SO YOU WANT TO TAKE OVER A BOTNET...
Agenda

- “I’m fighting back. What’s the big deal?”
- Ethics and The Menlo Report
- What it takes to “do it right”
- Case studies (maybe not) and observations
- Conclusions
Frustration and Loathing

- “Law enforcement is not doing their job.”
- “I’m tired of being passive and taking punches. It’s time to go on the offensive.”
- “I have a right to self-defense.”

“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
FAQ: Disabling the new Hlux/Kelihos Botnet

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

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 HiLux 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 HiLux: 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 HiLux 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 5539 votes were counted.
Existing Ethics Standards

- The IEEE, ACM, etc: Codes of Ethics
- The Belmont Report, the National Research Act, and Institutional Review Boards (IRB)
  - 45 CFR 46
- “Rules of Engagement”
  - The Law of Armed Conflict
  - Dittrich/Himma: Active Response Continuum
- Other Organizational Codes (Universities, Corporations, etc.)
Existing Ethical Norms

<table>
<thead>
<tr>
<th>Principle</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defense</td>
<td>Population being protected is identified?</td>
</tr>
<tr>
<td>Defense</td>
<td>Looks like use of force?</td>
</tr>
<tr>
<td>Defense</td>
<td>Actions are proportional?</td>
</tr>
<tr>
<td>Defense</td>
<td>Necessary to repel or prevent harm?</td>
</tr>
<tr>
<td>Defense</td>
<td>Benefits of disclosure favor victims over attackers?</td>
</tr>
<tr>
<td>Defense</td>
<td>Actions are appropriately directed?</td>
</tr>
<tr>
<td>Necessity</td>
<td>Greater moral good defined?</td>
</tr>
<tr>
<td>Necessity</td>
<td>No other reasonable options available?</td>
</tr>
<tr>
<td>Necessity</td>
<td>Otherwise respectful of rights?</td>
</tr>
<tr>
<td>Punishment</td>
<td>Avoids punitive motives?</td>
</tr>
<tr>
<td>Retribution</td>
<td>Avoids retributive motives?</td>
</tr>
<tr>
<td>Evidentiary</td>
<td>Adequate reason to think preconditions of applying other principles are met?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Principle</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do Good</td>
<td>Positively impacts human well-being?</td>
</tr>
<tr>
<td>Avoid Harm</td>
<td>Harms users, public, employees, or employers?</td>
</tr>
<tr>
<td>Avoid Harm</td>
<td>Efforts made to mitigate or undo negative consequences?</td>
</tr>
<tr>
<td>Be Honest</td>
<td>Honors property rights?</td>
</tr>
<tr>
<td>Be Honest</td>
<td>Gives proper credit?</td>
</tr>
<tr>
<td>Be Honest</td>
<td>Honors confidentiality?</td>
</tr>
<tr>
<td>Be Fair</td>
<td>Discriminates on basis of race, sex, religion, age, disability, or nationality?</td>
</tr>
<tr>
<td>Be Fair</td>
<td>Inequities exist between groups?</td>
</tr>
<tr>
<td>Privacy</td>
<td>Minimal information collected?</td>
</tr>
<tr>
<td>Privacy</td>
<td>Protected from unauthorized access?</td>
</tr>
<tr>
<td>Privacy</td>
<td>Data used only for intended purposes?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Principle</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respect for Persons</td>
<td>Individuals treated as autonomous agents?</td>
</tr>
<tr>
<td>Respect for Persons</td>
<td>Individuals (or their providers) informed and allowed to consent?</td>
</tr>
<tr>
<td>Respect for Persons</td>
<td>Individuals with diminished autonomy protected?</td>
</tr>
<tr>
<td>Respect for Persons</td>
<td>Identities of innocents are protected?</td>
</tr>
<tr>
<td>Beneficence</td>
<td>Low potential to inflict harm?</td>
</tr>
<tr>
<td>Beneficence</td>
<td>Maximize possible benefits and minimize harms</td>
</tr>
<tr>
<td>Beneficence</td>
<td>Risks and benefits systematically evaluated</td>
</tr>
<tr>
<td>Justice</td>
<td>Who benefits?</td>
</tr>
<tr>
<td>Justice</td>
<td>Fairness (neutrality) of procedures</td>
</tr>
</tbody>
</table>

Active Response Continuum

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

<table>
<thead>
<tr>
<th>Level</th>
<th>Actor’s Posture</th>
<th>Characteristic Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Non-cooperative</td>
<td>Intelligence collection, tracebacks, cease &amp; desist, retaliatory counterstrike [takedown/takeover]</td>
</tr>
<tr>
<td>3</td>
<td>Cooperative</td>
<td>Joint traceback, collaboration, sharing</td>
</tr>
<tr>
<td>2</td>
<td>Interactive</td>
<td>Modify own systems in response to attack</td>
</tr>
<tr>
<td>1</td>
<td>Involved</td>
<td>Uses AV, simple firewalls, basic encryption</td>
</tr>
<tr>
<td>0</td>
<td>Unaware</td>
<td>None (expect others to protect them)</td>
</tr>
</tbody>
</table>

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 4 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”)**

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

A Protected REpository for Defense of Infrastructure against Cyber Threats

- PREDICT Program Objective
  “To advance the state of the research and commercial development (of network security ‘products’) we need to produce datasets for information security testing and evaluation of maturing networking technologies.”

- Rationale / Background / Historical:
  - Researchers with insufficient access to data unable to adequately test their research prototypes
  - Government technology decision-makers with no data to evaluate competing “products”

End Goal: Improve the quality of defensive cyber security technologies
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
## The Menlo Report

<table>
<thead>
<tr>
<th>Belmont Principle</th>
<th>Menlo Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respect for Persons</td>
<td>➢ Identify stakeholders</td>
</tr>
<tr>
<td></td>
<td>➢ Informed consent</td>
</tr>
<tr>
<td>Beneficence</td>
<td>➢ Identify potential benefits and harms</td>
</tr>
<tr>
<td></td>
<td>➢ Balance risks and benefits</td>
</tr>
<tr>
<td></td>
<td>➢ Mitigate realized harms</td>
</tr>
<tr>
<td>Justice</td>
<td>➢ Fairness and equity</td>
</tr>
<tr>
<td>Additional Menlo Principle:</td>
<td>➢ Compliance</td>
</tr>
<tr>
<td>for the Law and Public Interest</td>
<td>➢ Transparency and accountability</td>
</tr>
</tbody>
</table>

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”

---


How to do it “right”

You must be this tall to take down a botnet
What’s necessary

- We need to name things better
- We need to count things better
  - “Not everything that counts can be measured. Not everything that can be measured counts.” Albert Einstein
- We need to see the forest, not just the trees
- We need to work & play well together (better)
- We need to demonstrate integrity
  - Able 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

The United States Military
A bot is a bot. Unless its not. A bot.

Bot
Dropper
Exploit Kit
Browser Exploit Pack
Control panel
Keylogger
Remote Access Trojan
C&C server
Trojan
RFI server
Worm
P2P bot
Mothership
Fast-flux
Dropzone
Config server
Cache
Injection server
Drive-by-download server
...
Multi-phase operation

Multi-phase infection

Deconstructing the Black Hole Exploit Kit, December 2011.

Getting the full picture is hard.

“[It] is uncommon to have a complete data set covering all aspects of the attackers' operations. Some may have access to data regarding the attackers' activities once inside a particular network. Others may have extensive collections of malware samples and historical data on command and control infrastructure. Others may have information on how the attackers use various exploits, or craft targeted spear phishing emails and other methods focused on compromising particular targets. Others may have data retrieved from the attackers that indicate the identity of those who have been compromised. And finally still others may have the necessary geopolitical knowledge to interpret the attacks within a broader context.

Often, investigations do not have the luxury of such a full data set and must rely on incomplete information and partial observations. Further complicating matters is that any of this information is often dependent on mistakes made by the attackers, which typically lead to slices of an overall network instead of a comprehensive view. “

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) Sinkhole

- March 21, 2012
- Dell SecureWorks, CrowdStrike, Kaspersky, and the Honeynet Project
  - FAQ on Kelihos.B/Hlux sinkholing [http://www.honeynet.org/node/836](http://www.honeynet.org/node/836)
**Question:** Who are all the stakeholders involved in the Kelihos.B/Hzux.B botnet?

The Honeynet Project

**FAQ on Kelihos.B/Hzux.B sinkholing**

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


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/Hzux sinkholing operation.

- 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 receive 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.
Microsoft W32/Fifesock.I

Payload

Spammer:Win32/Fifesock.I (?)

Anot Encyclopedia entry
user Updated: May 02, 2011 | Published: Apr 08, 2011
user
Aliases
Once Not available

tn
Alert Level (?)
Severe

Antimalware protection details
Microsoft recommends that you download the latest definitions to get protected.

Detection initially created:
Definition: 1.101.1074.0
Released: Apr 08, 2011

Summary
Spammer:Win32/Fifesock.I is a component of Win32/Fifesock - a multiple component trojan family that injects code into Internet Explorer and Firefox in order to steal the user's social networking credentials for sites such as Facebook, Twitter and Blogspot, and then uses these credentials to send spam to their contacts. It may also download and execute arbitrary files. Some variants have also been observed to install rogue security software such as Rogue:Win32/Winwebsec.

- HKCU\Software\facebook
### Malware for ip: 95.64.9.20 - Clean MX - realtime

<table>
<thead>
<tr>
<th>#</th>
<th>Odate</th>
<th>Oclosed</th>
<th>Ohours</th>
<th>Contributor</th>
<th>Virusname</th>
<th>URL</th>
<th>Op state</th>
</tr>
</thead>
</table>

**Attention:** column contributor=ecommerce, this indicates cases shop owners shall update their outdated ecommerce installations asap.
Dynamoo links Fifesock to Lizamoon

Dynamoo's Blog

Saturday, 2 April 2011

**alisa-carter.com, lizamoon.com and world-of-books.com**

The injection attacks from lizamoon.com and other domains continue, and they link back to a popular blog post about a very different attack site at world-of-books.com because at the moment, all these sites appear to be on the same server at 95.64.9.18 belonging to Intermedia TOP SRL.

The following sites are on that malicious server:
- alexbiane.com
- alisa-carter.com
- lizamoon.com
- tfrytv56.info
- taddygus.com
- world-of-books.com

Right now the safest thing to do is block traffic to 95.64.8.0.2 (95.64.8.0 - 95.64.8.255) at the very least. But given that there are several bad networks now within the mostly Romanian 98.84.0.0/16, there’s very little to lose in blocking the whole /16 for now if you don’t have dealings with Romania.

If you need to block bad traffic due to the situation in some other way, then I’d be interested in this blog...
Mr. Waledac: The Peter North of Spamming

ssh 193.27.246.171
ssh: connect to host 193.27.246.171 port 22: No route to host

Ip-server must have resolved the outage, because the server that Severa was complaining about — 193.27.246.171 — would be flagged a day later by malware analysts, and tagged as a control server for the Waledac botnet.

On Monday, Microsoft filed papers with a Virginia court stating that Kelihos was operated by Andrey N. Sabelnikov, a St. Petersburg man who once worked at Russian antivirus and security firm Avira. But according to the researcher who shared that intelligence with
Trojan Nap aka Kelihos/Hlux - Feb. 2013 Status Update

Update Feb 11, 2012 Regarding media headlines that it is a "new version":
Please note that this post is a "status update" on the growth of the Kelihos botnet. It is the same botnet and malware as we saw last year. The goal of the post is to highlight the rapid re-growth after the March 2012 takedown and share the recent known someihoma server data.

FirEye posted details about the sleep function found in Kehilohs/Hlux (An encounter with Trojan Nap), which is interesting, and indeed is present in some of the samples we saw. The trojan, of course, has many more features, and most of them were documented in previous publications online. This post is a quick update on the state of Kelihos/Hlux botnet, along with the list of known fast flux domains (~150+) associated with with Kelihos distribution or Command & Control. (current, > 2012). The current and most active name servers are pointed to the ns[1-6] boonsaco.com, ns[1-6] lpxion.com, and ns[1-6] zampaklu.ru which are also fast flux domains. The double fast flux nature of the botnet makes it very difficult to take down, and sinkholing is a temporary measure. Despite the two large attempts to take it down (Sep.2011 and Mar. 2012), the botnet is definitely on the rise again.

Previously published research about Kelihos

Feb. 2013 - An encounter with Trojan Nap - FireEye
Jan. 2013 - Weledac Gets Cozy with Vultr - Symantec (Symantec call Kelihos "Weledac (Kelihos)"
Jan. 2013 - Beware of Kelihos-27 - Portable Apps member note
Dec. 2012 - A Quick Update On Spambot Kelihos - abuse.ch
Mar. 2012 - Kelihos R/Hlux B. botnet takes down - Honeynet Project
Mar. 2012 - Botnet Shutdown Success Story - again: Disabling the new Hlux/Kelihos Botnet - Securitlist
Mar. 2012 - Kelihos: not Alien Resurrection, more Attack of the Clones - ESET
Mar. 2012 - FAQ: Disabling the new Hlux/Kelihos Botnet - Securitlist
Mar. 2012 - Kelihos Back In Town Using Fast Flux - Abuse.ch
Feb. 2012 - Long life to Kelihos! - Webensee / Gianluca Guaitani
Feb. 2012 - The where and way of HLUX - Security
Jan. 2012 - Kelihos/Hlux botnet returns with new techniques - Securitlist
Sep. 2011 - Botnet Shutdown Success Story: How Kaspersky Lab Disabled the Hlux/Kelihos Botnet
Sep. 2011 - Microsoft Neutralizes Kelihos Botnet, Names Defendant In Case
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

Polls

*How should Kaspersky proceed with the Hlux/Kelihos Botnet?*

- Leave the botnet alone
  - 359 [4%]
- Keep the sinkholing up and provide IP address logs to the appropriate contacts so they can take actions
  - 755 [9%]
- Push a cleanup tool that removes the infections
  - 6493 [85%]
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 Recent Takedowns

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

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 abandoned, facts in [64, 96, 49] suggest the “success” is qualified.
10. Total infections observed by Microsoft since 2007. Damalilla 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 Polka 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.
Observations

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

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)
Conclusions

- We sometimes have conflicting goals and we’re starting to eat our own young

Conclusions

- We sometimes fail Stephen Carter’s *integrity* test
- We are in an arms race
  - Cost of attacking $< <$ cost of countering attacks
  - Cost of being thorough $>>$ cutting corners

"Instead of making pie charts, we should treat a botnet as a crime scene and not just a research project."  David Dagon, Georgia Tech
[http://security.ulitzer.com/node/1305941](http://security.ulitzer.com/node/1305941)
Conclusions

- We can do a better job, and we must
  - Better integrate analyses and observations
  - Use the scientific method (i.e., lab a.o.t. field)
  - Better coordinate actions, investigations
  - Mature our understanding of legal/ethical/technical/political considerations and options

Bottom line: It is possible to put ego aside, act in ways that serve others, and do things because they make the world a better place.
Contact

- Dave Dittrich
  Applied Physics Laboratory
  University of Washington
  dittrich at apl dot uw dot edu
  http://staff.washington.edu/dittrich/