OFFENSIVE ANTI-BOTNET - SO YOU WANT TO TAKE OVER A BOTNET...

David Dittrich
University of Washington

NANOG 59
October 8, 2013 Phoenix, AZ

Slides available at: http://staff.washington.edu/dittrich/talks/nanog59/

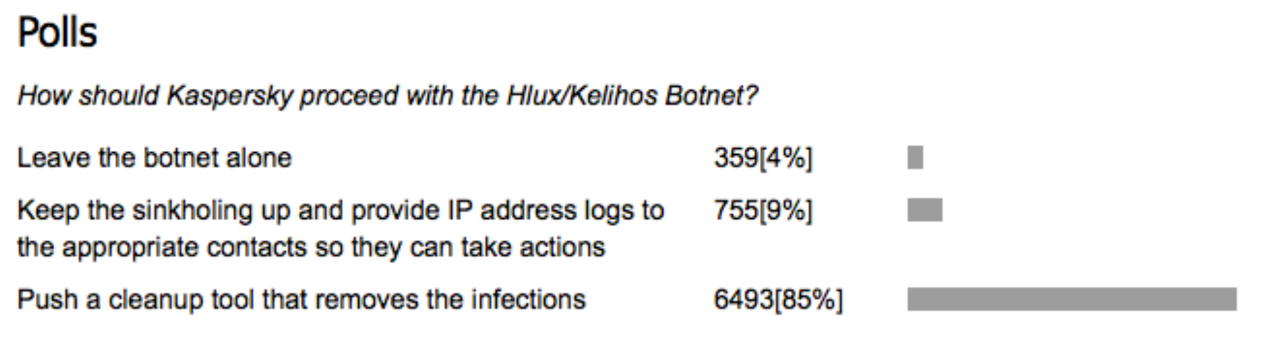
AGENDA

- "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

"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'm tired of being passive and taking punches. It's time to go on the offensive."
- "I have a right to self-defense."



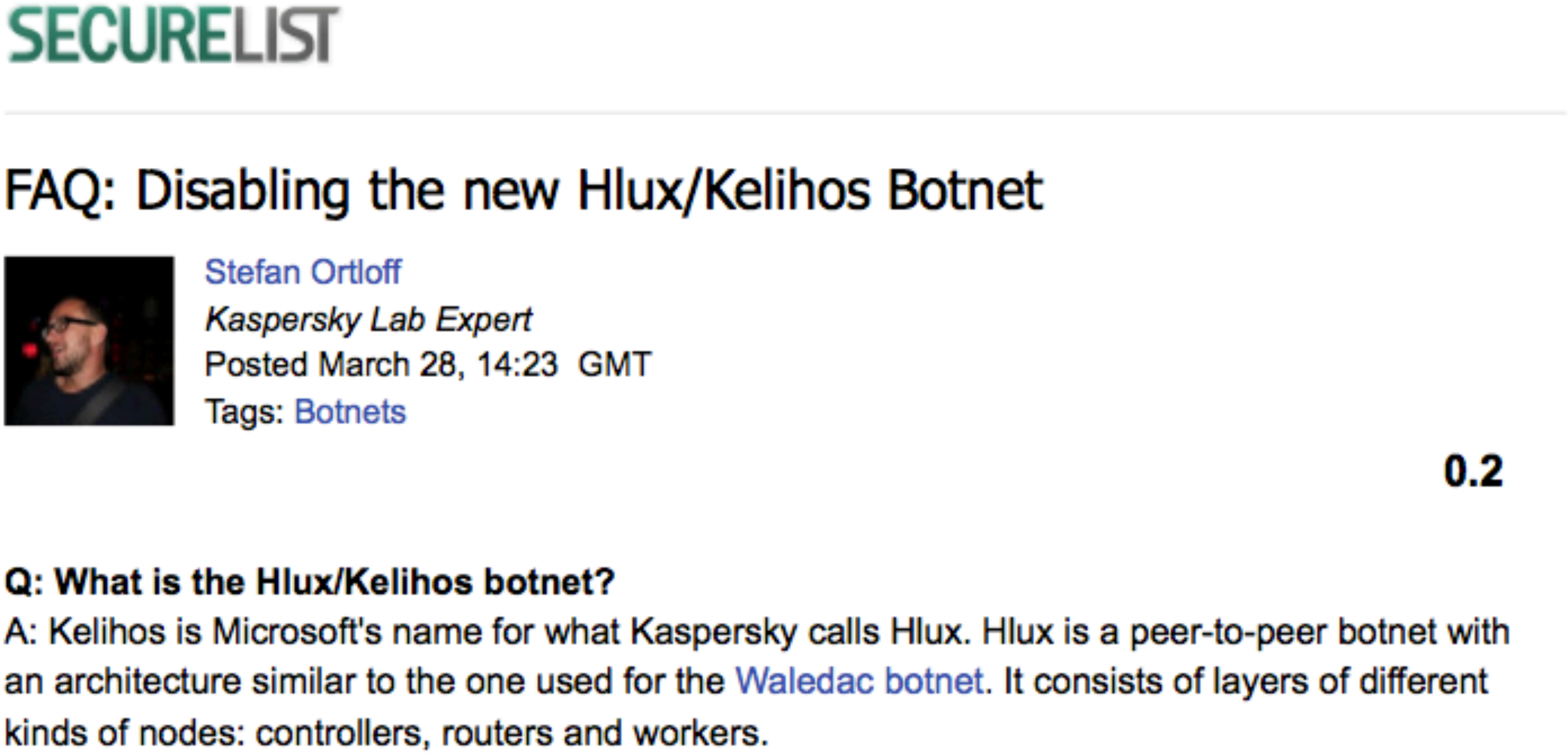
Polls

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%]	▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮

S. Ortloff. FAQ: Disabling the new Hlux/Kelihos Botnet, March 2012.
http://www.securelist.com/en/blog/208193438/FAQ_Disabling_the_new_Hlux_Kelihos_Botnet

Sinkhole as a Service?



SECURELIST

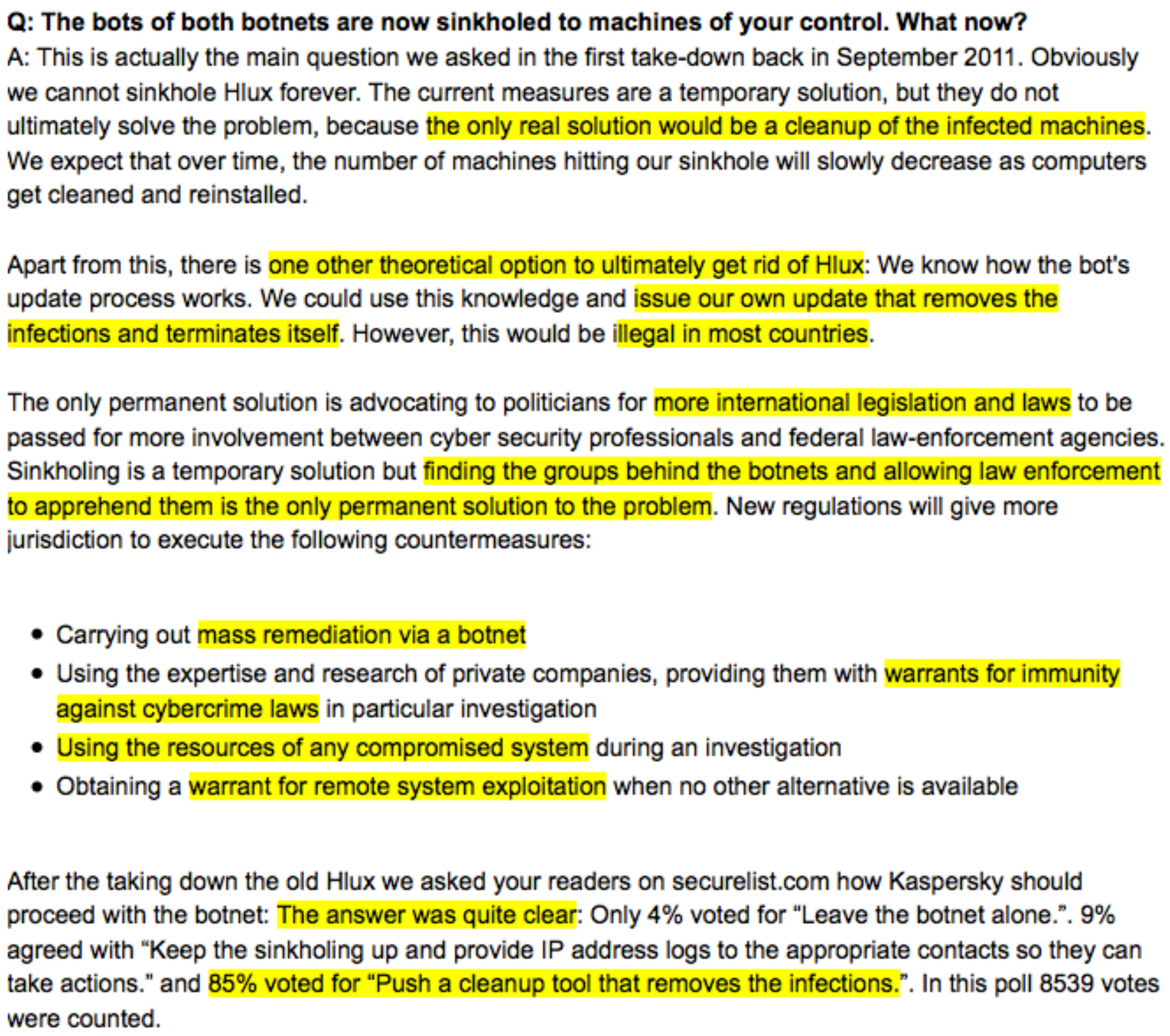
FAQ: Disabling the new Hlux/Kelihos Botnet

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:

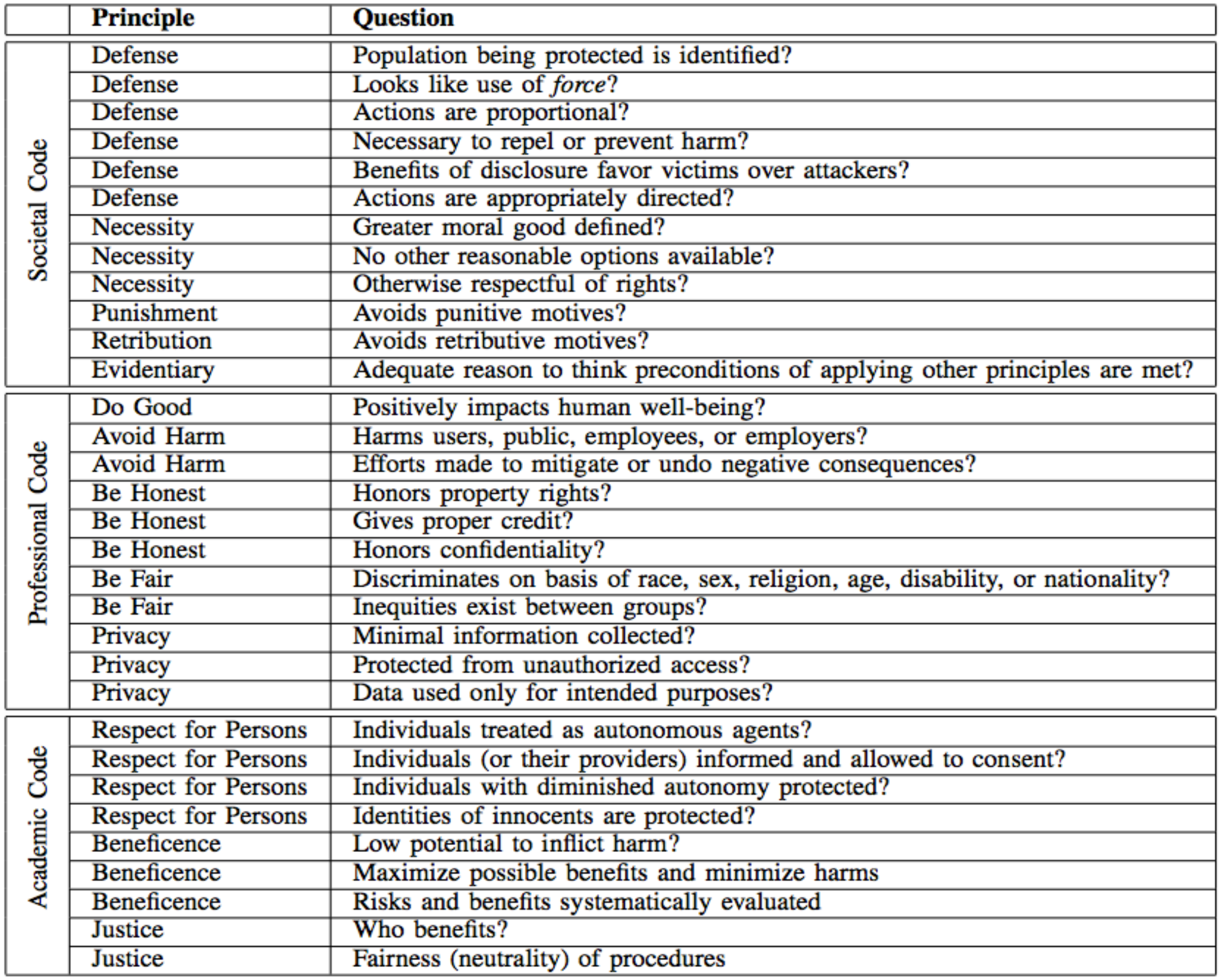
- Carrying out mass remediation via a botnet
- Using the expertise and research of private companies, providing them with warrants for immunity against cybercrime laws in particular investigation
- Using the resources of any compromised system during an investigation
- Obtaining a warrant for remote 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.

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



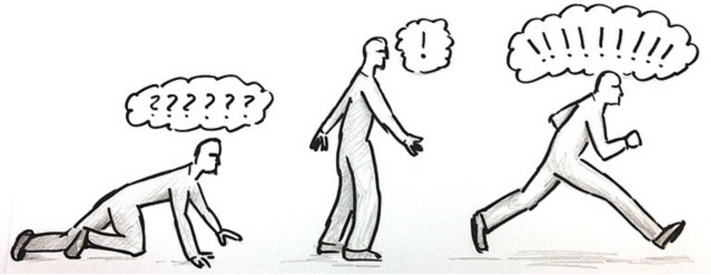
	Principle	Question
Societal Code	Defense	Population being protected is identified?
	Defense	Looks like use of *force*?
	Defense	Actions are proportional?
	Defense	Necessary to repel or prevent harm?
	Defense	Benefits of disclosure favor victims over attackers?
	Defense	Actions are appropriately directed?
	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.*

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)

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 4 Levels

“Active Response Continuum” is a better phrase

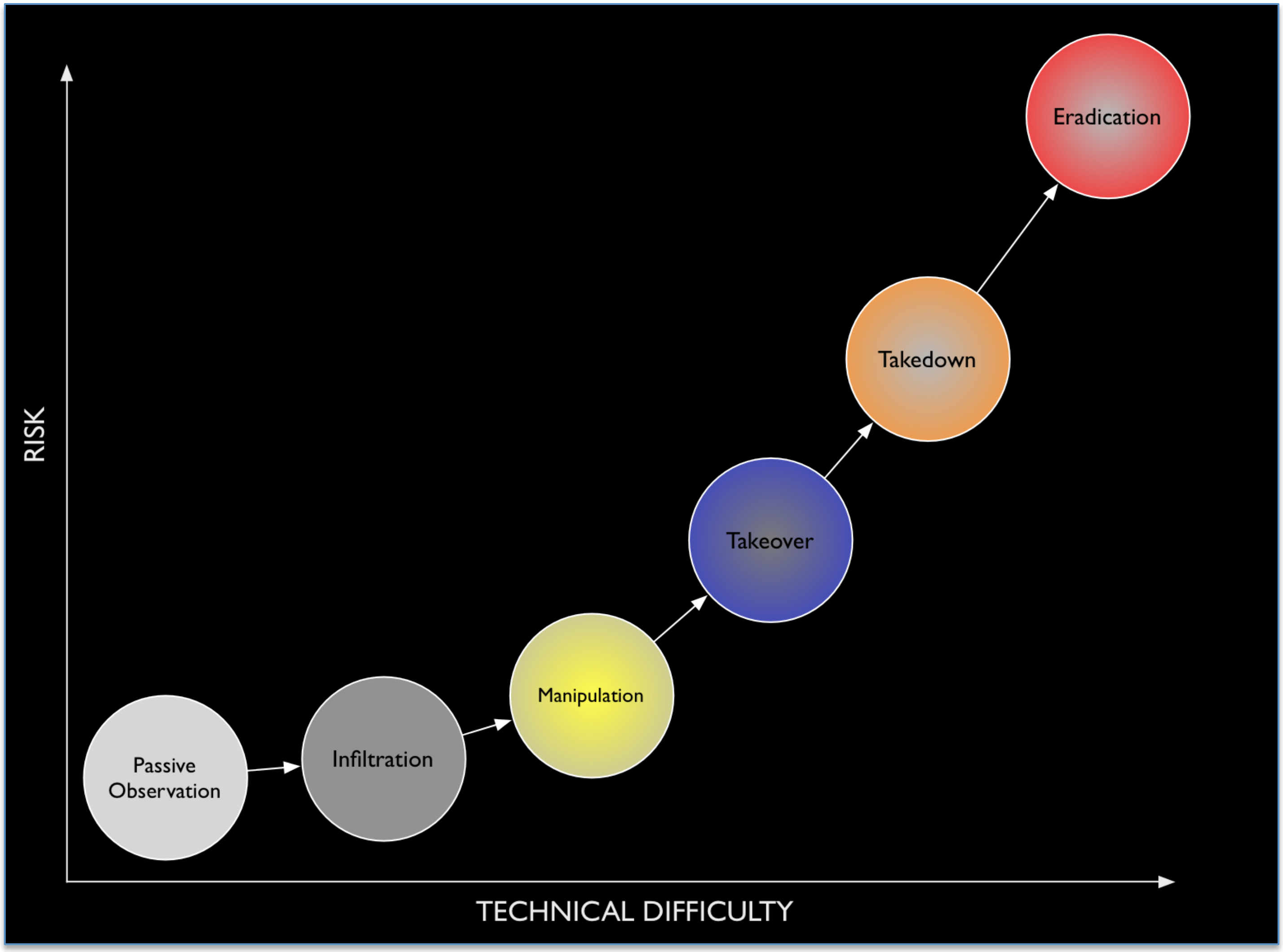
D. Dittrich. Debating the Active Response Continuum: Defining the Terms of the Debate, May 2013. http://www.honeynet.org/node/1048

LEVEL 4 OF THE ACTIVE RESPONSE CONTINUUM

- 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



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

DENNING AND STRAWSER: 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; and 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.

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

Dittrich and Kenneally (editors). The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research, December 2011. http://www.cyber.st.dhs.gov/wp-content/uploads/2011/12/MenloPrinciplesCORE-20110915-r560.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"

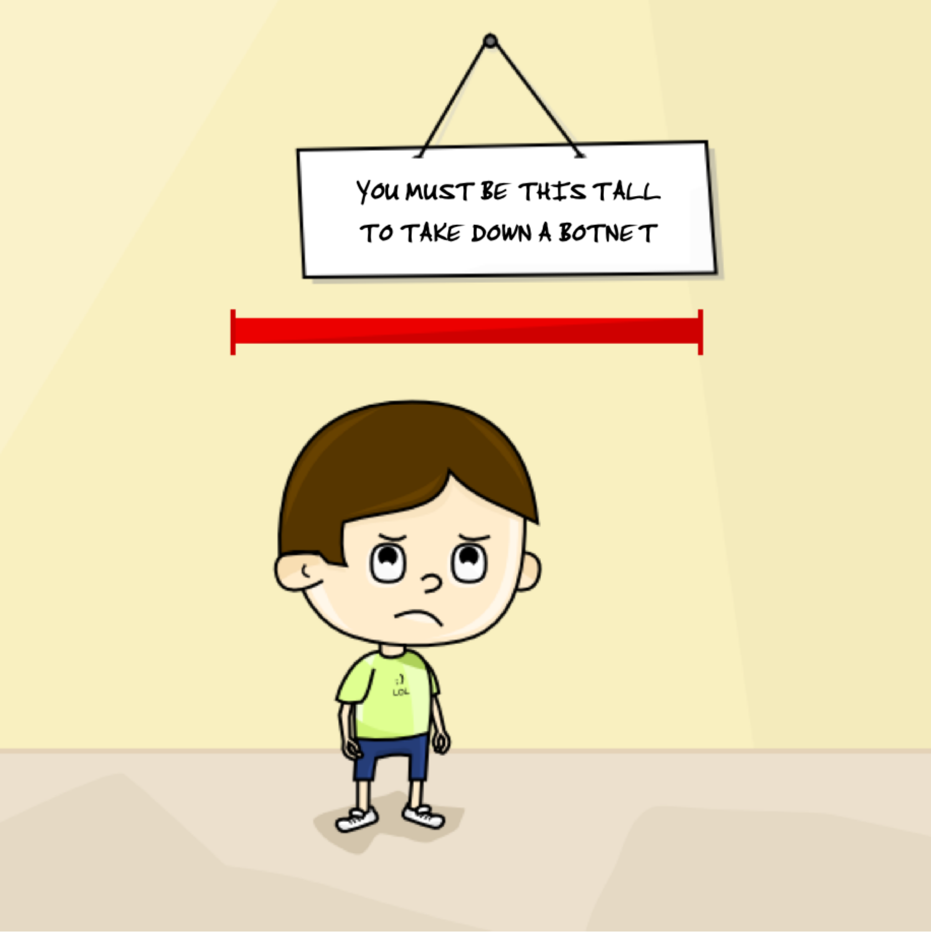
D. Dittrich. FAQ on Kelihos.B/Hlux.B sinkholing, March 2012. http://www.honeynet.org/node/836

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

How to do it "right"



WHAT'S NECESSARY

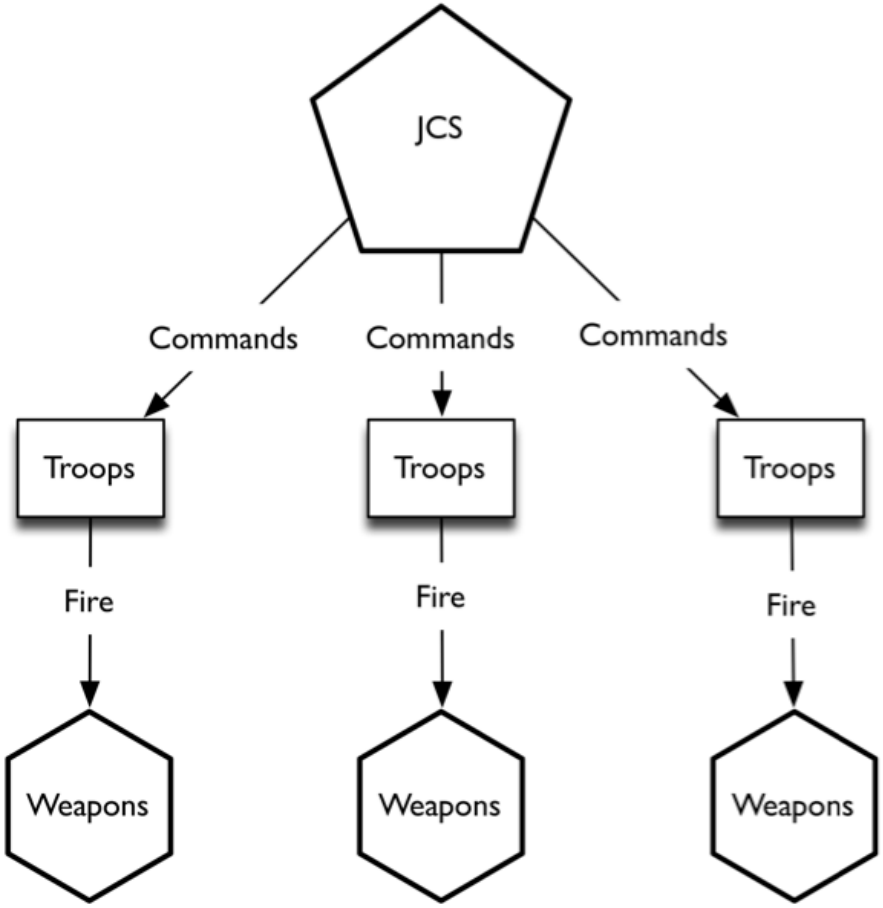
- We need to name things better
- We need to count things better
  - "Not everything that counts can be measured. Not everything that can be measured counts." Albert Einstein
- We need to see the forest, not just the trees
- We need to work & play well together (even better)

WHAT'S NECESSARY

- We need to demonstrate *integrity*
  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

The U. S. Military



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
…

A BOT, IS A BOT. UNLESS IT'S NOT. A BOT.

WHAT'S IN A NAME?

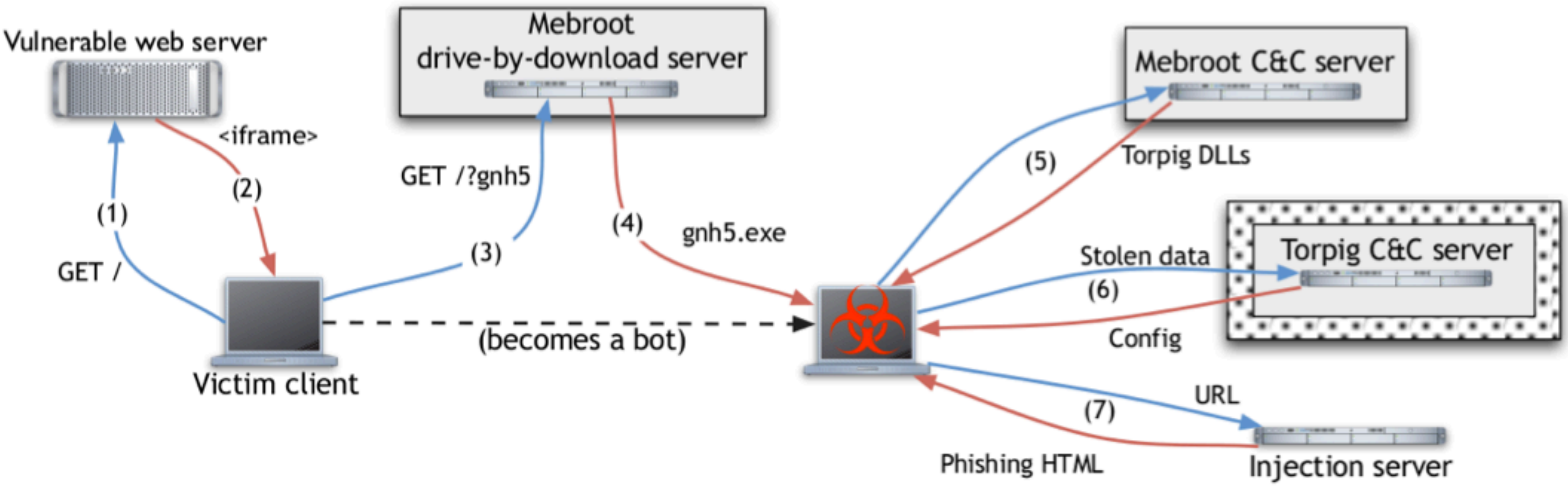
Mandiant	CrowdStrike	Dell	Trend	A.K.A.
APT1	Comment Panda	Comment Crew (Shady RAT?)	Comment Crew	Comment Group
APT12	Numbered Panda	?	IXESHE	DynCalc, JoyRAT

The problem makes it more difficult for threat-intelligence firms to share information with each other about threats, says Adam Meyers, vice president of intelligence for CrowdStrike.

"We've seen a problem in that there is no common lexicon for how we describe targeted attacks," Meyers says. "We are quickly turning into the antivirus industry."

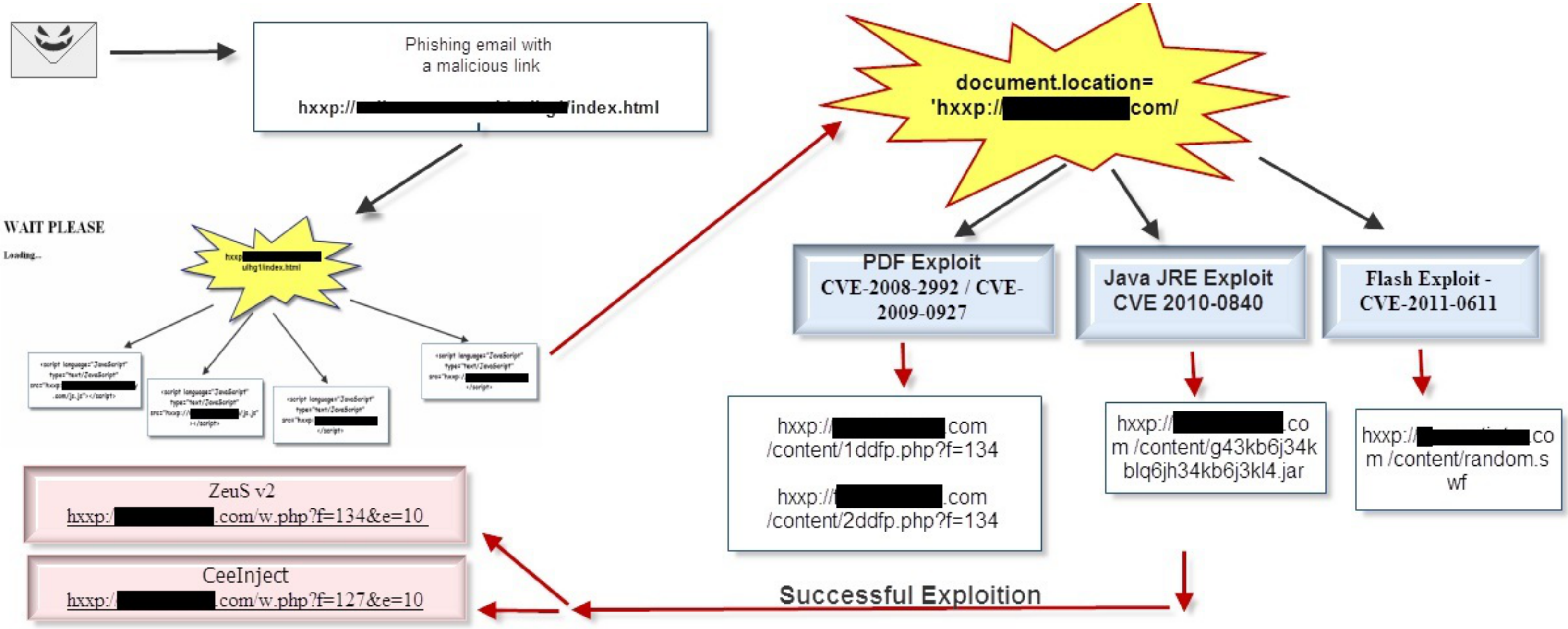
R. Lemos. Firms Far From Taming The Tower Of APT Babel, July 2013. http://www.darkreading.com/threat-intelligence/firms-far-from-taming-the-tower-of-apt-b/240158923

MULTI-PHASE OPERATION



Brett Stone-Gross, et al. Your Botnet is My Botnet: Analysis of a Botnet Takeover. In Proceedings of the ACM CCS, November 2009.

MULTI-PHASE INFECTION



Phishing email with a malicious link

hxxp://[redacted]/index.html

WAIT PLEASE

Loading...

hxxp[redacted] ulhg1index.html

<script language="JavaScript" type="text/JavaScript" src="hxxp:[redacted] .com/js.js"></script>

<script language="JavaScript" type="text/JavaScript" src="hxxp://[redacted]/js.js" ></script>

<script language="JavaScript" type="text/JavaScript" src="hxxp:[redacted] </script>

<script language="JavaScript" type="text/JavaScript" src="hxxp:/[redacted] </script>

document.location= 'hxxp://[redacted]com/

PDF Exploit CVE-2008-2992 / CVE-2009-0927

Java JRE Exploit CVE 2010-0840

Flash Exploit - CVE-2011-0611

hxxp://[redacted].com /content/1ddfp.php?f=134

hxxp://[redacted].com /content/2ddfp.php?f=134

hxxp://[redacted].com /content/g43kb6j34kblq6jh34kb6j3kl4.jar

hxxp://[redacted].com /content/random.swf

Successful Exploition

ZeuS v2 hxxp:/[redacted].com/w.php?f=134&e=10

CeeInject hxxp:/[redacted].com/w.php?f=127&e=10

Deconstructing the Black Hole Exploit Kit, December 2011. http://blog.imperva.com/2011/12/deconstructing-the-black-hole-exploit-kit.html

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. “

Information Warfare Monitor and The Shadowserver Foundation. Shadows in the Cloud: An investigation into cyber espionage 2.0, April 2010. http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0

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?"

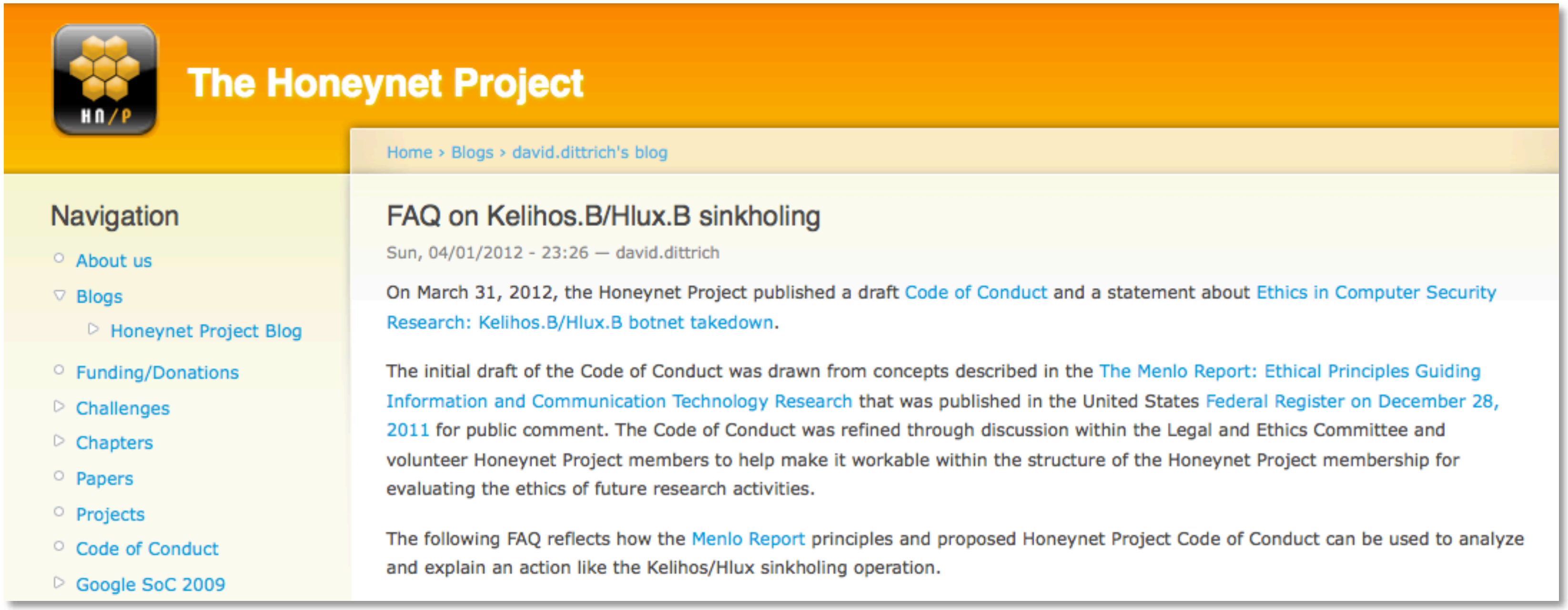
Paul Vixie

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 Sinkhole FAQ

Question: Who are all the stakeholders involved in the Kelihos.B/Hlux.B botnet?



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.

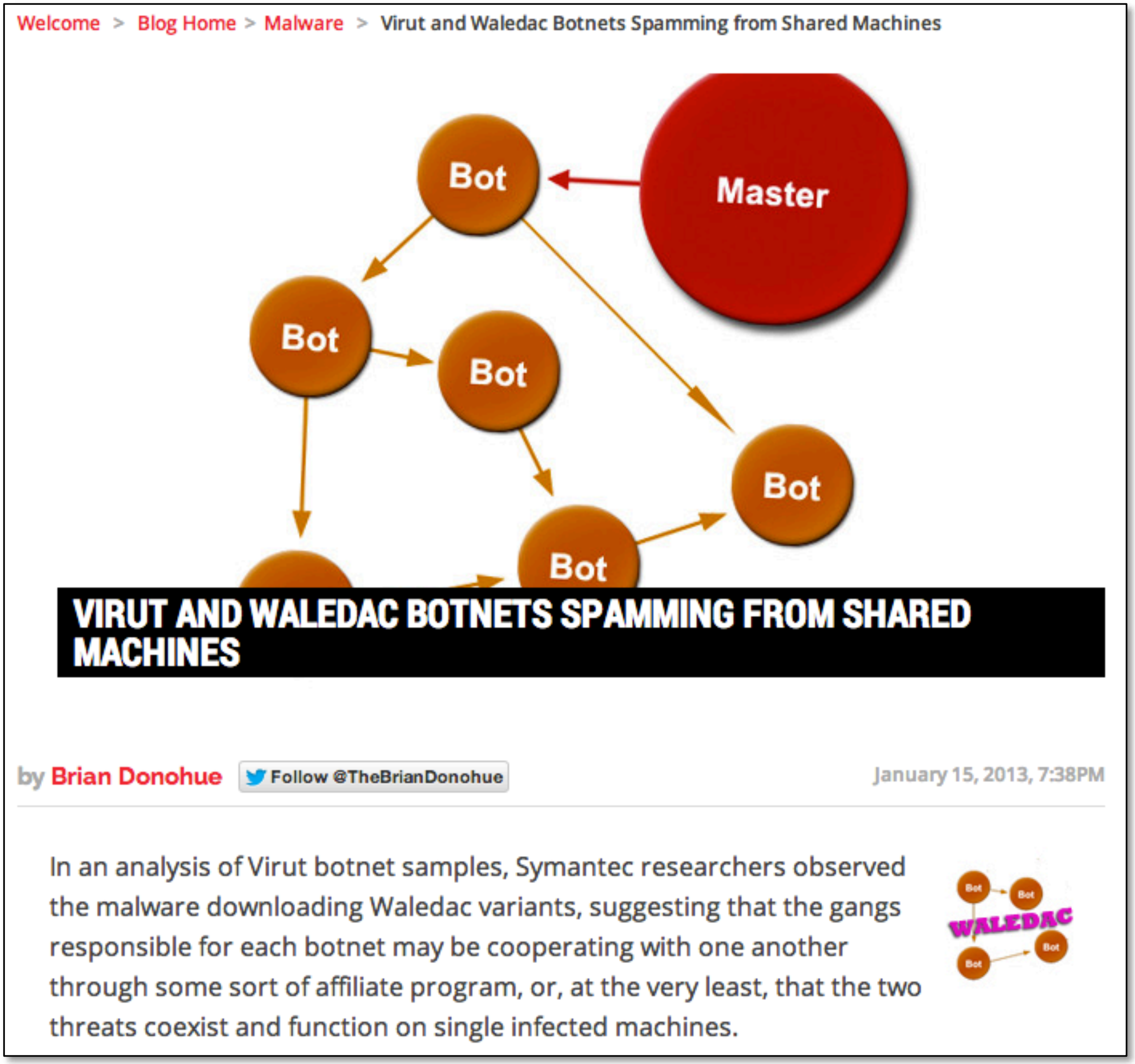
The initial draft of the Code of Conduct was drawn from concepts described in the The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research that was published in the United States Federal Register on December 28, 2011 for public comment. The Code of Conduct was refined 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.

- 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.



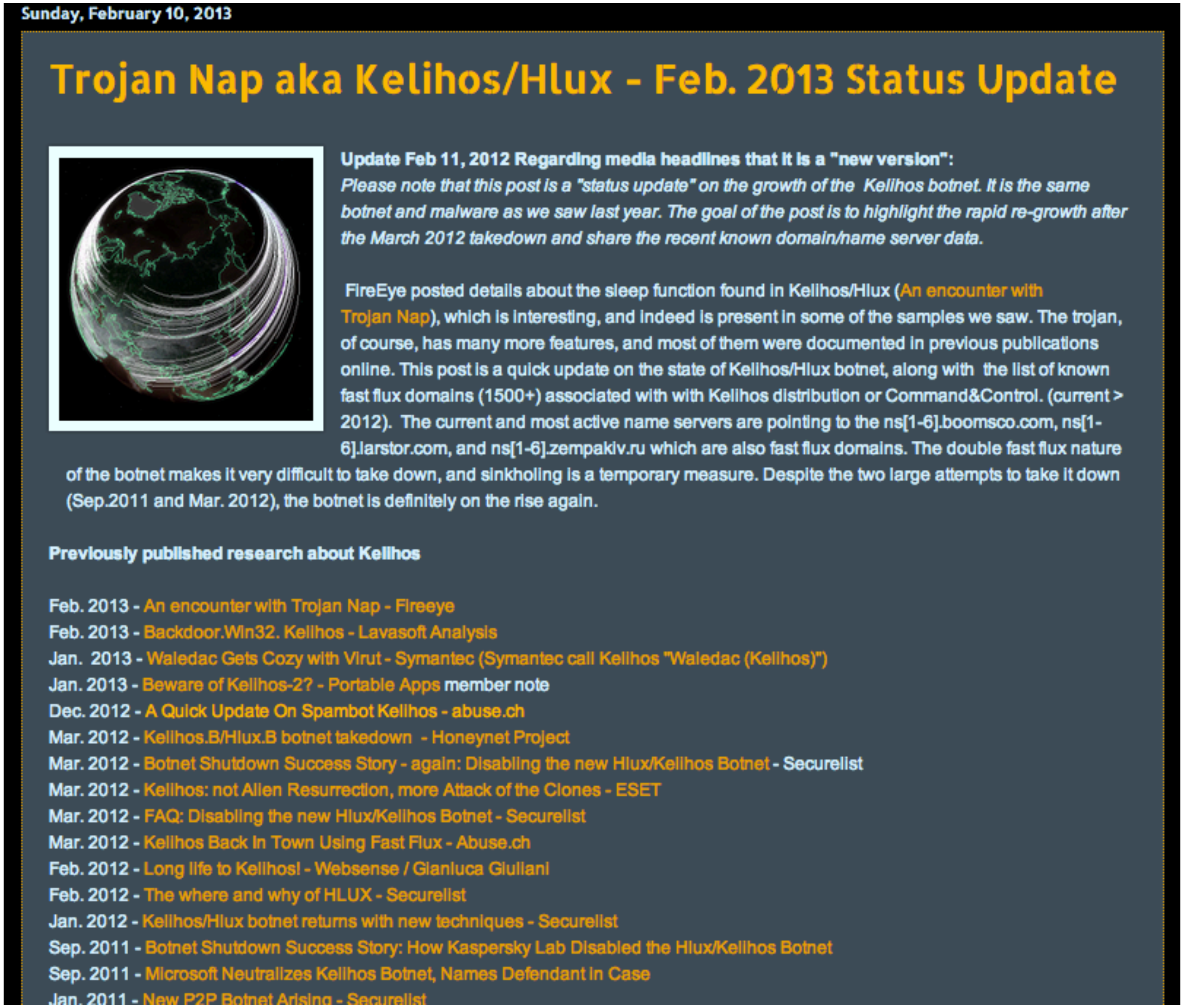
Welcome > Blog Home > Malware > Virut and Waledac Botnets Spamming from Shared Machines

VIRUT AND WALEDAC BOTNETS SPAMMING FROM SHARED MACHINES

by Brian Donohue Follow @TheBrianDonohue January 15, 2013, 7:38PM

In an analysis of Virut botnet samples, Symantec researchers observed the malware downloading Waledac variants, suggesting that the gangs responsible for each botnet may be cooperating with one another through some sort of affiliate program, or, at the very least, that the two threats coexist and function on single infected machines.

HTTP://WWW.DEEPENDRESEARCH.ORG/



Sunday, February 10, 2013

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 domain/name server data.

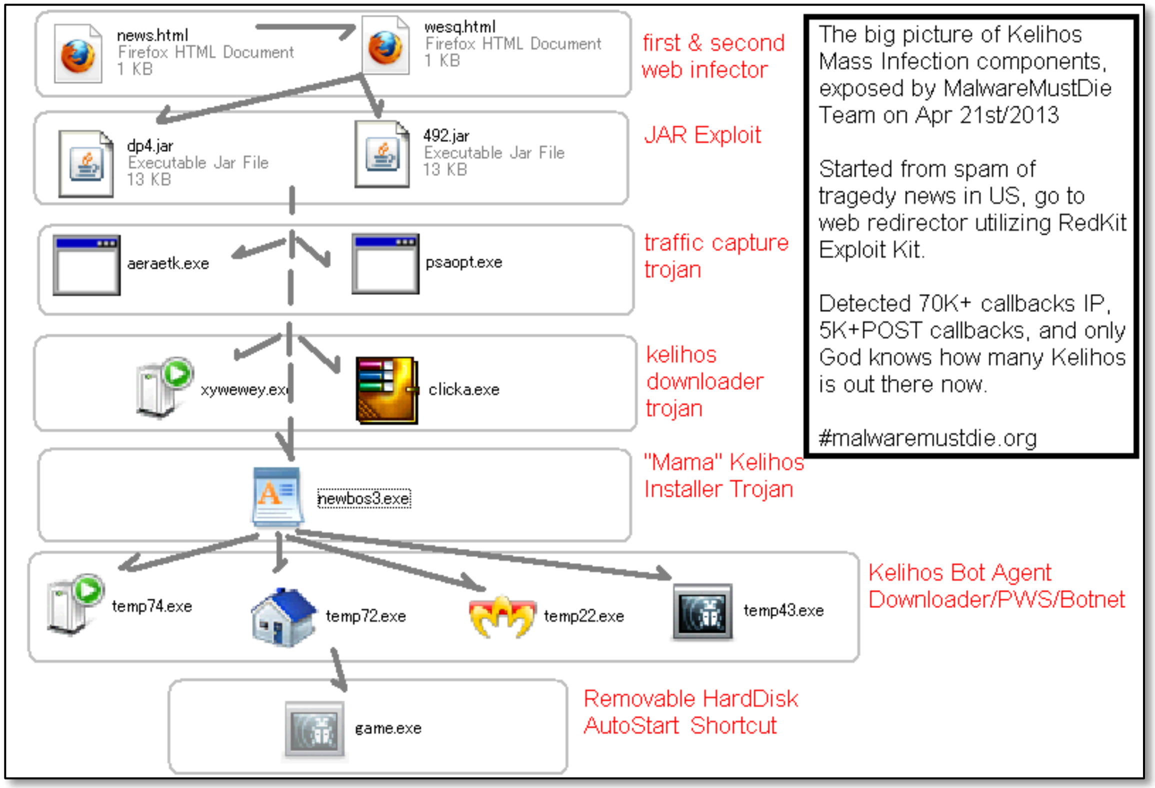
FireEye posted details about the sleep function found in Kelihos/Hlux (An encounter with Trojan Nap), which is interesting, and indeed is present in some of the samples we saw. The trojan, of course, has many more features, and most of them were documented in previous publications online. This post is a quick update on the state of Kelihos/Hlux botnet, along with the list of known fast flux domains (1500+) associated with with Kelihos distribution or Command&Control. (current > 2012). The current and most active name servers are pointing to the ns[1-6].boomsco.com, ns[1-6].larstor.com, and ns[1-6].zempakiv.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
Feb. 2013 - Backdoor.Win32. Kelihos - Lavasoft Analysis
Jan. 2013 - Waledac Gets Cozy with Virut - Symantec (Symantec call Kelihos "Waledac (Kelihos)")
Jan. 2013 - Beware of Kelihos-2? - Portable Apps member note
Dec. 2012 - A Quick Update On Spambot Kelihos - abuse.ch
Mar. 2012 - Kelihos.B/Hlux.B botnet takedown - Honeynet Project
Mar. 2012 - Botnet Shutdown Success Story - again: Disabling the new Hlux/Kelihos Botnet - Securelist
Mar. 2012 - Kelihos: not Alien Resurrection, more Attack of the Clones - ESET
Mar. 2012 - FAQ: Disabling the new Hlux/Kelihos Botnet - Securelist
Mar. 2012 - Kelihos Back in Town Using Fast Flux - Abuse.ch
Feb. 2012 - Long life to Kelihos! - Websense / Gianluca Giuliani
Feb. 2012 - The where and why of HLUX - Securelist
Jan. 2012 - Kelihos/Hlux botnet returns with new techniques - Securelist
Sep. 2011 - Botnet Shutdown Success Story: How Kaspersky Lab Disabled the Hlux/Kelihos Botnet
Sep. 2011 - Microsoft Neutralizes Kelihos Botnet, Names Defendant in Case
Jan. 2011 - New P2P Botnet Arising - Securelist

MALWAREMUSTDIE (PUHLEEZ!)

- April 20, 2013
- Kelihos dropped by Redkit?!
- Waledac/Kelihos operator has so far used Conficker, Fifesock, Virut, Redkit, ???…



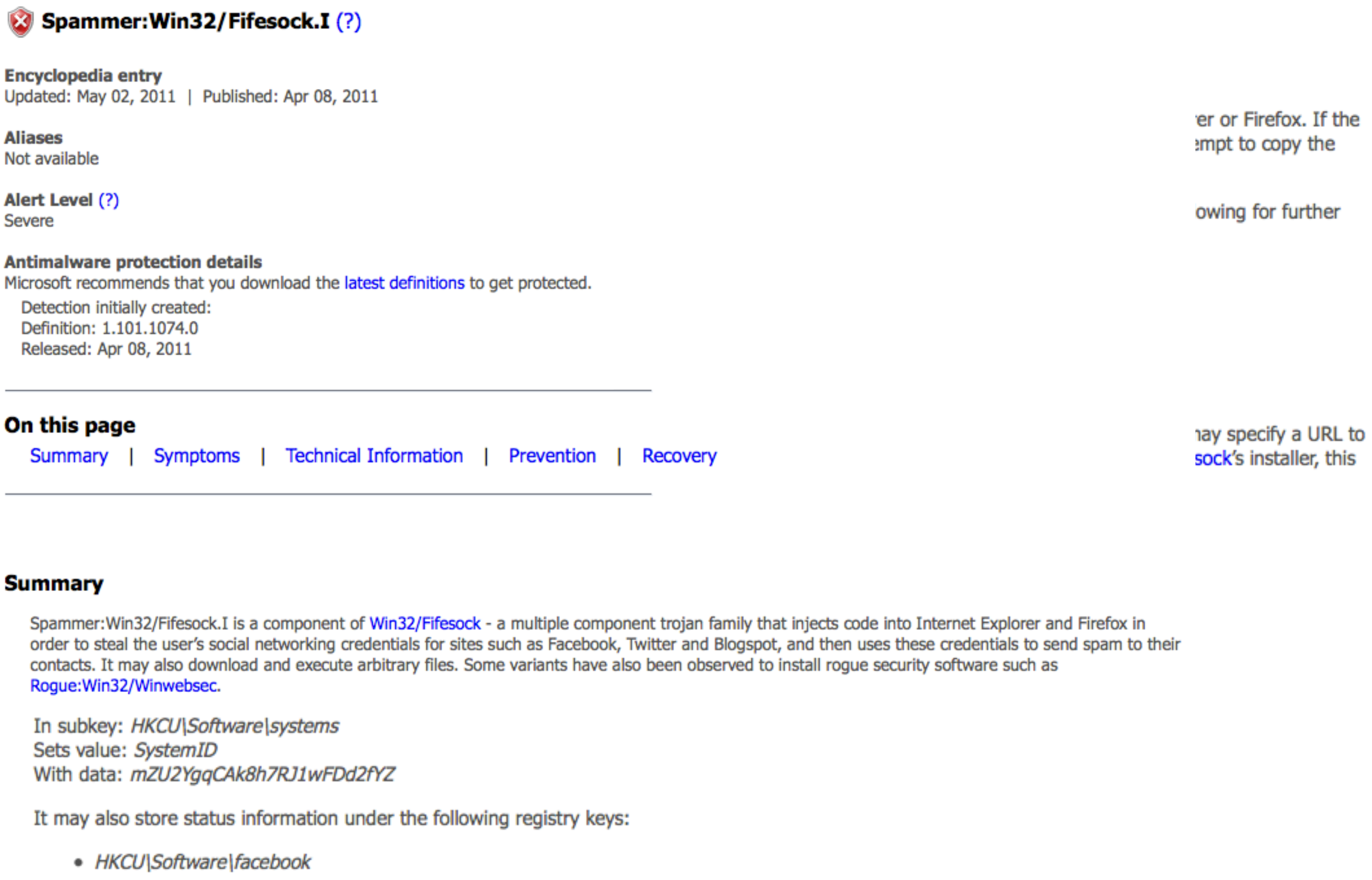
The big picture of Kelihos Mass Infection components, exposed by MalwareMustDie Team on Apr 21st/2013

Started from spam of tragedy news in US, go to web redirector utilizing RedKit Exploit Kit.

Detected 70K+ callbacks IP, 5K+POST callbacks, and only God knows how many Kelihos is out there now.

#malwaremustdie.org

MICROSOFT W32/FIFESOCK.I



Spammer:Win32/Fifesock.I (?)

Encyclopedia entry
Updated: May 02, 2011 | Published: Apr 08, 2011

Aliases
Not available

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

On this page
Summary | Symptoms | Technical Information | Prevention | Recovery

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.

In subkey: *HKCU\Software\systems*
Sets value: *SystemID*
With data: *mZU2YgqCAk8h7RJ1wFDd2fYZ*

It may also store status information under the following registry keys:

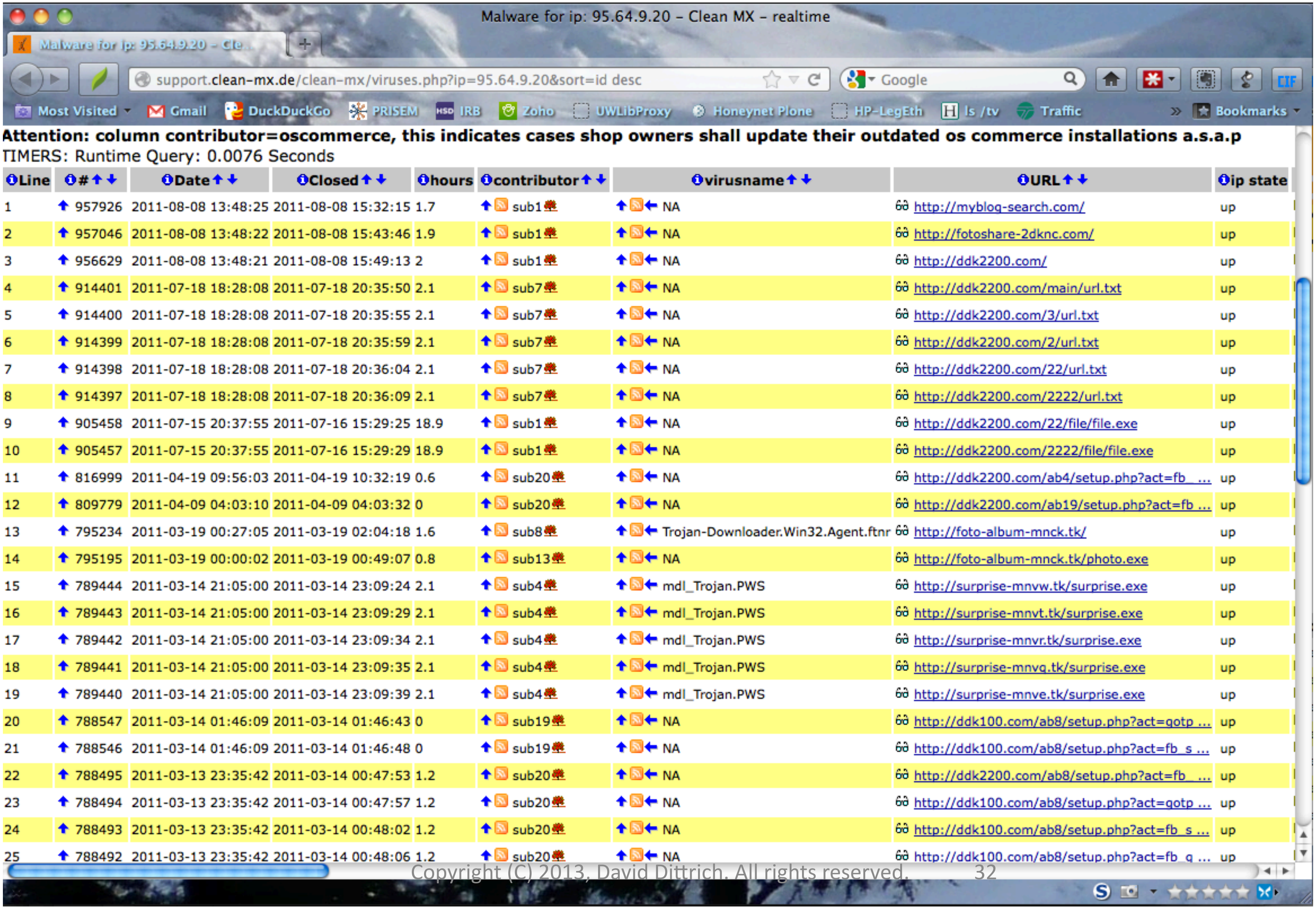
- *HKCU\Software\facebook*

er or Firefox. If the
empt to copy the

owing for further

nay specify a URL to
sock's installer, this

CLEANMX.DE DDK2200.COM

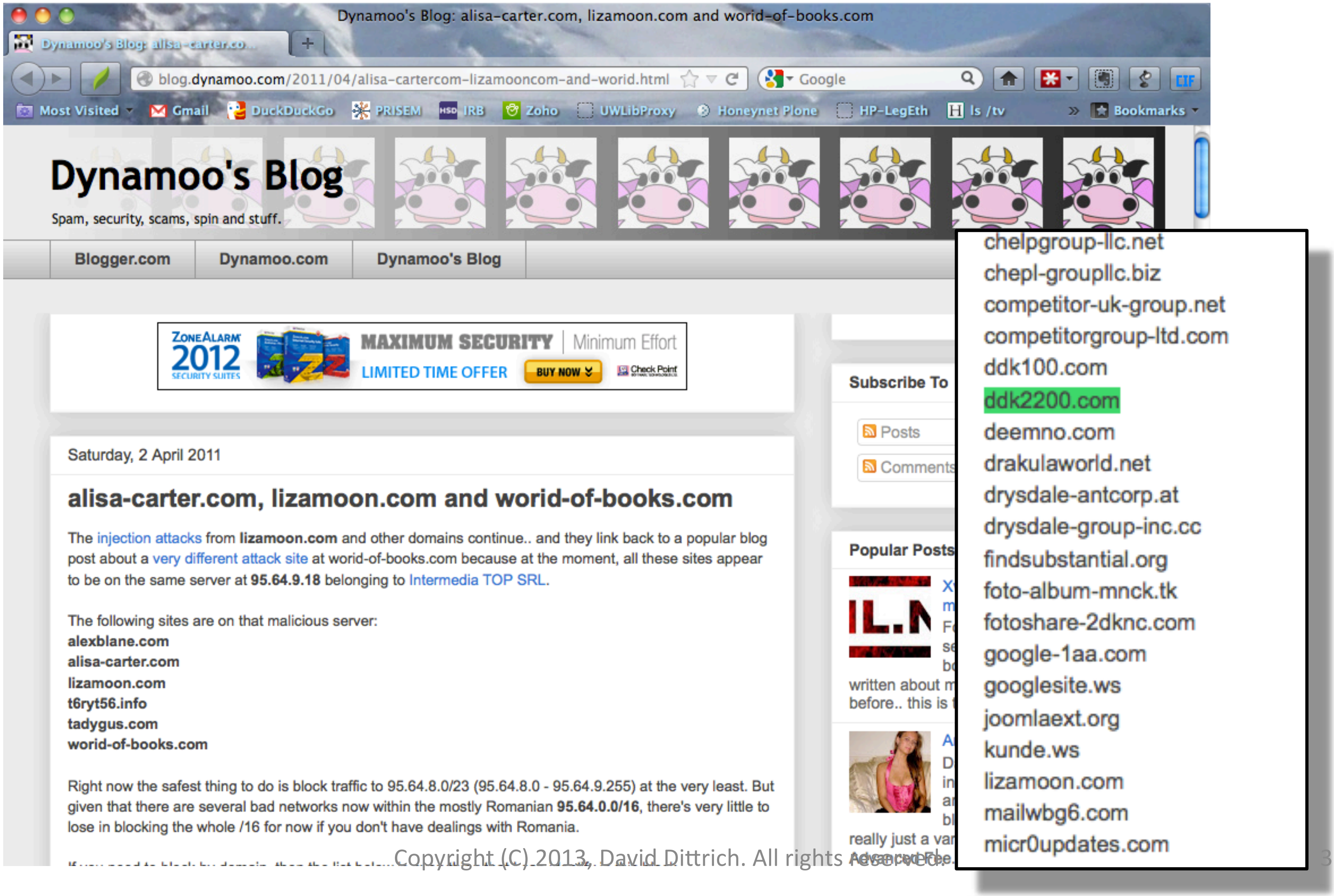

Malware for ip: 95.64.9.20 – Clean MX – realtime
Malware for ip: 95.64.9.20 – Cle...
support.clean-mx.de/clean-mx/viruses.php?ip=95.64.9.20&sort=id desc
Google
Most Visited
Gmail
DuckDuckGo
PRISEM
IRB
Zoho
UWLibProxy
Honeynet Plone
HP-LegEth
ls /tv
Traffic
Bookmarks

Attention: column contributor=oscommerce, this indicates cases shop owners shall update their outdated os commerce installations a.s.a.p

TIMERS: Runtime Query: 0.0076 Seconds

Line	#	Date	Closed	hours	contributor	virusname	URL	ip state
1	957926	2011-08-08 13:48:25	2011-08-08 15:32:15	1.7	sub1	NA	http://myblog-search.com/	up
2	957046	2011-08-08 13:48:22	2011-08-08 15:43:46	1.9	sub1	NA	http://fotoshare-2dknc.com/	up
3	956629	2011-08-08 13:48:21	2011-08-08 15:49:13	2	sub1	NA	http://ddk2200.com/	up
4	914401	2011-07-18 18:28:08	2011-07-18 20:35:50	2.1	sub7	NA	http://ddk2200.com/main/url.txt	up
5	914400	2011-07-18 18:28:08	2011-07-18 20:35:55	2.1	sub7	NA	http://ddk2200.com/3/url.txt	up
6	914399	2011-07-18 18:28:08	2011-07-18 20:35:59	2.1	sub7	NA	http://ddk2200.com/2/url.txt	up
7	914398	2011-07-18 18:28:08	2011-07-18 20:36:04	2.1	sub7	NA	http://ddk2200.com/22/url.txt	up
8	914397	2011-07-18 18:28:08	2011-07-18 20:36:09	2.1	sub7	NA	http://ddk2200.com/2222/url.txt	up
9	905458	2011-07-15 20:37:55	2011-07-16 15:29:25	18.9	sub1	NA	http://ddk2200.com/22/file/file.exe	up
10	905457	2011-07-15 20:37:55	2011-07-16 15:29:29	18.9	sub1	NA	http://ddk2200.com/2222/file/file.exe	up
11	816999	2011-04-19 09:56:03	2011-04-19 10:32:19	0.6	sub20	NA	http://ddk2200.com/ab4/setup.php?act=fb_ ...	up
12	809779	2011-04-09 04:03:10	2011-04-09 04:03:32	0	sub20	NA	http://ddk2200.com/ab19/setup.php?act=fb ...	up
13	795234	2011-03-19 00:27:05	2011-03-19 02:04:18	1.6	sub8	Trojan-Downloader.Win32.Agent.ftnr	http://foto-album-mnck.tk/	up
14	795195	2011-03-19 00:00:02	2011-03-19 00:49:07	0.8	sub13	NA	http://foto-album-mnck.tk/photo.exe	up
15	789444	2011-03-14 21:05:00	2011-03-14 23:09:24	2.1	sub4	mdl_Trojan.PWS	http://surprise-mnvw.tk/surprise.exe	up
16	789443	2011-03-14 21:05:00	2011-03-14 23:09:29	2.1	sub4	mdl_Trojan.PWS	http://surprise-mnvt.tk/surprise.exe	up
17	789442	2011-03-14 21:05:00	2011-03-14 23:09:34	2.1	sub4	mdl_Trojan.PWS	http://surprise-mnvr.tk/surprise.exe	up
18	789441	2011-03-14 21:05:00	2011-03-14 23:09:35	2.1	sub4	mdl_Trojan.PWS	http://surprise-mnvq.tk/surprise.exe	up
19	789440	2011-03-14 21:05:00	2011-03-14 23:09:39	2.1	sub4	mdl_Trojan.PWS	http://surprise-mnve.tk/surprise.exe	up
20	788547	2011-03-14 01:46:09	2011-03-14 01:46:43	0	sub19	NA	http://ddk100.com/ab8/setup.php?act=gotp ...	up
21	788546	2011-03-14 01:46:09	2011-03-14 01:46:48	0	sub19	NA	http://ddk100.com/ab8/setup.php?act=fb_s ...	up
22	788495	2011-03-13 23:35:42	2011-03-14 00:47:53	1.2	sub20	NA	http://ddk2200.com/ab8/setup.php?act=fb_ ...	up
23	788494	2011-03-13 23:35:42	2011-03-14 00:47:57	1.2	sub20	NA	http://ddk100.com/ab8/setup.php?act=gotp ...	up
24	788493	2011-03-13 23:35:42	2011-03-14 00:48:02	1.2	sub20	NA	http://ddk100.com/ab8/setup.php?act=fb_s ...	up
25	788492	2011-03-13 23:35:42	2011-03-14 00:48:06	1.2	sub20	NA	http://ddk100.com/ab8/setup.php?act=fb_q ...	up

DYNAMOO LINKS
FIFESOCK TO LIZAMOON


Dynamoo's Blog: alisa-carter.com, lizamoon.com and worid-of-books.com
Dynamoo's Blog: alisa-carter.co...
blog.dynamoo.com/2011/04/alisa-cartercom-lizamooncom-and-worid.html
Google
Most Visited
Gmail
DuckDuckGo
PRISEM
IRB
Zoho
UWLibProxy
Honeynet Plone
HP-LegEth
Is /tv
Bookmarks
Dynamoo's Blog
Spam, security, scams, spin and stuff.
Blogger.com
Dynamoo.com
Dynamoo's Blog
ZONEALARM 2012 SECURITY SUITES
MAXIMUM SECURITY | Minimum Effort
LIMITED TIME OFFER
BUY NOW
Check Point
Subscribe To
Posts
Comments
Popular Posts

Saturday, 2 April 2011

alisa-carter.com, lizamoon.com and worid-of-books.com

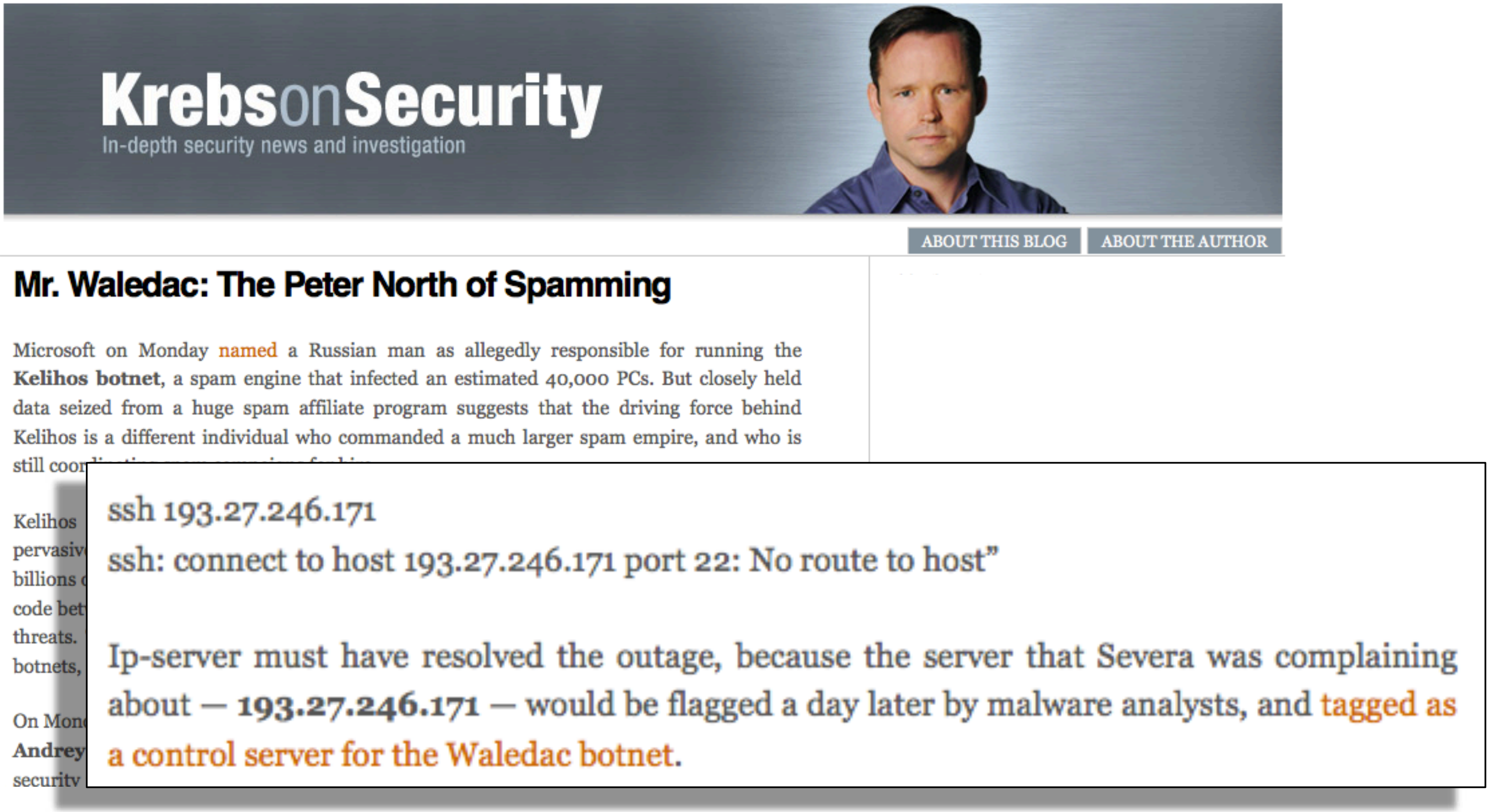
The injection attacks from **lizamoon.com** and other domains continue.. and they link back to a popular blog post about a very different attack site at worid-of-books.com because at the moment, all these sites appear to be on the same server at **95.64.9.18** belonging to Intermedia TOP SRL.

The following sites are on that malicious server:
alexblane.com
alisa-carter.com
lizamoon.com
t6ryt56.info
tadygus.com
worid-of-books.com

Right now the safest thing to do is block traffic to 95.64.8.0/23 (95.64.8.0 - 95.64.9.255) at the very least. But given that there are several bad networks now within the mostly Romanian **95.64.0.0/16**, there's very little to lose in blocking the whole /16 for now if you don't have dealings with Romania.

chelpgroup-llc.net
chepl-groupllc.biz
competitor-uk-group.net
competitorgroup-ltd.com
ddk100.com
ddk2200.com
deemno.com
drakulaworld.net
drysdale-antcorp.at
drysdale-group-inc.cc
findsubstantial.org
foto-album-mnck.tk
fotoshare-2dknc.com
google-1aa.com
googlesite.ws
joomlaext.org
kunde.ws
lizamoon.com
mailwbg6.com
micr0updates.com

KREBSONSECURITY



Mr. Waledac: The Peter North of Spamming

Microsoft on Monday named a Russian man as allegedly responsible for running the **Kelihos botnet**, a spam engine that infected an estimated 40,000 PCs. But closely held data seized from a huge spam affiliate program suggests that the driving force behind Kelihos is a different individual who commanded a much larger spam empire, and who is still coor

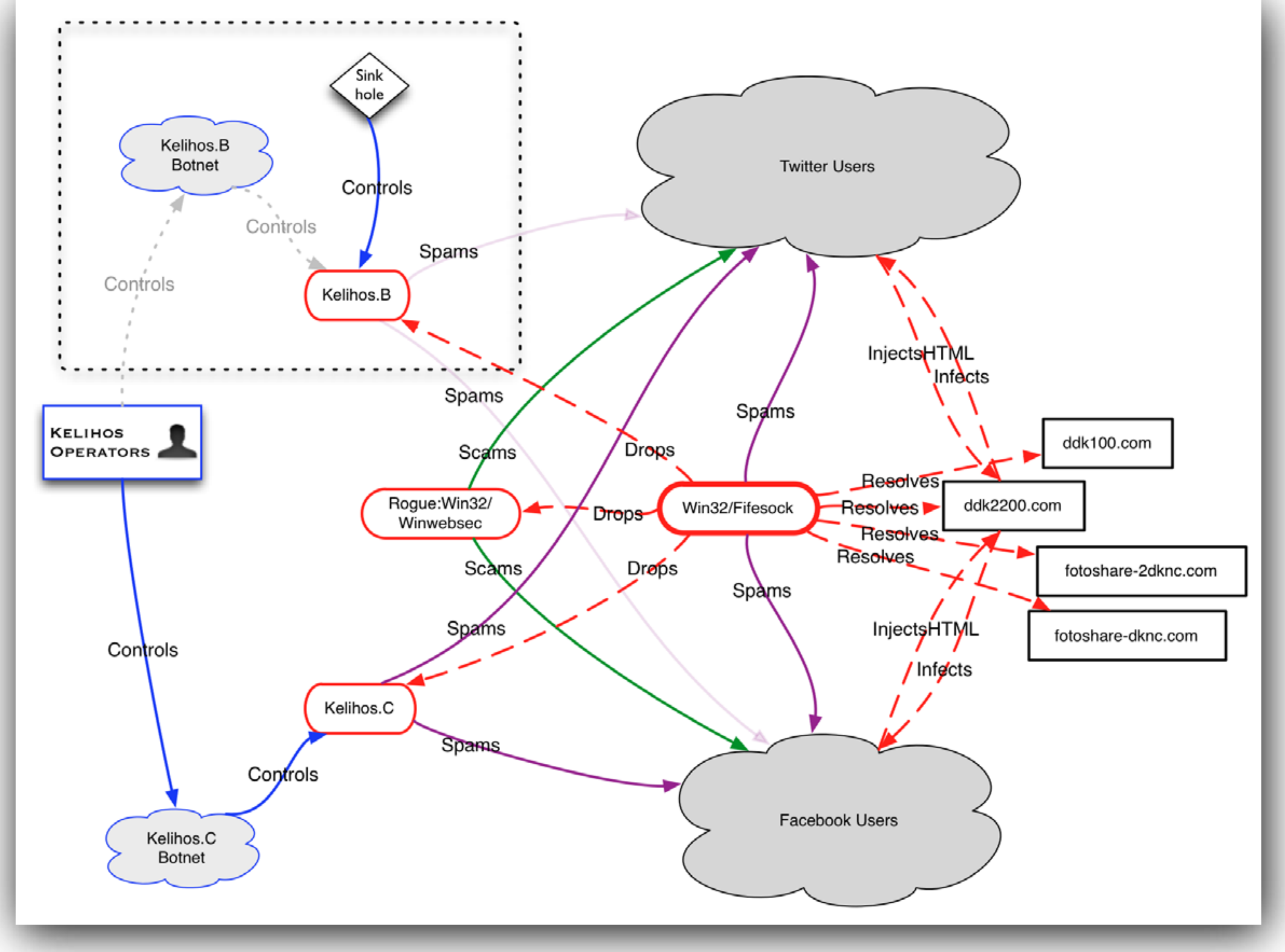
Kelihos
pervasiv
billions
code bet
threats.
botnets,

On Mon
Andrey
security

```
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.

Roles & Relationships



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

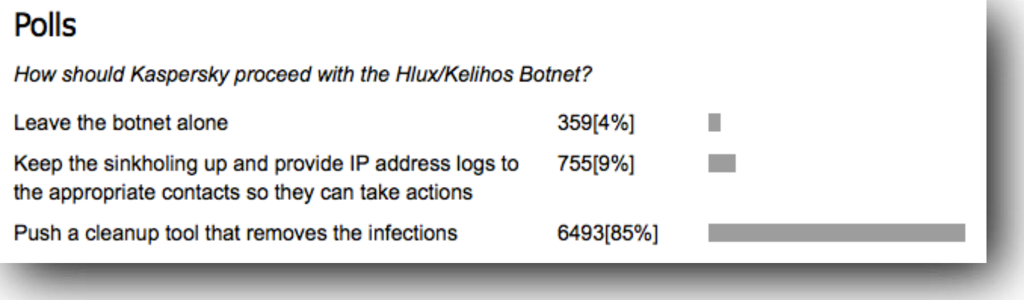
- A.k.a., Spam-Mailbot.c
- First reported early 2006
- First detailed RE reports early 2007
- Central C&C servers hosted on non-cooperative "bullet-proof" hosting companies
- Microsoft *Operation b107* on March 6, 2011
  - Involves ex parte TRO, search warrants, US Marshall assistance, taking out core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



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%]	▬▬▬▬▬▬▬▬▬▬

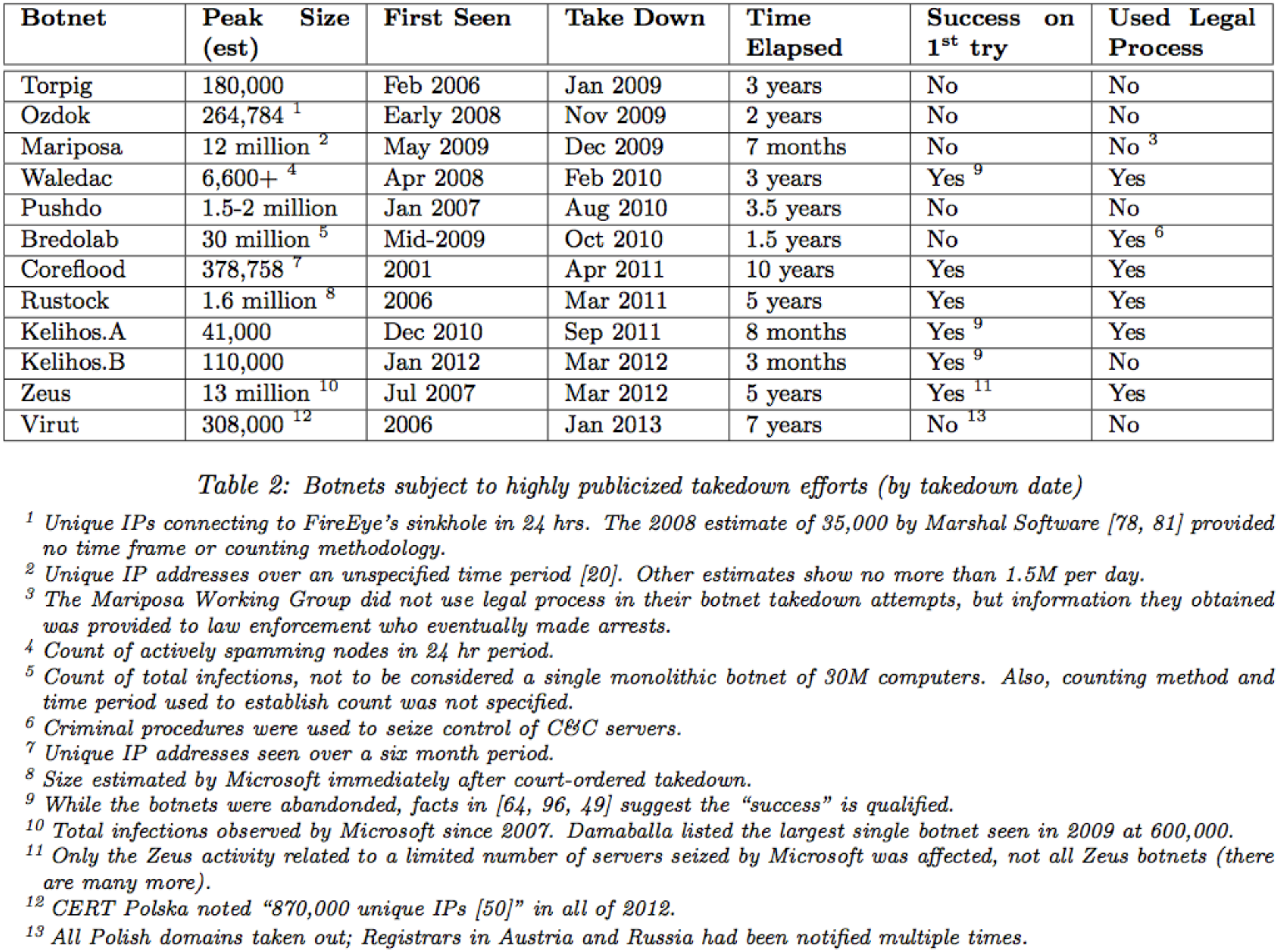
Virut

- 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)

Virut

- 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



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).*

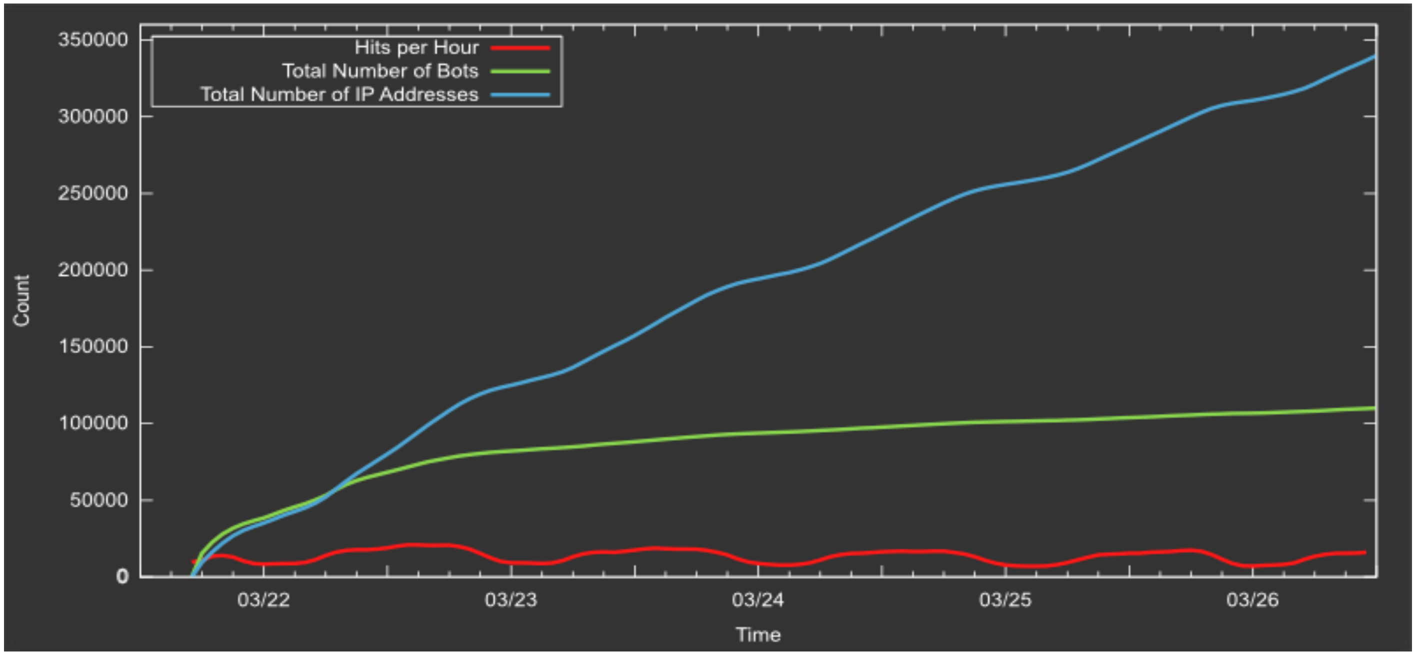
[12] *CERT Polska noted "870,000 unique IPs [50]" in all of 2012.*

[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

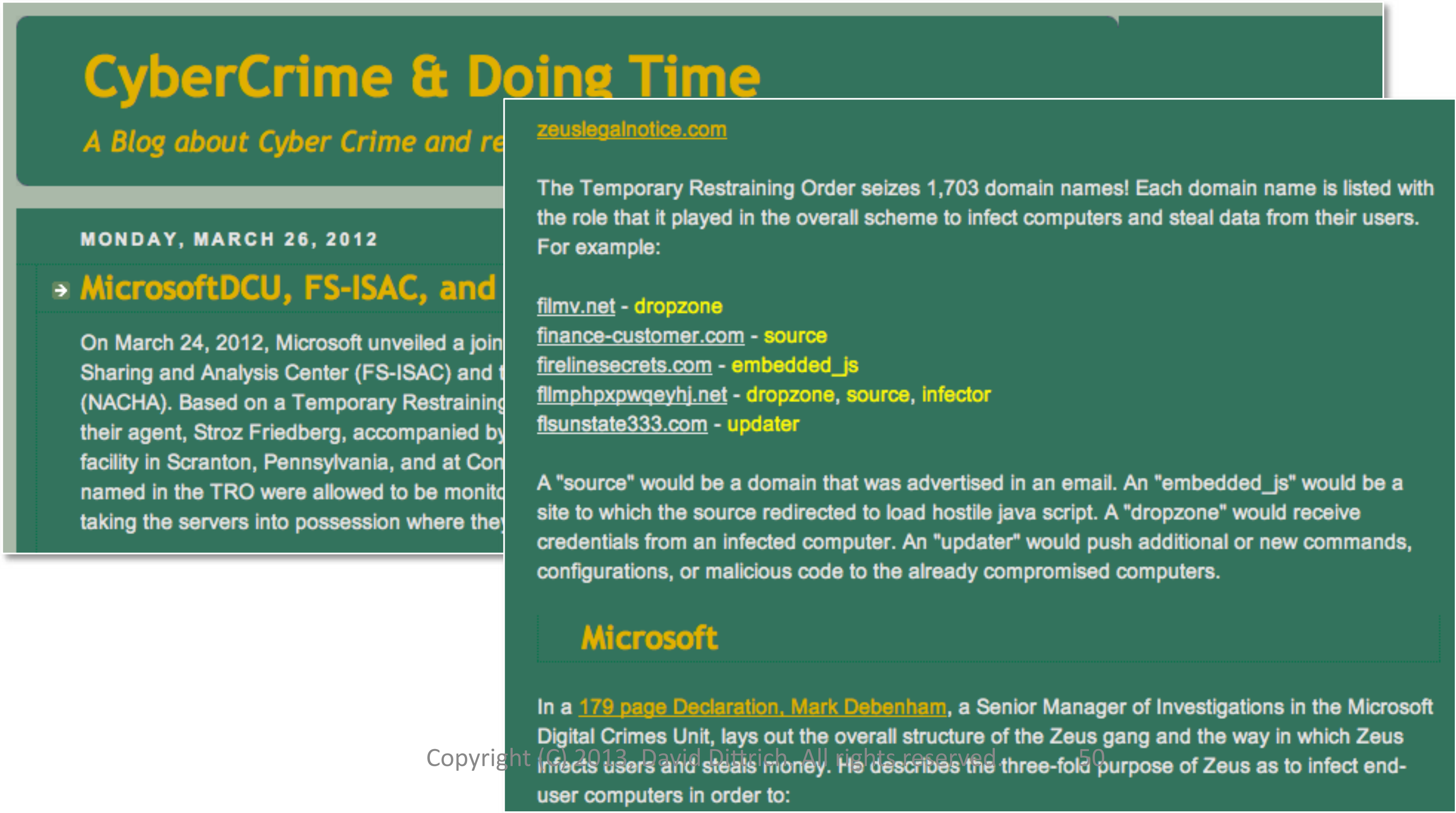
- Size estimates vary by orders of magnitude
  - Incentive to inflate numbers
  - Easy to exploit IP over-counting and conflate with “infections”



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



CyberCrime & Doing Time

A Blog about Cyber Crime and re

MONDAY, MARCH 26, 2012

MicrosoftDCU, FS-ISAC, and

On March 24, 2012, Microsoft unveiled a join
Sharing and Analysis Center (FS-ISAC) and t
(NACHA). Based on a Temporary Restraining
their agent, Stroz Friedberg, accompanied by
facility in Scranton, Pennsylvania, and at Con
named in the TRO were allowed to be monito
taking the servers into possession where they

zeuslegalnotice.com

The Temporary Restraining Order seizes 1,703 domain names! Each domain name is listed with the role that it played in the overall scheme to infect computers and steal data from their users. For example:

filmv.net - dropzone
finance-customer.com - source
firelinesecrets.com - embedded_js
fllmphpxpwqeyhj.net - dropzone, source, infector
flsunstate333.com - updater

A "source" would be a domain that was advertised in an email. An "embedded_js" would be a site to which the source redirected to load hostile java script. A "dropzone" would receive credentials from an infected computer. An "updater" would push additional or new commands, configurations, or malicious code to the already compromised computers.

Microsoft

In a 179 page Declaration, Mark Debenham, a Senior Manager of Investigations in the Microsoft Digital Crimes Unit, lays out the overall structure of the Zeus gang and the way in which Zeus infects users and steals money. He describes the three-fold purpose of Zeus as to infect end-user computers in order to:

OBSERVATIONS (CONTINUED)

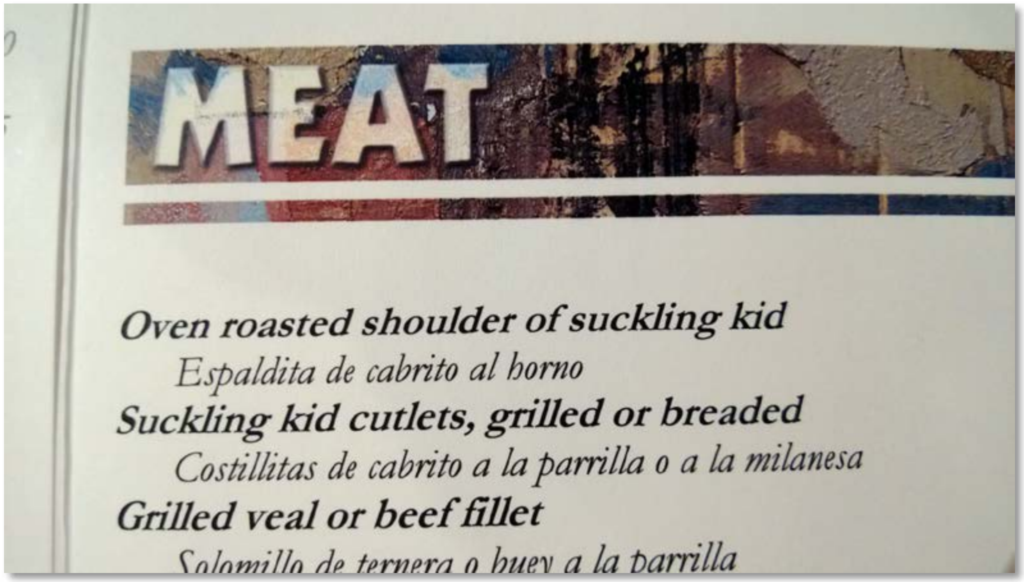
- All(?) takedowns combining legal process and technical methods succeeded on first try
- (…or did they really *all fail*?)
  - Those using *only* technical means, or relying on *cooperation* of all parties involved, did not
  - It's not always about taking the botnet down
  - Today's most sophisticated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



MEAT

Oven roasted shoulder of suckling kid
Espaldita de cabrito al horno
Suckling kid cutlets, grilled or breaded
Costillitas de cabrito a la parrilla o a la milanesa
Grilled veal or beef fillet
Solomillo de ternera o buey a la parrilla

Good read: "Hackers: Crime and the Digital Sublime," by Paul A. Taylor, Routledge Press, 1999, ISBN 0-415-18072-4

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

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
  University of Washington
  dittrich *at* uw *dot* edu
  http://staff.washington.edu/dittrich/

Slides available at: http://staff.washington.edu/dittrich/talks/nanog59/