Taking Down Botnets - Background

David Dittrich <dittrich@speakeasy.net>

April 10, 2015

1 Introduction

While some botnet takedowns have been done with involvement of national and international law enforcement agencies, these agencies do not perform these takedowns by themselves: they rely on support from private sector actors, be they self-proclaimed *researchers*, academics, or corporate employees. Many other takedowns in the past have been performed using only technical means by private sector actors, often without any involvement with law enforcement or use of legal process, and without any formally accepted code of conduct, standards for ethical evaluation, or external review [6, 13, 11].

Aggressively countering and disrupting botnets has risks. As botnets get more and more dangerous, so do the risks of trying to aggressively disrupt and disable them. Consider two examples:

- The *Mariposa* (or *Butterfly*) botnet takedown was initially deemed a success, but then temporarily reversed when the operator regained control and turned the botnet back on the Mariposa Working Group members who were fighting for control. The hacker then, "launched a distributed denial of service attack against Defense Intelligence's Web site, using more than a million PCs the gang had managed to corral back into the Mariposa botnet. That assault, which forced the infected PCs to flood the company's site with junk Web traffic, not only knocked Defence Intelligence offline, but took out networks of several other organizations that were using the same Internet service provider, including a local university and a few government agencies in Ottawa [19]." Had it not been for a mistake during the fight, the operator might have never been caught. The damage caused by the attack was used in sentencing, but do the ends justify the means (and the luck involved), or should such takedowns be more carefully planned and contingencies considered before even initiating such an operation?

- The takedown of the Kelihos botnet in 2012 also appeared at first to be a wild success, but the next day it was clear the criminals behind it had simply reconstituted their network and continued apace. While much engineering effort was spent on attacking the command and control to sinkhole the computers infected with Kelihos, little attention was paid to the distribution mechanism, which allowed the botnet to be reconstituted in a matter of hours for a likely cost of $10,000 or less, possibly two orders of magnitude less than the market rate for the time spent by the engineers who performed the sinkholing [15]. These same entities who took shortcuts then called for changes in laws to grant them authority to go even further [22], which raises serious red flags about the need to better understand such legislative changes before making them.

Ignoring the mistakes of the past, and the risks associated with disruptive actions, may put the public at an unacceptable risk of as harm. Anger and frustration at the growth of computer crime cannot be allowed to blind those purporting to do good such that they end up causing unnecessary harm to innocent third parties who may be unaware their computing resources are even involved. Knowing how to avoid accidental counterstrike damage, or taking insufficient measures to obtain a stated desired outcome, are key elements that are prerequisite to changing any laws or granting any new authorities that would allow the private sector to freely engage in such aggressive takedowns.

2 Principle Issues

There are three main issues related to aggressive responses to cybercrime, including botnet takedowns. The first has to do with technical aspects, such as defining terminology and what actions are being taken (regardless of who takes them). The second issue has to do with who is acting, under what authority, and under what supervision and guidance. The third issue has to do with evaluating the ethical and legal issues and deciding when and how to move forward in countering criminal activity on computer resources that may be owned and operated by innocent third parties.

The technical fundamentals of botnet takedowns, including case studies of the takedown or takeover of *Torpig* (a.k.a., *Mebroot*, *Sinowal* and *Anserin*), *Ozdok* (a.k.a., *Mega-D*), *Mariposa*, *Waledac*, *Bredolab*, *Pushdo/Cutwail* (a.k.a., *Pandex*), *Rustock*, *Coreflood*, *Kelihos* (a.k.a., *Hlux* and *Darlev*) and *Zeus* (a.k.a., *Kneber*, *NTOS*, and *Wsnpoem*) was presented in 2012 [8]. Of these, the *Mariposa*, *Bredolab* and *Coreflood* takedowns involved law enforcement, *Waledac*, *Rustock*, *Kelihos*, and *Zeus* involved civil legal process, and the rest were done by the private sector using solely technical means and cooperation of sites who owned some of the command and control resources. (Other botnet takedown case studies can be found in works dealing with the ethical issues of private sector researchers doing aggressive computer security research projects involving manipulation of botnets [5, 13].)

In terms of ethical analysis, work sponsored by the Department of Homeland Defense known as the *Menlo Report* [2] has informed presentations on botnet takedowns at the Microsoft Digital Crimes Community meetings in Barcelona (February 2013) [12] and Singapore (March 2014) [15], the North American Network Operators (NANOG) meeting 59 (October 2013) [10], and CyCon 2014 [14].

The Companion document to the Menlo Report borrows from case studies examining the ethical principles used by academic and private sector actors who are engaged in fighting cyber crime using technical (takedown) methods [6, 13]. These are some of the key players in takedowns past and future, so learning lessons from both success and failure is crucial. The methodology of stakeholder analysis developed by the Menlo Report Working Group has proven useful and has been applied to analyzing decisions about remote mitigation of botnets [16], evaluating the ethics of research involving *social honeypots* to counter criminal activity targeting social network users [9], as the foundation for a *Code of Conduct* for the Honeynet Project [23] and a blog post covering *Frequently Asked Questions* about the Kelihos.B botnet takedown in 2012 [7]. A group has been formed (known as the "Cybercrime Response Advisory Group", or *CRAG*) that can do before-the-fact and after-action review of aggressive responses to cybercrime. This group can hopefully guide future takedown efforts by both law enforcement and the private sector to cause minimal harm to innocent third parties (or *friendly-fire* accidents), and maximize achieving aims of justice against cybercrime. Much more research into this topic area has been called for by many [24].

3 Conclusions

There has been an increasing number of botnet takedown actions using both civil legal process and criminal process (e.g., Microsoft's *Bladabindi* and *Jenxcus* takedowns [3, 18] the *Game Over Zeus* and *Cryptolocker* takedown by combined private sector and U.S. and U.K. law enforcement with indictment of a Russian suspect [1], the *Lecpetex* botnet takedown by Facebook with arrests by Greek police [17, 20], and the *Shylock* botnet takedown by the U.K. National Crime Agency, FBI, German Federal Police, and the European Cyber Crime Center (EC3) [21].

More work needs to be done on establishing norms of behavior on the internet, normalize legal procedures and cooperation among international law enforcement, and encouraging the private sector who are being victimized to work together within their respective sectors, as well as bringing evidence to law enforcement and working hand in hand to strengthen the legal system, not bypass it and take matters into the private sector's own hands. Some elements that a viable framework should include are: handling *deconfliction* issues between takedown by separate entities; providing before- and after-action review to learn from, and pass along, lessons of both successes and failures; favoring government over private sector action at the extreme end of the Active Response Continuum; favoring civil/criminal process over extra-judicial private sector action; and following a virtue ethics approach of *integrity* (as defined by Stephen Carter [4]) and "Right Action" justification for the actions being taken [14].

References

[1] Warwick Ashford. Russian cyber crime kingpin sought after worldwide server raids. http://www.computerweekly.com/news/2240221821/Russian-cyber-crime-kingpin-sought-after-wordwide-server-raids, June 2014.

[2] Michael Bailey, David Dittrich, Erin Kenneally, and Douglas Maughan. The Menlo Report. *Security & Privacy, IEEE*, 10(2):71–75, March/April 2012. http://www.caida.org/publications/papers/2012/menlo_report/menlo_report.pdf.

[3] Richard Boscovich. Microsoft takes on global cybercrime epidemic in tenth malware disruption. http://blogs.technet.com/b/microsoft_blog/archive/2014/06/30/microsoft-takes-on-global-cybercrime-epidemic-in-tenth-malware-disruption.aspx, June 2014.

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

[5] David Dittrich and Erin Kenneally (eds.). Applying Ethical Principles to Information and Communication Technology Research: A Companion to the Department of Homeland Security Menlo Report. http://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCOMPANION-20120103-r731.pdf, January 2012.

[6] D. Dittrich, M. Bailey, and S. Dietrich. Building An Active Computer Security Ethics Community. *Security Privacy, IEEE*, 9(4):32–40, July/August 2011. https://staff.washington.edu/dittrich/papers/ieee-snp-ethics-2011.pdf.

[7] David Dittrich. FAQ on Kelihos.B/Hlux.B sinkholing. http://www.honeynet.org/node/836, March 2012.

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

[9] David Dittrich. The Ethics of Social Honeypots. Available at SSRN http://ssrn.com/abstract=2184997, November 2012.

[10] David Dittrich. Offensive Anti-Botnet – So you want to take over a botnet... http://www.youtube.com/watch?v=zqUL1mUEvGg&list=PLO8DR5ZGla8j7_jnNYY3d8JBOHfdXe85X, http://staff.washington.edu/dittrich/talks/nanog59/, October 2013. Presentation to the North American Network Operators Group (NANOG) meeting 59.

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

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

[13] David Dittrich, Michael Bailey, and Sven Dietrich. Towards Community Standards for Ethical Behavior in Computer Security Research. Technical Report CS 2009-01, Stevens Institute of Technology, April 2009. http://staff.washington.edu/dittrich/papers/dbd2009tr1/.

[14] David Dittrich and Katherine Carpenter. Protecting Property in Cyberspace using "Force": Legal and Ethical Justifications. https://ccdcoe.org/cycon/2014/app.html (04.06.14, Strategy and Law track), June 2014. Presentation to the NATO CCDCOE Cyber Conflict 2014 conference.

[15] David Dittrich and Katherine Carpenter. The Legal and Ethical Challenges with Aggressive Computer Security Research and Operations Actions. http://staff.washington.edu/dittrich/talks/dcc2013_dittrich_botnets.pdf, March 2014. Presentation to Microsoft Digital Crimes Consortium 2014 meeting.

[16] David Dittrich, Felix Leder, and Tillmann Werner. A Case Study in Ethical Decision Making Regarding Remote Mitigation of Botnets. In *Proceedings of the 14th International Conference on Financial Cryptograpy and Data Security*, FC'10, pages 216–230, Berlin, Heidelberg, 2010. Springer-Verlag. http://staff.washington.edu/dittrich/papers/wecsr2010-botethics-dlw.pdf.

[17] Facebook. Taking Down the Lecpetex Botnet. https://www.facebook.com/notes/protect-the-graph/taking-down-the-lecpetex-botnet/1477464749160338, July 2014.

[18] Dennis Fisher. Latest Microsoft Malware Takedown Causes Waves in Security Community. http://threatpost.com/latest-microsoft-malware-takedown-causes-waves-in-security-community/106939, June 2014.

[19] Brian Krebs. 'Mariposa' Botnet Authors May Avoid Jail Time. http://krebsonsecurity.com/2010/03/mariposa-botnet-authors-may-avoid-jail-time/, March 2010.

[20] Michael Mimoso. Facebook Carries Out Lecpetex Botnet Takedown. http://threatpost.com/facebook-carries-out-lecpetex-botnet-takedown/107096, July 2014.

[21] Michael Mimoso. International Authorities Take Down Shylock Banking Malware. http://threatpost.com/international-authorities-take-down-shylock-banking-malware/107122, July 2014.

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

[23] The Honeynet Project. Code of Conduct. https://honeynet.org/codeofconduct, March 2012.

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