Botnet Takedown Initiatives: A Taxonomy and Performance Model

Reza Shirazi

" Men rise from one ambition to another: first, they seek to secure themselves against attack, and then they attack others. "

Niccolò di Bernardo dei Machiavelli (1469–1527)
Historian, politician, diplomat, philosopher, and humanist

Botnets have become one of the fastest-growing threats to the computer systems, assets, data, and capabilities relied upon by individuals and organizations worldwide. Botnet takedown initiatives are complex and as varied as the botnets themselves. However, there is no comprehensive database of botnet takedowns available to researchers and practitioners, nor is there a theoretical model to help predict the success or failure of future takedown initiatives. This article reports on the author's ongoing research that is contributing to both of these challenges and introduces a set of hypotheses relating to the performance of botnet takedown initiatives. In addition to researchers, the article will be of particular interest to personnel in technical, legal, and management functions of organizations interested in improving the quality of their communications and accelerating decision making for the purpose of launching and operating botnet takedown initiatives. It will also be of interest to entrepreneurs who wish to launch and grow cybersecurity ventures that provide solutions to botnet and malware threats.

Introduction

Botnets are a persistent threat to all Internet users. They are networks of computers infected with malicious software that are connected over the Internet and can be instructed to carry out specific tasks – typically without the owners of those computers knowing it (Nadji et al., 2013; Plohmann et al., 2011; Whitehouse, 2014). Those who control botnets use them to steal identities, personal and financial information, illicitly gain access to bank accounts; distribute spam e-mails; shut down websites by overwhelming them with traffic (i.e., distributed denial-of-service or DDoS attacks); launch new custom-made botnets; or spread malware and ransomware (Cremonini & Riccardi, 2009; Plohmann et al., 2011; Zeidanloo et al., 2010).

Over the last 20 years, botnets have developed "from a subject of curiosity to highly sophisticated instruments" for illegal activities (Czosseck et al., 2011). Botnets increase the computing resources available to cybercriminals exponentially without revealing their identities (Feily et al., 2009; Whitehouse, 2014). Stealth, resilient, and cost-effective botnets have been designed to operate using general overlay networks such as those offered by Skype (Nappa, et al., 2010).

Botnets are difficult to track, disrupt, and dismantle because they operate in various time zones, languages, and laws (Abu Rajab et al., 2006; Schaffer, 2006). Botnet takedown initiatives refer to the actions that lead to the identification and disruption of the botnet's command-and-control infrastructure. The literature on botnet takedowns includes studies on accelerating the botnet takedown process (Nadji et al., 2013), employing botnet takedown methods (Dagon et. al., 2007; Freiling et al., 2005), minimizing botnet profitability (Tiirmaa-Klaar et al., 2013a), and detecting botnets (Dittrich, 2012; Nappa et al., 2010; Zeidanloo et al., 2010; Zhao et al., 2009). Studies have also looked at the managerial implications of botnet takedowns (Borrett et al., 2013; Scully, 2013), botnet lifecycles (Kok & Kurz, 2011), botnet types (Czosseck et al., 2011; Dagon et al., 2007), and practices to prevent and respond to botnet threats (Plohmann et al., 2011). However, there is no comprehensive database of botnet takedowns available to researchers and practitioners, nor is there a theoretical model to help predict the success or failure of future takedown initiatives. This article reports on the author's ongoing research that is contributing to both of these challenges and introduces a set of hypotheses relating to the performance of botnet takedowns.

Developing a Database of Botnet Takedown Initiatives

As of late 2014, a readily accessible comprehensive database on botnet takedown initiatives was not available. Responding to the need to develop such a resource, a Google search (using keywords such as "botnet takedown", "botnet disruption", and "botnet dismantled") was conducted, which returned data from various sources, including: recent hearings on crime and terrorism (e.g., Whitehouse, 2014); lists of botnets that appear in large public websites (e.g., Wikipedia, 2014); websites of major IT firms (e.g., Microsoft), cybersecurity institutes (e.g., Symantec), and news agencies; and academic journals and conference proceedings.

Based on the data from these sources, a preliminary database of 19 botnet takedown initiatives was created. The database is being developed and maintained by the Technology Innovation Management program (TIM; timprogram.ca) at Carleton University in Ottawa, Canada, and it will be made publicly available once it is sufficiently mature. Table 1 summarizes the botnets and malware listed in the database, including each botnet's name (alias), its date of discovery, the date its takedown initiative began, its estimated size, and its purpose or tasks performed. However, the full database captures the following additional dimensions about the botnets and their associated takedown initiatives: unique features, means of dissemination, vulnerabilities exploited, responsible entity, impact, takedown leader, takedown process, involvement of authorities, legal issues, and timeline of key dates. As research progress and understanding of consequential dimensions grows, these dimensions will be refined.

Botnet Takedown Performance Model

Informed by the evolving database on botnet takedown initiatives described in the previous section, this study proposes a botnet takedown model to enable diverse, proficient individuals working in IT organizations to understand botnet takedown initiatives. Because there are no existing models to explain the performance of botnet takedowns, Ferrier's (2001) model of the drivers and consequences of competitive aggressiveness on business was used as a starting point to construct an effective barrier against the economic growth of botnets. Ferrier's process model of competitive interaction aims to describe characteristics of forces that influence competitive aggressiveness and the consequential organizational performance. Building on Ferrier's (2001) study, the new two-part model is summarized in Figure 1.

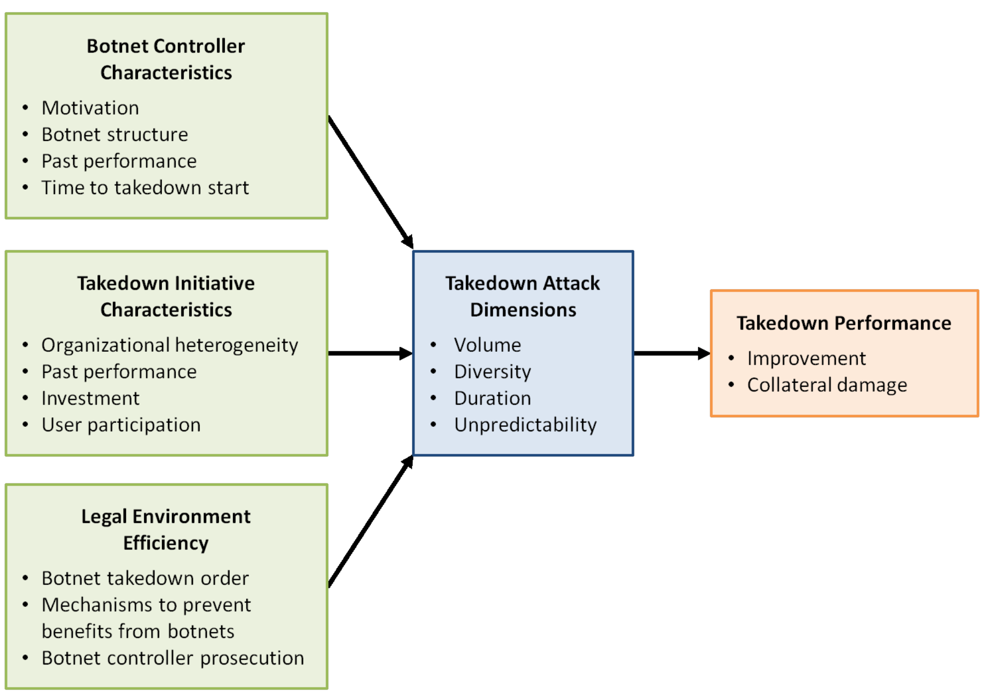

Figure 1. Botnet takedown performance model. Adapted from Ferrier (2001).

Botnet Takedown Initiatives: A Taxonomy and Performance Model

Reza Shirazi

Table 1. Summary of botnets and malware listed in the preliminary database of takedown initiatives

	Botnet Alias	Date Discovered	Date Takedown Disclosed	Estimated Size	Purpose
1	Bamital botnet	2010 (June)	2013 (Feb 6)	8 million bots	Hijack search results; perpetrate click frauds; direct traffic to selected websites
2	Blackshades malware	2012 (June 19)	2014 (May)	500+ thousand computers in 100 countries	Distribute malware used to control the webcam to turn PC into a surveillance/spy device; record keystrokes to steal usernames and passwords for online accounts (e.g., login into bank accounts; make unauthorized money transfers); encrypt files and demand ransom to unlock them
3	BredoLab botnet (Oficla)	2009 (May)	2010 (Oct)	30 million bots	Lease parts of botnets to enable fraudulent activities of others
4	Citadel malware	2012 (Jan)	2013 (Jun 5)	1,462 botnets	Spread malware to manage bots
5	Coreflood botnet	2001	2011 (Apr 13)	2 million bots	Withdraw money from bank accounts; steal private personal financial information
6	Cryptolocker malware	2013 (Sep)	2014 (May)	500 thousand victims	Encrypt files and then demand payment for decryption
7	Cutwail botnet	2007	2009 (June) 2010 (August)	1.5 to 2.1 million bots	Send unsolicited traffic; rent for others to send unsolicited traffic; deliver DDoS attacks
8	Gameover Zeus botnet	2011 (Sep)	2014 (June)	500 thousand to 1 million bots	Commit bank fraud; distribute other malware using “man-in- the-middle” attacks; distribute CryptoLocker malware
9	Grum botnet (Tedroo, Reddyb)	2009	2012 (July 19)	560-840 thousand bots	Send unsolicited traffic, particularly about pharmaceutical products
10	Kelihos botnet (Waledac 2.0 or Hlux)	2010	2011, 2012 (Several)	300 thousand bots	Steal Bitcoin wallets; send unsolicited emails; deliver DDoS attacks
11	Lethic botnet	2008	2010 (January)	260 thousand bots	Send unsolicited traffic, particularly about pharmaceutical products; orchestrate scams
12	Mariposa botnet	2009 (June)	2009 (Dec 23)	15.5 million bots	Sell parts of the botnet to cybercriminals; install pay-per-install toolbars; sell stolen credentials for online services; launder stolen bank login credentials and credit card details via an international network of money mules; manipulate search engines to serve pop-up ads
13	Mega-D botnet		2009 (Oct 11)	509 thousand bots	Send unsolicited traffic
14	Pushdo A botnet	2007 Revived in 2013 (May)	Multiple attempts (2008, 2009, 2010); still Active	1.5 million bots in10 countries	Deliver financial malware using spamming modules; orchestrate spam campaigns with controllers of other botnets; install framework for other botnets; update infected computers with newer version of malware
15	Rustock botnet (RKRustok, Costrat)	2006 (June)	2008 2011 (March)	1 million bots	Send unsolicited traffic
16	Srizbi botnet (Cbeplay, Exchanger)	2007 (March)	2008 (Nov)	450 thousand bots	Send unsolicited traffic to support political causes
17	Storm botnet	2007 (Jan)	2008	160 thousand bots	Send unsolicited traffic with provocative subject matter
18	Waledac botnet (Waled, Waledpak)	2008	2010 (March)	80 thousand bots	Send unsolicited traffic
19	ZeroAccess botnet (Sirefef)		2013 (6 Dec)	2 million bots	Mine Bitcoins; hijack search results; perpetrate click frauds; direct traffic to selected websites

Botnet Takedown Initiatives: A Taxonomy and Performance Model
Reza Shirazi

The first part of the model examines how the volume, diversity, duration, and unpredictability of the botnet takedown are influenced by the characteristics of the botnet controller (i.e., the individuals and systems that run the botnet), the characteristics of the takedown initiative, and the efficacy of the legal environment. The second part of the model examines how the characteristics of the takedown attack influence the performance of the botnet takedown initiative (assessed as improvement and collateral damage). The dimensions used to measure botnet takedown performance are consistent with the approach to accelerate takedown process proposed by Nadji and colleagues (2013).

Takedown attack dimensions
1. *Volume:* the number of uninterrupted action events that comprise each takedown initiative. The actions events can be legal (i.e., a court or enforcement authorities are involved), technology (i.e., hardware or software is used), capacity (i.e., the domain of effectiveness of legal or technology actions), promotion (i.e., actions to gather more supports and users' participation for attack initiatives), and service (i.e., required by end users of compromised devices before and after attack)

2. *Diversity:* the extent to which the sequence of actions of a takedown initiative is comprised of actions of many different types. For example, a low-diversity attack initiative would be one where all 10 actions are technology related, where as a high-diversity attack initiative would include actions of many types.

3. *Duration:* the time elapsed from the beginning to the end of the botnet takedown initiative.

4. *Unpredictability:* the extent to which the sequential order of the novel actions in the botnet takedown initiative is dissimilar from previous takedown initiatives on the same botnet or other botnets from the botnet controller's perspective.

Botnet controller characteristics
1. *Motivation:* a statement that explains why the botnet controllers do what they do. Czosseck and colleagues (2011) conclude, "botnets have developed from a subject of curiosity to highly sophisticated instruments for illegally earning money".

2. *Botnet structure:* refers to whether the botnet has a command-and-control infrastructure, a peer-to-peer infrastructure, or a mixture of the two. Most botnets use a command-and-control infrastructure (Nadji et al., 2013), but regardless of what type of network is used to communicate between nodes, when a network of bots is available, they all follow the instructions from a command-and-control server (Freiling et al., 2005).

3. *Past performance:* measured by the size of the botnet. Past studies have employed various definitions of botnet size due to cloning, temporary migration, and hidden structure issues (Abu Rajab et al., 2007).

4. *Time to takedown start:* the time elapsed from when the botnet was first discovered to the time when the botnet takedown initiative is launched.

Takedown initiative characteristics
1. *Organizational heterogeneity:* the diversity of a takedown organization's demographics, knowledge, and experience. Ferrier (2001) suggests that homogeneity results in a persistent and dominant logic and cognitive strategy, but the heterogeneity that comes with different types of demographics, knowledge, and experience enables organizations to generate more complex and unpredictable strategic actions, facilitate better problem sensing, and match complex competitive challenges.

2. *Past performance:* the number of botnets that the members of the initiative have taken down in the past.

3. *Investment:* refers to the investment a takedown organization makes in security measures.

4. *User participation:* the number of users and organizations that need to act to bring the botnet down.

Legal environment efficacy
1. Botnet takedown order: the order in which a legal authority gives permission to law enforcement units to shutdown or seize botnet elements. Watters and colleagues (2013) investigated legal activities by the Internet Corporation for Assigned Names and Numbers (ICANN) as one of the tools to prevent botnet attacks and found that ICANN lacks the ability and interest in ensuring data integrity is maintained as a priority. They advocate that ICANN should reform its policies, procedures, and standards to exert influence and authority on registrars.

2. Mechanisms to prevent benefits from botnets: examples include approaches focused on scaling and metric values and the "walled garden" technique

Botnet Takedown Initiatives: A Taxonomy and Performance Model
Reza Shirazi

(i.e., restricting convenient access to non-approved information and applications). In examining scaling and metric values of activities between hosts and resources, Tiirmaa-Klaar and colleagues (2013b) identified various benefits, including effective mitigation of various attacks and activities. However, the techniques also caused extensive damage such as blocking legitimate activities and impacting user acceptance. In examining the walled garden technique, they identified critical side effects because it was not accepted by all customers of internet service providers and led to difficult legal situations. Although some negative impacts were identified, this model highlights how up-to-date and dynamic prevention rules and policies (beyond public awareness) make botnets less attractive and profitable.

3. *Botnet controller prosecution:* empowers the takedown attack and protects the cyberspace from similar attacks and should decrease the duration of takedown attack.

Takedown performance
1. *Improvement:* results from the takedown initiative, such as reducing the volume of spam traffic, reducing the number of data breaches, or reducing the number of infected machines.

2. *Collateral damage:* the number of organizations that were negatively affected due to execution of the botnet takedown initiative.

Hypotheses
The model provides a framework in which to cast important questions and to enhance understanding of what constructs are of principal consequence for positively contributing to botnet takedowns while minimizing collateral damage. Thus, based on this model, several hypotheses can be derived:

Hypothesis 1. *More aggressive legal action is positively correlated with an improvement in takedown performance.* (This hypothesis is tentatively supported by the observation that, with the exception of four botnet takedowns [Pushdo, Kelihos, Lethic and Storm], the majority of the successful takedowns had a significant legal component.)

Hypothesis 2. *More informed legal action and past attack and defense performance reduces collateral damage.*

Hypothesis 3. *Organizational heterogeneity of the takedown initiative is positively correlated with takedown attack unpredictability.* (This hypothesis is analogous to H1a from Ferrier [2001].)

Hypothesis 4. *Takedown attack volume is positively correlated with an improvement in takedown performance.* (This hypothesis is analogous to H5 from Ferrier [2001].)

Hypothesis 5. *Takedown attack duration is positively correlated with an improvement in takedown performance.* (This hypothesis is analogous to H6 from Ferrier [2001].)

Hypothesis 6. *A decentralized botnet structure is negatively correlated with takedown performance and unpredictability.*

Conclusions

In support of enhancing botnet takedown performance, this article has provided two contributions: i) an overview of a preliminary database of botnet takedown initiatives and ii) a theoretical model to help predict the success or failure of future takedown initiatives.

This work is relevant to researchers, policy makers, and industry professionals. In particular, personnel in technical, legal, and management functions of organizations interested can use the suggested model to improve the quality of their communications by using similar taxonomy and accelerate decision making for the purpose of launching and operating botnet takedown initiatives. Also, these findings will be relevant to entrepreneurs who wish to launch and grown cybersecurity ventures that provide solutions to botnet and malware problems.

The preliminary database and proposed model mark the beginning of a potentially fruitful avenue of research. The database needs to be augmented and refined; the model and its associated hypotheses need to be tested. As our knowledge improves, the intention is that the empirical data and the model constructs will evolve and cybersecurity experts will become more efficient in taking down botnets through various means.

Citation: Shirazi, R. 2015. Botnet Takedown Initiatives: A Taxonomy and Performance Model. *Technology Innovation Management Review*, 5(1): 15–20. http://timreview.ca/article/862

Keywords: botnet takedowns, dismantle cybercriminal networks, disrupt online networks, cyber-attacks

Botnet Takedown Initiatives: A Taxonomy and Performance Model

Reza Shirazi

About the Author

Reza Shirazi is an Analyst Programmer at the Canada Revenue Agency, Information Technology Branch. Previously, he worked for various government departments and the private sector. He holds a BSc in Computer Software Engineering from the Islamic Azad University in Tehran, Iran, and an MEng in Technology Innovation Management from Carleton University in Ottawa, Canada.

References

Abu Rajab, M., Zarfoss, J., Monrose, F., & Terzis, A. 2006. A Multifaceted Approach to Understanding the Botnet Phenomenon. In *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement:* 41–52. New York, NY: Association for Computing Machinery. http://dx.doi.org/10.1145/1177080.1177086

Abu Rajab, M., Zarfoss, J., Monrose, F., & Terzis, A. 2007. My Botnet is Bigger than Yours (Maybe, Better than Yours): Why Size Estimates Remain Challenging. In *Proceedings of the HotBots '07 First Workshop on Understanding Botnets:* 5. Berkeley, CA: USENIX Association.

Borrett, M., Carter, R., & Wespi, A. 2013. How Is Cyber Threat Evolving and What Do Organizations Need to Consider. *Journal of Business Continuity & Emergency Planning,* 7(2):163–171.

Cremonini, M., & Riccardi, M. 2009. The Dorothy Project: An Open Botnet Analysis Framework for Automatic Tracking and Activity Visualization. In *Proceedings of the 2009 European Conference on Computer Network Defense (EC2ND):* 52–54. Washington, DC: IEEE Computer Society.

Czosseck, C., Klein, G., & Leder, F. 2011. On the Arms Race around Botnets: Setting up and Taking down Botnets. In *Proceedings of the 3rd International Conference on Cyber Conflict (ICCC 2011):* 1-14. Washington, DC: IEEE Computer Society.

Dagon, D., Gu, G., Lee, C. P., & Lee, W. 2007. A Taxonomy of Botnet Structures. In *Proceedings of the 23rd Annual Computer Security Applications Conference (ACSAC 2007):* 325–339. http://dx.doi.org/10.1109/ACSAC.2007.44

Dittrich, D. 2012. So You Want to Take Over a Botnet. In *Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats (LEET 2012):* 6. Berkeley, CA: USENIX Association.

Feily, M., Shahrestani, A., & Ramadass, S. 2009. A Survey of Botnet and Botnet Detection. In *Proceedings of the Third International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2009):* 268–273. Washington, DC: IEEE Computer Society.

Ferrier, W. 2001. Navigating the Competitive Landscape: The Drivers and Consequences of Competitive Aggressiveness. *Academy of Management Journal,* 44(4): 858–877. http://dx.doi.org/10.2307/3069419

Freiling, F. C., Holz, T., & Wicherski, G. 2005. Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks. In *Computer Security: Lecture Notes in Computer Science, 3679:* 319–335. Berlin: Springer Berlin Heidelberg. http://dx.doi.org/10.1007/11555827_19

Kok, J., & Kurz, B. 2011. Analysis of the Botnet Ecosystem. In *Proceedings of the 10th Conference of Telecommunication, Media and Internet Techno-Economics (CTTE 2011):* 1–10. Berlin: VDE.

Nadji, Y., Antonakakis, M., Perdisci, R., Dagon, D. & Lee, W. 2013. Beheading Hydras: Performing Effective Botnet Takedowns. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security:* 121–132. New York, NY: Association for Computing Machinery. http://dx.doi.org/10.1145/2508859.2516749

Nappa, A., Fattori, A., Balduzzi, M., Dell'Amico, M., & Cavallaro, L. 2010. Take a Deep Breath: A Stealthy, Resilient and Cost-Effective Botnet Using Skype. In *Detection of Intrusions and Malware, and Vulnerability Assessment: Lecture Notes in Computer Science, 6201:* 81–100. Berlin: Springer Berlin Heidelberg. http://dx.doi.org/10.1007/978-3-642-14215-4_5

Plohmann, D., Gerhards-Padilla, E., & Leder, F. 2011. *Botnets: Detection, Measurement, Disinfection & Defence.* Heraklion, Greece: European Network and Information Security Agency.

Schaffer, G. P. 2006. Worms and Viruses and Botnets, Oh My! Rational Responses to Emerging Internet Threats. *IEEE Security and Privacy,* 4(3): 52–58. http://dx.doi.org/10.1109/MSP.2006.83

Scully, T. 2013. The Cyber Security Threat Stops in the Boardroom. *Journal of Business Continuity & Emergency Planning,* 7(2): 139–147.

Tiirmaa-Klaar, H., Gassen, J., Gerhards-Padilla, E., & Martini, P. 2013a. Botnets, Cybercrime and National Security. In *Botnets:* 1–40. London: Springer. http://dx.doi.org/10.1007/978-1-4471-5216-3_1

Tiirmaa-Klaar, H., Gassen, J., Gerhards-Padilla, E., & Martini, P. 2013b. Botnets: How to Fight the Ever-Growing Threat on a Technical Level. In *Botnets:* 41–97. London: Springer. http://dx.doi.org/10.1007/978-1-4471-5216-3_2

Watters, P. A., Herps, A., Layton, R., & McCombie, S. 2013. ICANN or ICANT: Is WHOIS an Enabler of Cybercrime? In *Proceedings of the Fourth Cybercrime and Trustworthy Computing Workshop (CTC 2013):* 44–49. Washington, DC: IEEE. http://dx.doi.org/10.1109/CTC.2013.13

Whitehouse, S. 2014. Opening Statement. In *Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks.* Washington, DC: U.S. Senate Judiciary Subcommittee on Crime and Terrorism.

Wikipedia. 2014. Botnet. *Wikipedia.* Accessed January 10, 2015: http://en.wikipedia.org/wiki/botnet

Zeidanloo, H. R., Shooshtari, M. J. Z., Amoli, P. V., Safari, M., & Zamani, M. 2010. A Taxonomy of Botnet Detection Techniques. In *Proceedings of the 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT 2010),* 2: 158–162. Washington, DC: IEEE. http://dx.doi.org/10.1109/ICCSIT.2010.5563555

Zhao, Y., Xie, Y., Yu, F., Ke, Q., Yu, Y., Chen, Y., & Gillum, E. 2009. BotGraph: Large Scale Spamming Botnet Detection. In *Proceedings of the 4th USENIX Symposium on Networked Systems Design & Implementation (NSDI 2009),* 9: 321–334.