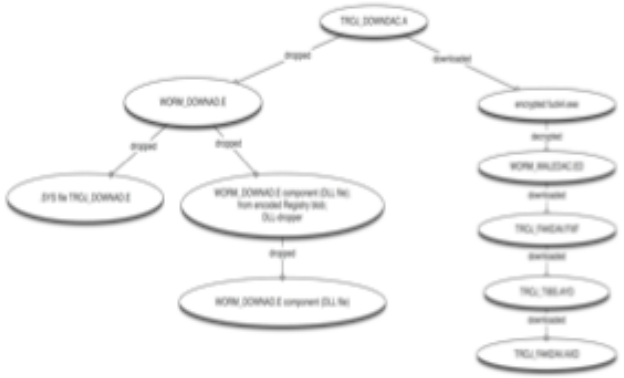
FRUSTRATION AND LOATHING

"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."

We *must* take risks

- Understanding fraud (e.g., spam and phishing)
- Bots that are vetted ("made bot")
- New techniques/tactics seen daily
- LE *investigates* and SecOps *mitigate*; they don't do R&D
- Sophisticated malware *frameworks* tomorrow's biggest threat



SINKHOLE AS A SERVICE?

SECURELIST

FAQ: Disabling the new Hlux/Kelihos Botnet

Stefan Ortloff
Kaspersky Lab Expert
Posted March 28, 14:23 GMT
Tags: Botnets

0.2

Q: What is the Hlux/Kelihos botnet?
A: Kelihos is Microsoft's name for what Kaspersky calls Hlux. Hlux is a peer-to-peer botnet with an architecture similar to the one used for the Waledac botnet. It consists of layers of different kinds of nodes: controllers, routers and workers.

…OR AS SLIPPERY SLOPE?

Q: The bots of both botnets are now sinkholed to machines of your control. What now?
A: This is actually the main question we asked in the first take-down back in September 2011. Obviously we cannot sinkhole Hlux forever. The current measures are a temporary solution, but they do not ultimately solve the problem, because the only real solution would be a cleanup of the infected machines. We expect that over time, the number of machines hitting our sinkhole will slowly decrease as computers get cleaned and reinstalled.

Apart from this, there is one other theoretical option to ultimately get rid of Hlux: We know how the bot's update process works. We could use this knowledge and issue our own update that removes the infections and terminates itself. However, this would be illegal in most countries.

The only permanent solution is advocating to politicians for more international legislation and laws to be passed for more involvement between cyber security professionals and federal law-enforcement agencies. Sinkholing is a temporary solution but finding the groups behind the botnets and allowing law enforcement to apprehend them is the only permanent solution to the problem. New regulations will give more jurisdiction to execute the following countermeasures:

- Carrying out mass remediation via a botnet
- Using the expertise and research of private companies, providing them with warrants for immunity against cybercrime laws in particular investigation
- Using the resources of any compromised system during an investigation
- Obtaining a warrant for remote system exploitation when no other alternative is available

After the taking down the old Hlux we asked your readers on securelist.com how Kaspersky should proceed with the botnet: The answer was quite clear: Only 4% voted for "Leave the botnet alone.". 9% agreed with "Keep the sinkholing up and provide IP address logs to the appropriate contacts so they can take actions." and 85% voted for "Push a cleanup tool that removes the infections.". In this poll 8539 votes were counted.

Credible Risk?

"A graduate of Justice's computer crime section once shut down a discussion on this topic by saying, 'What if you followed the hacker back to a hospital network, and in trying to catch him you shut down computers in the intensive care unit? That's a felony murder rap.'"

Stewart Baker. Is network offense the best network defense?, June 2012. http://www.volokh.com/2012/06/17/is-network-offense-the-best-network-defense/

See also Himma (2004) ("For example, a set of zombies network could ... have the direct effect of impairing the performance of the life-support system and hence could result in death of any number of innocent bystanders"). If such argument is correct, would driving a car be morally wrong because of a remote probability that the driver can fatally hit somebody?

J. Kesan and R. Majuca. Hacking Back: The Optimal Use of Self-Defense in Cyberspace, March 2009. Chicago-Kent Law Review, Vol. 84, No. 3, 2010; Illinois Public Law Research Paper No. 08-20. Available at SSRN: http://ssrn.com/abstract=1363932

Although we could have sent a blank configuration file to potentially remove the web sites currently targeted by Torpig, we did not do so to avoid unforeseen consequences (e.g., changing the behavior of the malware on critical computer systems, such as a server in a hospital).

B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna. Your Botnet is My Botnet: Analysis of a Botnet Takeover. Technical report, University of California, May 2009.

Credible Risk.

California Man Pleads Guilty in "Botnet" Attack That Impacted Seattle Hospital and Defense Department (May 4, 2006)

May 4, 2006
U.S. Department of Justice
Western District of Washington
United States Attorney's Office
Emily Langlie, Public Affairs Officer
Contact Information: (206) 553-4110

California Man Pleads Guilty in "Botnet" Attack That Impacted Seattle Hospital and Defense Department

CHRISTOPHER MAXWELL, 20, of Vacaville, California, pleaded guilty in U. S. District Court in Seattle today to Conspiracy to Intentionally cause Damage to a Protected Computer and to Commit Computer Fraud, and Intentionally Causing or Intending to Cause Damage to a Protected Computer. MAXWELL's creation of what is called a "botnet" led to computer malfunctions at Seattle's Northwest Hospital in January, 2005. Further investigation revealed MAXWELL's computer intrusions also did more than $135,000 of damage to military computers in the United States and overseas.

http://www.justice.gov/criminal/cybercrime/press-releases/2006/maxwellPlea.htm

Credible Risk.

According to court filings, as the botnet searched for additional computers to compromise, it infected the computer network at Northwest Hospital in north Seattle. The increase in computer traffic as the botnet scanned the system interrupted normal hospital computer communications. These disruptions affected the hospital's systems in numerous ways: doors to the operating rooms did not open, pagers did not work and computers in the intensive care unit shut down. By going to back up systems the hospital was able to avoid any compromise in the level of patient care.

Credible Risk.

Conficker infected critical hospital equipment, expert says

Hundreds of PCs and medical devices at hospitals in the U.S. were found to be infected with the Conficker worm recently, a security expert says.

by **Elinor Mills** | April 23, 2009 4:23 PM PDT

Updated 7:50 a.m. PDT April 24 to specify that the infection was in the U.S.

SAN FRANCISCO--The **Conficker [http://news.cnet.com/conficker-virus/]** worm infected several hundred machines and critical medical equipment in an undisclosed number of U.S. hospitals recently, a security expert said on Thursday in a panel at the RSA security conference.

"It was not widespread, but it raises the awareness of what we would do if there were millions" of computers infected at hospitals or in critical infrastructure locations, Marcus Sachs told CNET News after the session. Sachs is the director of the SANS Internet Storm Center and a former White House cybersecurity official.

It is unclear how the devices, which control things like heart monitors and MRI machines, and the PCs got infected, he said. The computers are older machines running Windows NT and Windows 2000 in a local area network that was not supposed to have access to the Internet, however, the network was connected to one that has direct Internet access and so they were infected, he said.

http://news.cnet.com/8301-1009_3-10226448-83.html

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
- Experiment with an advisory body to evaluate risky CS operations before and after action

THE LEGAL ISSUES

The Justice *System*

- Civil and/or Criminal Process
- Regulation (e.g., CFR in the USA)
- Code Law vs. Common Law
- Justice is a "deliberative" process
  - Innocent until proven guilty
  - Constitutional protections (Bill of Rights)
  - The Grand Jury
  - MLAT system for trans-national criminal investigations

International Law

- Sovereigns
  - "Law of War"
  - International humanitarian law
  - Treaties and Conventions
- Civilians
  - Extradition and Dual-criminality

Conflicts

- Civil action vs. Criminal action
- Interference with a criminal investigation
- Collecting + selling victim information vs. reporting to LE + cooperative mitigation
  - Misprision of a Felony? (18 U.S.C. § 4)

> "Whoever, having knowledge of the actual commission of a felony cognizable by a court of the United States, conceals and does not as soon as possible make known the same to some judge or other person in civil or military authority under the United States, shall be fined under this title or imprisoned not more than three years, or both."

Last line of defense?

COMPUTERWORLD

Print Article Close Window

Reverse hacker wins $4.3M in suit against Sandia Labs

Shawn Carpenter used his own hacking techniques to probe outside breach

Jaikumar Vijayan

February 14, 2007 (Computerworld)

Shawn Carpenter, a network security analyst at Sandia National Laboratories who was fired in January 2005 for his independent probe of a network security breach at the agency, has been awarded $4.3 million by a New Mexico jury for wrongful termination.

In announcing its decision yesterday, the jury also awarded Carpenter $350,000 for emotional distress and more than $36,000 for lost wages, benefits and other costs.

A spokesman from Sandia expressed "disappointment" with the verdict and said the lab will consider whether to appeal it or not.

The highly publicized case involved Carpenter's investigation of a network break-in at Sandia in 2003.

After initially telling superiors about the incident, Carpenter launched an independent, months-long investigation during which he used hacking techniques of his own to eventually trace the attacks back to a Chinese cyberespionage group. The group, called Titan Rain by federal authorities, was believed responsible for carrying out similar attacks against a large number of U.S. government, military and commercial interests.

Carpenter shared information from his investigation, initially with individuals at the Army Counterintelligence Group and later with the FBI.

When Sandia officials learned of the investigation and of his sharing information with the FBI and other outside agencies, they terminated him for inappropriate use of confidential information that he had gathered in his role as a network security manager for the laboratory.

Yesterday's verdict is a "vindication of his decision to do the right thing and turn over the information he obtained to the proper federal authorities in the interests of national security," said Philip Davis, one of the attorneys who represented Carpenter in his lawsuit.

The verdict highlights "the jury's belief that Shawn Carpenter is a patriot and did what he did to protect the national interest," Davis said. "That was more important than Sandia's own interest in taking care of itself."

THE ETHICAL ISSUES

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

Reflect Ethics

"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."

- 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?

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.

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
  - "Companion to the Menlo Report" nearing completion
  - Engaging Industry, other USG, IRB community, …

THE MENLO REPORT

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

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

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"

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

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.

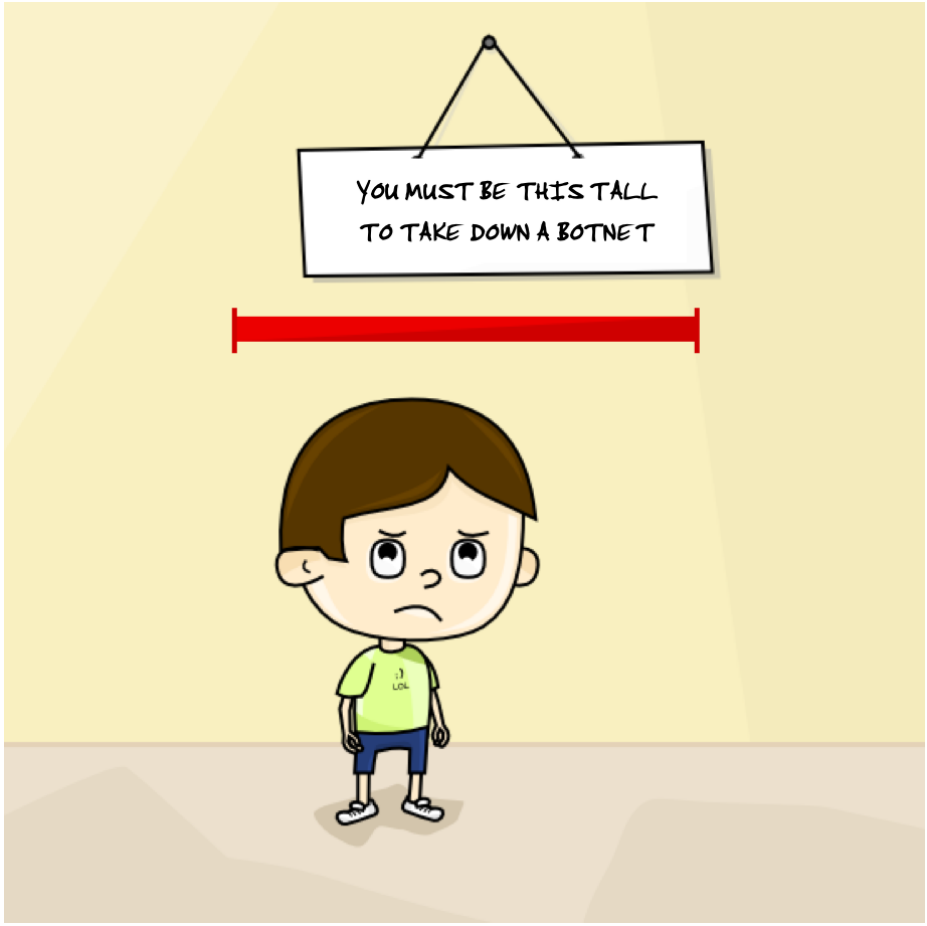
Those (secondary) stakeholders who are involved as intermediaries:

- 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.

Anatomy of a "Successful" Takedown?



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

KELIHOS (HLUX) "B" SINKHOLE

- March 21, 2012
- Dell SecureWorks, CrowdStrike, Kaspersky, and the Honeynet Project
  - Kelihos.B/Hlux.B botnet takedown

    http://honeynet.org/node/833
  - Statement about Ethics in Computer Security Research: Kelihos.B/Hlux.B botnet takedown https://honeynet.org/node/834
  - FAQ on Kelihos .B/Hlux sinkholing http://www.honeynet.org/node/836

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

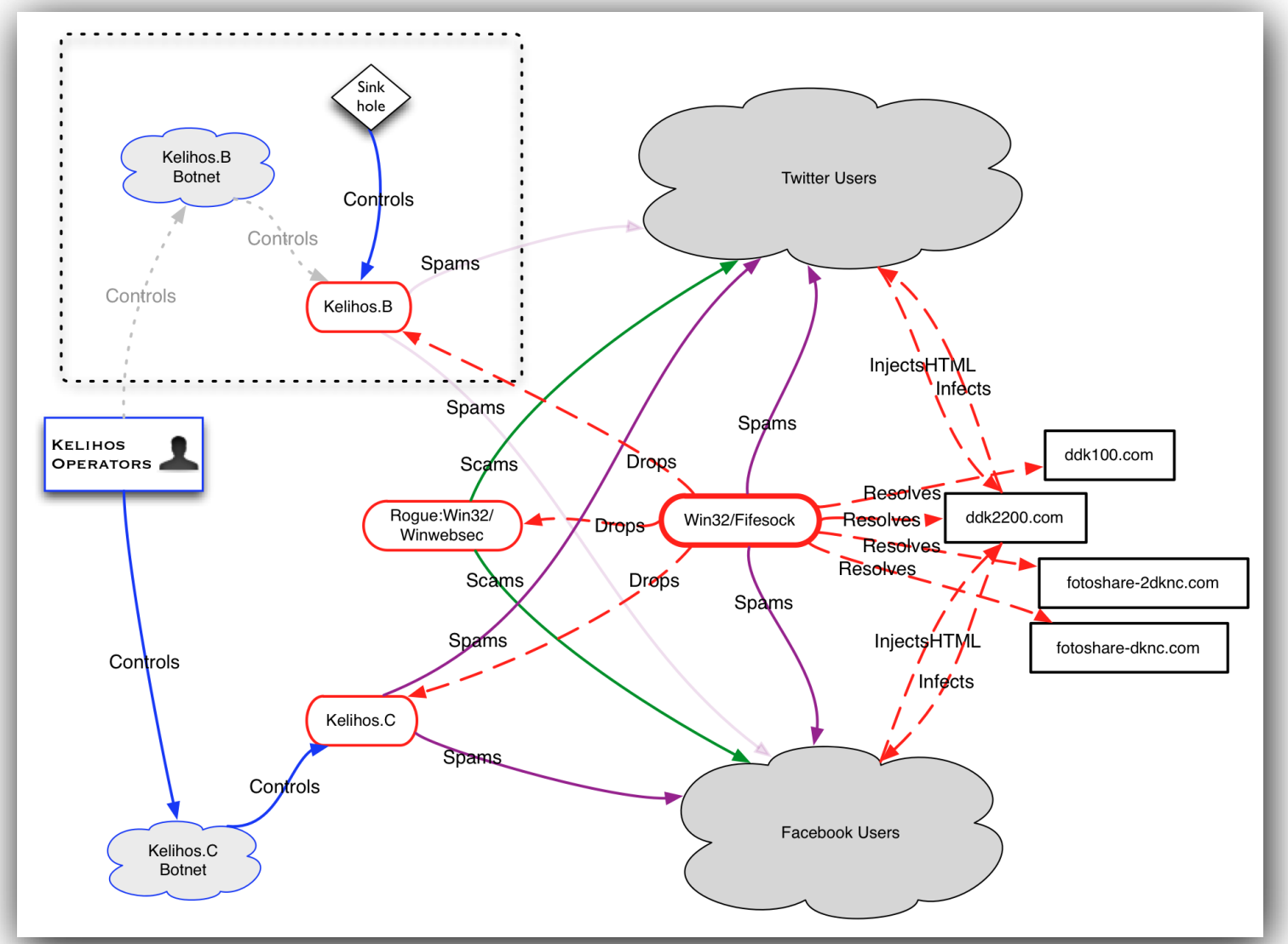
Less than one day after botnet hunters announced they had crippled the Kelihos.B/Hlux.B botnet, a new version of the tenacious botnet is now back up and running today.

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.

Roles & Relationships



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.

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.

Back of the Envelope

The prices are as follows:

- 1,000 hosts World Mix go for $25, 5,000 hosts World Mix go for $110, and 10,000 hosts World Mix go for $200
- 1,000 hosts EU Mix go for $50, 5,000 hosts EU Mix go for $225, and 10,000 hosts EU Mix go for $400
- 1,000 hosts DE, CA and GB, go for $80, 5,000 hosts go for $350, and 10,000 hosts go for $600
- Naturally, access to a U.S.-based host is more expensive compared to the rest of the world. A 1,000 U.S. hosts go for $120, 5,000 U.S. hosts go for $550 and 10,000 U.S hosts go for $1,000

Cost to replace Kelihos in 24 hours

Bots	Rate	Cost
108,000	$200/10K	$2,160
108,000	$400/10K	$4,320
108,000	$1K/10K	$10,800

Comparative cost to *initiate* sinkhole

Hours	Rate	Cost
36	$300/hr	$10,800
72	$150/hr	$10,800
108	$100/hr	$10,800

CASE STUDIES AND OBSERVATIONS

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

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

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
  - Intel given to Spanish police; arrests follow in Spain, Slovenia

Mariposa

- Update (2014)

BBC NEWS

TECHNOLOGY

24 December 2013 Last updated at 06:25 ET

Mariposa botnet 'mastermind' jailed in Slovenia

A hacker accused of masterminding one of the biggest ever botnets has been sentenced to just under 5 years in jail.

Matjaz Skorjanc was arrested in 2010 after a two-year investigation into malware that had hijacked about 12.7 million computers around the world.

The 27-year-old was found guilty of creating the Mariposa botnet software, assisting others in "wrongdoings" and money laundering.

His lawyer said he would appeal.

In addition to the 58-month jail term, Skorjanc was also ordered to pay a 4,000 euro ($4,100; £2,510) fine and give up a flat and car he was alleged to have bought with money he had received from a Spanish criminal syndicate.

28 July 2010 Last updated at 05:14 ET

182 Share

Botnet hacker caught in Slovenia

A computer hacker known as Iserdo has been arrested in Slovenia.

The 23-year-old is believed to have written the program behind the mariposa virus, also known as butterfly.

The botnet, one of the world's largest, was dismantled earlier this year after infecting 12.7 million computers.

The FBI described the capture of Iserdo as a "huge break" in the ongoing Mariposa investigation.

It was designed to steal personal financial details and was also found in the PCs of banks and major companies. Officials from around the world have been chasing the cyber criminals.

In December 2009, three people believed to have been running it were arrested in Spain.

"To use an analogy here, as opposed to arresting the guy who broke into your home, we've arrested the guy that gave him the crowbar, the map and the best houses in the neighbourhood," Jeffrey Troy, deputy assistant director for the FBI cyber division told Associated Press.

Related Stories

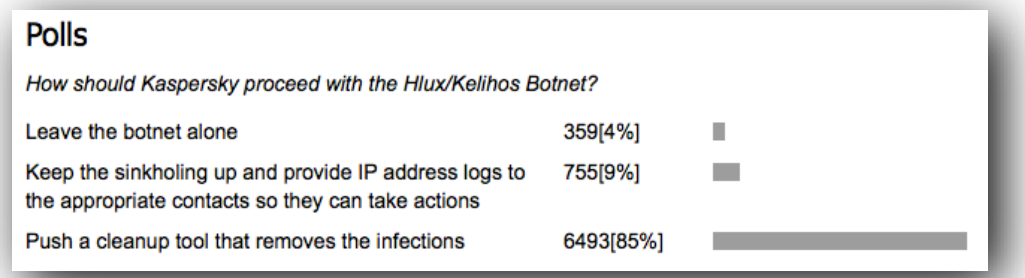
- Breaking the butterfly botnet
- Spanish police smash huge botnet
- Police computers struck by virus

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

Kelihos

- A.k.a., Hlux, Darlev, Waledac, Trojan Nap
- 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
- Sinkholed again in 2012 & 2013



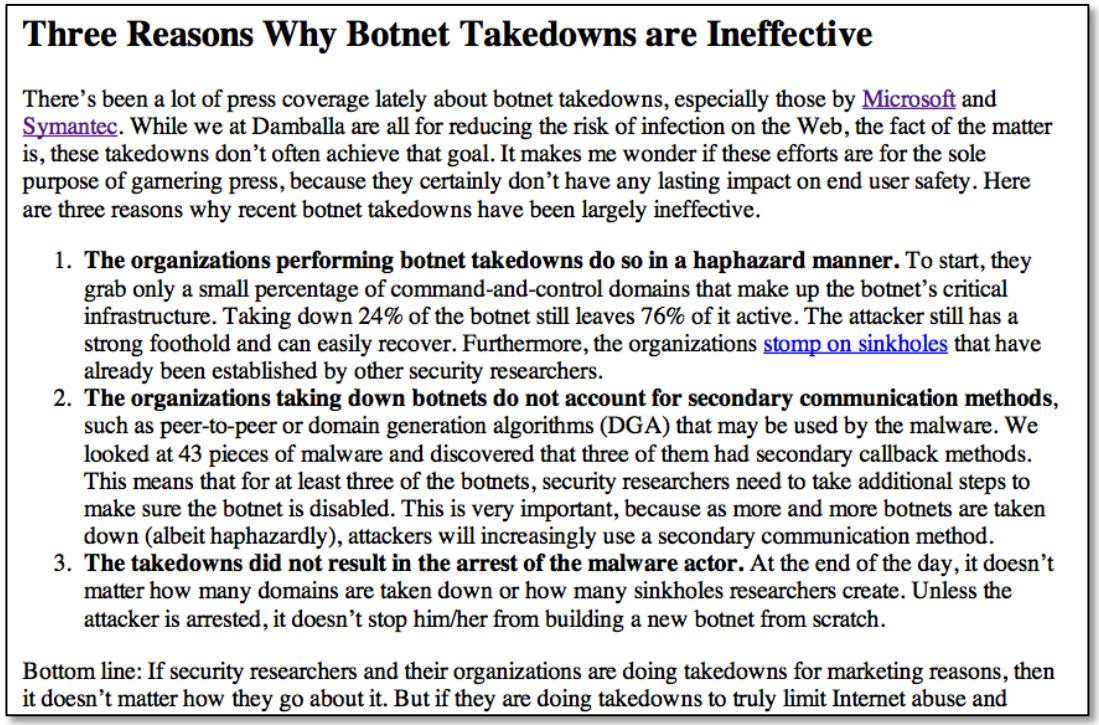
Zeus, SpyEye, Ice-X

- A.k.a., Win32/Zbot
- Zeus first appeared 2008
  - SpyEye merged with Zeus
  - Not just one botnet! (Sold as package)
- June 12, 2012 *Operation b71*
  - Microsoft, Kyrus Tech, Financial Services ISAC, National Automated Clearing House Association (NACHA) file complaint against 39 "John Doe" defendants

Criticism of Zeus Takedown

> Lastly, he says that this move will only spur cyber crooks to implement new countermeasures, which will likely involve updating their software to include P2P techniques to send commands to bots or encrypted communication between the bot herders and their bots.

Z. Zorz. Microsoft Citadel takedown ultimately counterproductive, June 2013. https://www.net-security.org/malware_news.php?id=2514



Three Reasons Why Botnet Takedowns are Ineffective

There's been a lot of press coverage lately about botnet takedowns, especially those by Microsoft and Symantec. While we at Damballa are all for reducing the risk of infection on the Web, the fact of the matter is, these takedowns don't often achieve that goal. It makes me wonder if these efforts are for the sole purpose of garnering press, because they certainly don't have any lasting impact on end user safety. Here are three reasons why recent botnet takedowns have been largely ineffective.

1. **The organizations performing botnet takedowns do so in a haphazard manner.** To start, they grab only a small percentage of command-and-control domains that make up the botnet's critical infrastructure. Taking down 24% of the botnet still leaves 76% of it active. The attacker still has a strong foothold and can easily recover. Furthermore, the organizations stomp on sinkholes that have already been established by other security researchers.
2. **The organizations taking down botnets do not account for secondary communication methods**, such as peer-to-peer or domain generation algorithms (DGA) that may be used by the malware. We looked at 43 pieces of malware and discovered that three of them had secondary callback methods. This means that for at least three of the botnets, security researchers need to take additional steps to make sure the botnet is disabled. This is very important, because as more and more botnets are taken down (albeit haphazardly), attackers will increasingly use a secondary communication method.
3. **The takedowns did not result in the arrest of the malware actor.** At the end of the day, it doesn't matter how many domains are taken down or how many sinkholes researchers create. Unless the attacker is arrested, it doesn't stop him/her from building a new botnet from scratch.

Bottom line: If security researchers and their organizations are doing takedowns for marketing reasons, then it doesn't matter how they go about it. But if they are doing takedowns to truly limit Internet abuse and

B. Foster. Three Reasons Why Botnet Takedowns are Ineffective, November 2013. https://blog.damballa.com/ archives/2195

Citadel

- Variant of published Zeus code
- June 6, 2013, *Operation b54*
  - Microsoft, FBI
  - 1,400 botnets disrupted
  - Responsible for over $500,000,000 in losses

According to Swiss security expert Roman Hüssy who runs the Zeus, SpyEye and Palevo Trackers, the action effected by Microsoft in conjunction with the FBI and several industry partners has inflicted considerable damage to his and other researchers' efforts. […] "The problem with cybercrime is that it can't be solved with doing takedowns. It's only possible to solve this issue by implementing legislation related to cybercrime, enforce them by getting bad actors arrested and implementing security by design on different layers," says Hüssy, adding that even though Microsoft's operation might have partly reached its goal, the result is only temporary. *Source: https://www.net-security.org/malware_news.php?id=2514*

SpyEye

THE FBI FEDERAL BUREAU OF INVESTIGATION

REPORT THREATS

CONTACT US | ABOUT US | MOST WANTED | NEWS | STATS & SERVICES | SCAMS & SAFETY

Atlanta Division

Select Language

Home • Atlanta • Press Releases • 2014 • Cyber Criminal Pleads Guilty to Developing and Distributing Notorious SpyEye Malwa

Twitter (30) Facebook (49) Share

Cyber Criminal Pleads Guilty to Developing and Distributing Notorious SpyEye Malware

U.S. Attorney's Office — **Northern District of Georgia**
January 28, 2014 — (404) 581-6000

ATLANTA—Aleksandr Andreevich Panin, a Russian national also known as "Gribodemon" and "Harderman," has pleaded guilty to conspiracy to commit wire and bank fraud for his role as the primary developer and distributor of the malicious software known as "SpyEye," which, according to industry estimates, has infected more than 1.4 million computers in the United States and abroad.

"As several recent and widely reported data breaches have shown, cyber attacks pose a critical threat to our nation's economic security," said United States Attorney Sally Quillian Yates. "Today's plea is a great leap forward in our campaign against those attacks. Panin was the architect of a pernicious malware known as SpyEye that infected computers worldwide. He commercialized the wholesale theft of financial and personal information. And now he is being held to account for his actions. Cyber criminals be forewarned—you cannot hide in the shadows of the Internet. We will find you and bring you to justice."

FBI Jobs

Aleksander Panin of Tver, Russia, allegedly sold SpyEye to at least 150 clients intent on hijacking banking transactions. *Photo: RT*

Time between Mariposa takedown and Iserdo Conviction

December 23, 2009 – December 23, 2013

Takedown December 23, 2009
DDoS attack January 22, 2010
Spanish arrests in February, 2010
Slovenian arrest of Iserdo June, 2010
Iserdo sentenced to 5 years December 23, 2013

Time between Operation B79 Civil Legal Action and Plea Agreement

September 22, 2011 – October 19, 2012

Suit filed September 22, 2011
Defendant Piatti named September 26, 2011
Plea agreement reached with Piatti October 26, 2011
Defendant Sabelnikov named January 23, 2012
Plea agreement reached with Sabelnikov October 19, 2012

Time between Zeus/SpyEye Civil Legal Action and Criminal Guilty Plea

June 12, 2012 – January 28, 2014

Operation b79 Civil Legal Action June 12, 2012 (identifying Panin as suspect)
Panin arrest in Dominican Republic July 2013
Defendant Panin pleads guilty January 28, 2014

Takedown to Justice

January 1, 2010 | July 1, 2010 | January 1, 2011 | July 1, 2011 | January 1, 2012 | July 1, 2012 | January 1, 2013 | July 1, 2013

Time between Mariposa takedown and Iserdo Conviction

December 23, 2009 – December 23, 2013

Takedown December 23, 2009
DDoS attack January 22, 2010
Spanish arrests in February, 2010
Slovenian arrest of Iserdo June, 2010
Iserdo sentenced to 5 years December 23, 2013

013

Time between Operation B79 Civil Legal Action and Plea Agreement

September 22, 2011 – October 19, 2012

Suit filed September 22, 2011
Defendant Piatti named September 26, 2011
Plea agreement reached with Piatti October 26, 2011
Defendant Sabelnikov named January 23, 2012
Plea agreement reached with Sabelnikov October 19, 2012

Spy Eye v1.4

July 1, 2012

January 1, 2013

July 1, 2013


ration B79 Civil Legal Action and Plea Agreement
1 – October 19, 2012
Suit filed September 22, 2011
Defendant Piatti named September 26, 2011
Plea agreement reached with Piatti October 26, 2011
Defendant Sabelnikov named January 23, 2012
Plea agreement reached with Sabelnikov
Time between Zeus/SpyEye Civil Legal Action and Criminal Guilty Plea
June 12, 2012 – January 28, 2014
Spy Eye v1.4
Operation b79 Civil Legal Action June 12, 2012 (identifying Panin as suspect)
Panin arrest in Dominican Republic July 2013
Defendant Panin pleads guilty January 28, 2014
July 1, 2012
January 1, 2013
July 1, 2013
2012

Time between Mariposa takedown and Iserdo Conviction

December 23, 2009 – December 23, 2013

Takedown December 23, 2009
DDoS attack January 22, 2010
Spanish arrests in February, 2010
Slovenian arrest of Iserdo June, 2010
Iserdo sentenced to 5 years December 23, 2013

Time between Operation B79 Civil Legal Action and Plea Agreement

September 22, 2011 – October 19, 2012

Suit filed September 22, 2011
Defendant Piatti named September 26, 2011
Plea agreement reached with Piatti October 26, 2011
Defendant Sabelnikov named January 23, 2012
Plea agreement reached with Sabelnikov October 19, 2012

Time between Zeus/SpyEye Civil Legal Action and Criminal Guilty Plea

June 12, 2012 – January 28, 2014

Operation b79 Civil Legal Action June 12, 2012 (identifying Panin as suspect)
Panin arrest in Dominican Republic July 2013
Defendant Panin pleads guilty January 28, 2014

Takedown to Justice

January 1, 2010 | July 1, 2010 | January 1, 2011 | July 1, 2011 | January 1, 2012 | July 1, 2012 | January 1, 2013 | July 1, 2013

Conclusion

- We should work together more instead of fighting with each other
- Advisory body to evaluate risky CS operations before and after individuals, companies, or researchers take actions.

CONTACT

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

- Katherine Carpenter
  carpenter.katherinej @ gmail.com