Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 31 | Issue 2 Article 1

January 2014

Civil Cyberconflict: Microsoft, Cybercrime, and Botnets

Janine S. Hiller

CIVIL CYBERCONFLICT: MICROSOFT, CYBERCRIME, AND BOTNETS

Janine S. Hiller†

Cyber "warfare" and hackback by private companies is a hot discussion topic for its potential to fight cybercrime and promote cybersecurity. In the shadow of this provocative discussion, Microsoft has led a concerted, sustained fight against cybercriminals by using traditional legal theories and court actions to dismantle criminal networks known as botnets. This article brings focus to the role of the private sector in cybersecurity in light of the aggressive civil actions by Microsoft to address a thorny and seemingly intractable global problem. A botnet is a network of computers infected with unauthorized code that is controlled from a distance by malicious actors. The extent of botnet activity is staggering, and botnets have been called the plague of the Internet. The general public is more commonly aware of the damaging results of botnet activity rather than its operation, intrusion, or infection capabilities. Botnet activity may result in a website being unavailable due to a denial-of-service (DoS) attack, identity theft can occur because the botnet collects passwords from individual users, and bank accounts may be emptied related to botnet activity. Spam, fraud, spyware, and data breaches are all the result of botnet activity. Technical remedies for stopping botnet attacks and damages are ongoing, but technical solutions alone are inadequate. Law enforcement is active in tracking down criminal activities of botnets, yet the number and sophistication of the attackers overwhelm it. In a new development, multiple civil lawsuits by Microsoft have created the legal precedent for suing botnet operators and using existing law to dismantle botnets and decrease their global reach. This article reviews the threats created by botnets and describes the evolution of legal and technical strategies to address botnet proliferation. The distinctive aspects of each of the cases brought by Microsoft are described and analyzed and the complex questions surrounding a botnet takedown

† Janine S. Hiller is a Professor of Business Law, and the Richard E. Sorensen Professor in Finance, at Virginia Tech, Blacksburg, Va. (jhiller@vt.edu).

are identified. Discussion of the details of the lawsuits are important, because over a relatively short period of time, government and private sector roles have evolved considerably in the search for a methodology to deal effectively with botnets. Theoretical and international questions surrounding the sustainability and policy ramifications of private sector leadership in cybersecurity are examined, and questions for future research are identified.

TABLE OF CONTENTS

INTRODUCTION

Headlines of cyberattacks, data breaches, identity theft, spam, and social engineering draw public attention and outrage. Cyber "warfare" and hackback by private companies is a hot discussion topic for its potential to fight cybercrime and promote cybersecurity.[1] In the shadow of this provocative discussion, Microsoft has led a concerted, sustained fight against cybercriminals by using traditional legal theories and court actions to dismantle criminal networks known as botnets. This article brings focus to the role of the private sector in cybersecurity in light of the aggressive civil actions by Microsoft to address a thorny and seemingly intractable global problem.

The *method* for delivering cyberattacks damages is commonly by means of large numbers of "zombie" computers infected with malware. Criminals and hacktivists surreptitiously and without authorization install software on individual computers, allowing them to control and use the multitude of computers to accomplish illicit purposes. The group of computers controlled can number into the hundreds of thousands, and even millions. With these large numbers, a criminal is able to wield increased power and extend his reach around the globe. The group of connected, controlled computers just described is called a botnet. Botnets are the "plague of the Internet."[2]

Effective disarmament of growing numbers of global botnets is a difficult challenge; while technical solutions are developed to disrupt and disable them, the malicious controller responds with new tactics and increasingly sophisticated software. At the same time, the increasingly significant harm caused by these networks of "hijacked" computers, fueling cybercrime across the globe, makes it exponentially more important to control their spread. In addition, because botnets operate across national boundaries, disabling them can involve national and international legal and policy questions. As countries try to protect their citizens from malware that knows no physical boundaries, it is possible that the failure to control the growth and harmful effects of botnets could have such far-reaching effect as to create barriers within

1. *See* Jan E. Messerschmidt, *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm*, 52 COLUM. J. TRANSNAT'L L. 275 (2013) (discussing the debate and theory of hackback). For a cyberwar perspective discussing the relationship between military and private actors in cyberspace, and potential limitations, see Alan Butler, *When Cyberweapons End Up on Private Networks: Third Amendment Implications for Cybersecurity Policy*, 62 AM. U. L. REV. 1203 (2013).

2. A phrase used in many of the Microsoft civil suit court documents.

the fundamental Internet infrastructure and walled segments for protection.[3] However, preventing the spread of illegal botnet activity is not only a public safety issue for law enforcement; private parties and businesses have been active in the remediation of malicious software.

Thus, the questions surrounding a botnet takedown are complex. Over a relatively short period, government and private sector roles have evolved considerably in the search for a methodology to deal effectively with botnets. In order to understand the evolution, this article first provides a brief technical description of botnet operations and an explanation of why employing purely technical means have proven insufficient to handle the threat. Earlier voluntary efforts of loosely networked entities are explained and their limitations examined. Many private entities deserve recognition and credit for their fight against botnets. The limited focus of this article, however, is Microsoft's lead role in pursuing private civil action to thwart and disable botnets. The private, civil action legal approach to dismantling botnets is chronicled, highlighting the evolution of increasingly aggressive tactics and the involvement of law enforcement. A record of Microsoft's legal strategies is important to memorialize the precedent that was set by their aggressive legal actions to fight these cyberthreats, as this model could be adopted by other businesses. Wider adoption of Microsoft's legal approach to dismantle botnets needs further study. The article proposes four lenses for this future work: "crimtort," governance, strategic management, and international perspectives. At present, Microsoft, its partners, law enforcement, and international stakeholders express the willingness to collaborate; private sector leadership may prove to be the necessary ingredient for a sustained and successful fight against technically advanced and globally dispersed cybercrime.

I. BOTNETS AND TAKEDOWN APPROACHES

A basic understanding of how botnets are structured and controlled is necessary to appreciate why technical means alone are insufficient to destroy them. The difficulty of using technical means to defeat botnets is equaled by the challenges of assembling the appropriate persons or entities to disrupt them. While it may be counter intuitive law enforcement did not take the early lead in disrupting criminal botnets. Instead, a voluntary coalition of various private

3. *See* Andrea Renda, *Cybersecurity and Internet Governance*, COUNCIL ON FOREIGN REL. (May 3, 2013), http://www.cfr.org/cybersecurity/cybersecurity-internet-governance/p30621.

parties and an international corporation mounted a collaborative effort that produced positive results. When law enforcement in the United States did take aggressive action to remediate botnet activity, some criticism about their tactics emerged.[4] A brief technical background of botnets and a review of the collaborative and law enforcement efforts to rid the Internet of these threats provide an important backdrop to understanding Microsoft's legal tactics to reach similar results by different means.

A. Definitions and Threats

A bot is defined as a software "program [installed on a computer] that performs user centric tasks automatically without any interactions from a user."[5] Once a computer is infected with the controlling software (malware), it is commonly called a "bot." When a program is installed on a computer in a manner that joins similar computers into a network with the same program, then a bot*net* is created. In the beginning, networks of computers controlled by a centralized server were designed to automatically execute certain repetitive tasks; in other words, they were performing beneficial functions.[6] Although botnets do not have to be malicious, in today's environment they are almost always referred to as such.

An essential aspect of a botnet is that another party, at a distance, controls the network of infected computers. Interestingly, it is surmised that the systematic spread of bots was advanced by the music-sharing service Napster, which used a central server in order to facilitate music sharing.[7] Today, the entity or person in control of a botnet is known as a "botherder," or "botmaster."[8] The server(s), or computer(s), that

4. *See* Kim Zetter, *With Court Order, FBI Hijacks 'Coreflood' Botnet, Sends Kill Signal*, WIRED (Apr. 13, 2011, 6:17 P.M.), http://www.wired.com/2011/04/coreflood/ (quoting critical comments from Chris Palmer at the Electronic Frontier Foundation; about the possibility for unintended consequences).

5. JULIAN B. GRIZZARD ET AL., PEER-TO-PEER BOTNETS: OVERVIEW AND CASE STUDY 2 (2007), *available at* https://www.usenix.org/conference/hotbots-07/peer-peer-botnets-overview-and-case-study.

6. *See id.* at 1.

7. *Id.* at 2.

8. *See* LUIS VIHUL ET AL., NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE & EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, LEGAL IMPLICATIONS OF COUNTERING BOTNETS 4 (2012) (comparing the laws of Estonia and Germany as applied to botnet remediation efforts).

functions as a central control point of control for the bots is known as a "command and control" (C&C) server.[9]

In comparison to the C&C centralized architecture described above, botnets can employ a decentralized control system without a central control point. These distributed botnets use a peer-to-peer (P2P) communication system. Instead of querying the control server(s) for updates and instructions, P2P botnets are designed so that individual computers share and spread commands, thereby avoiding the vulnerability of a central C&C server. P2P botnets have become increasingly more complex and resilient to takedown, and the number of P2P botnets have increased five-fold over the last year.[10]

In the vast majority of cases, an unauthorized, malicious software/program is installed surreptitiously with the intent to use the bot in a botnet for a criminal and harmful purpose. Yet it is not always so. Groups of like-minded individuals can voluntarily allow their computers to be infected with a bot in order to accomplish a common purpose. The hactivist group Anonymous uses this strategy, making it as easy as checking a box to sign up to participate in a botnet.[11] As a result, individuals may become part of a greater online protest movement by voluntarily joining a botnet; for example, the botnet may be used to launch an attack on a website in order to make a political statement.[12]

Botnets have become a commodity. A person does not need to be technically advanced to rent a botnet by the hour or to buy one outright. In 2012, one could rent a botnet for $2 an hour, or could purchase it for $700.[13] More sophisticated botnets were recently "sold as a service" for

9. *See* ORG. FOR ECON. CO-OPERATION AND DEV., PROACTIVE POLICY MEASURES BY INTERNET SERVICE PROVIDERS AGAINST BOTNETS 8 (2012); *see also* Yacin Nadji et al., *Beheading Hydras: Performing Effective Botnet Takedowns*, *in* PROCEEDINGS OF THE 2013 ACM CONF. ON COMPUTER & COMMC'NS SEC. 121 (2013).

10. Michael Mimoso, *Number of Peer-to-Peer Botnets Grows 5X*, THREATPOST BLOG (June 5, 2013, 7:00 AM), http://threatpost.com/number-of-peer-to-peer-botnets-grows-5x.

11. *See* Ryan Singel, *Joining Pro-Wikileaks Attacks is as Easy as Clicking a Button*, WIRED (Dec. 10, 2010, 5:39 PM), http://www.wired.com/threatlevel/2010/12/web20-attack-anonymous/.

12 *See* NART VILLENEUVE, KOOBFACE: INSIDE A CRIMEWARE NETWORK 3 (2010), *available at* http://www.infowar-monitor.net/reports/iwm-koobface.pdf ("It [a botnet] can be used to direct computers to click on fake advertisements for Viagra or marshal them together to attack a meddlesome human rights website, as it is with increasing frequency from Iran and Kazakhstan to Burma and Vietnam.").

13. Ian Steadman, *The Russian Underground has Democratized Cybercrime*, WIRED (Nov. 2, 2012), http://www.wired.co.uk/news/archive/2012-11/02/russian-cybercrime.

$60,000 to $120,000 per year.[14] The cost of purchasing a botnet pales in comparison to the estimated potential income generated, between ten thousand and ten million dollars per month.[15]

The Trend Micro *Global Botnet Threat Activity Map*, capturing real-time activity, reported 9,451 C&C active servers, and 8,283,061 botnet connections, at the time this article was written.[16] It is difficult to measure the extent of botnet infections worldwide, or to estimate the cumulative damage to computer owners and ultimate victims. However, botnets provide a major transportation mode for cybercrime, and yearly estimates of cybercrime damages vary from between $110 billion to $1 trillion per year.[17]

It is only too obvious that botnets are a scourge of the Internet, despite concerted actions to thwart their spread. Companies adopt security defenses, individuals attempt to update security software, security firms and researchers work continuously to learn about and dismantle botnet threats. One of the first collaborative, large-scale, efforts took place to thwart the worm known as Conficker, which was poised to become a huge international botnet.[18] The takedown, described in the following section, was accomplished primarily by private entities with international cooperation, including ICANN and associated entity participation, but it lacked significant government involvement.[19]

---

14. *See* ALAN NEVILLE & ROSS GIBB, ZEROACCESS INDEPTH 10 (2013), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeroaccess_indepth.pdf.

15. *See* VIHUL ET AL., *supra* note 8, at 5. As discussed *infra* Part III with descriptions of each of the botnets, criminal activity that produces this income can derive from actions such as click-fraud, identity theft, password and bank account theft.

16. *Global Botnet Threat Activity Map*, TREND MICRO, http://www.trendmicro.com/us/security-intelligence/current-threat-activity/global-botnet-map/index.html (last visited Jan. 27, 2014).

17. *See* Paul Hyman, *Cybercrime: It's Serious, But Exactly How Serious?*, 56 COMMC'NS OF THE ACM 18, 18 (2013) (noting difference in estimates of cybercrime damages as reported by Symantec Corp. and McAfee Inc.).

18. *See* THE RENDON GROUP, CONFICKER WORKING GROUP: LESSONS LEARNED 13 (2011). This report was funded by the U.S. Department of Homeland Security's Science and Technology Directorate to study the Conficker Working Group and report on its success and challenges. *Id.* at 2.

19. *See id.* at 26 (stating that "the [federal] government's coordination with the Working Group was limited and contributed little to the private sector effort."); *see also id.* at 19 (describing the informal communication between some members of the Conficker Working Group and various agencies).

B. The Conficker Working Group

In October of 2008, Microsoft (MS) issued a "critical" security patch for certain Windows and Windows-server software because, in part, the malicious use of the vulnerability to install a computer worm known as Conficker could result in a computer being recruited into a botnet.[20] Ironically, releases of vulnerability information and patches are known to sometimes create the opposite result; malware can be propagated seeking to exploit the weakness before computers are updated. The Conficker worm, discovered in November 2008, sought to infect computers through this MS vulnerability, however it was different from other worms in its sophistication, growth, and resiliency.[21] While Conficker utilized a C&C framework whereby bots contact the central server for instructions, it also implemented a more dynamic communications structure. Conficker's first version used mathematical algorithms to generate multiple, dynamically changing, C&C locations from 250 domain names each (rather than IP addresses) from five top-level domains. Subsequent evolutions of the virus increased the number of control domain names significantly ("tens of thousands"),[22] and at one point resorted to peer-to-peer communications (rather than C&C), all in order to avoid detection and destruction.

Communication between the bot and control location was encrypted, and the strength of encryption increased in subsequent versions of Conficker.[23] For purposes of this discussion, it is enough to note that as security measures and tactics ratcheted up, each step was met with renewed sophistication in the worm architecture. Within one year, despite efforts of the security community, an estimated five to six million IP addresses (and perhaps up to 13 million computers) were infected with some version of Conficker, and therefore were potential weapons in a botnet arsenal.[24]

---

20. *See id*. at 3.

21. *See id*. at 5.

22. DAVE PISCITELLO, ICANN SECURITIES TEAM, CONFICKER SUMMARY AND REVIEW 17 (2010), *available at* https://www.icann.org/en/system/files/files/conficker-summary-review-07may10-en.pdf.

23. For a chronology of the evolution and different variations of Conficker, see KADRI KASKA, NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, CONFICKER CONSIDERATIONS IN LAW AND POLICY 8–15 (2012) (a report of the NATO Cooperative Cyber Defence in Centre of Excellence in Tallinn, Estonia).

24. *See* PISCITELLO, *supra* note 22, at 10.

Throughout the battle against Conficker, the identity of the worm's author was unknown, and it remains unknown today.[25] In addition, the *purpose* of the potentially powerful botnet was, and remains today, unknown.[26] This uncertainty and yet large potential for harm increased the sense of urgency to take action to defeat the potential use of the botnet.[27] At the outset, security firms, university researchers, and a variety of private entities worked in parallel, with information sharing based on personal trust, to develop methods to destroy the worm and to inform the public about patches.[28] It was not until a symposium on domain name system (DNS) security in Atlanta, Georgia in February 2009, however, that a coordinated effort began by means of the informal Conficker Working Group.[29] Representatives from the Internet Corporation for Assigned Names and Numbers (ICANN) were present at the meeting, and their cooperation became fundamental to the Conficker botnet takedown because of the fraudulent use of domain names to direct bots to a control server.[30] In order to takedown a botnet with a C&C server, discovering the identity of the server is key; knowing the identity and location of the server will allow measures to be taken to disrupt the communications or shut down the sever itself, perhaps even by physical means.[31]

When members of the Working Group decrypted the algorithm for the dynamic communications, they then determined to buy the domains from Internet registrars *ahead of* the automated Conficker program in order to block its orders and updates to individual computers.[32] However, the sheer volume of domains utilized proved too costly to purchase in bulk, even for a resource rich entity such as Microsoft who was involved in the effort.[33] In addition, the domains used different country codes, and therefore increased the complexity of the botnet mitigation efforts.[34] Although it was surmised that the

25. *See* KASKA, *supra* note 23, at 18.
26. *Id.*
27. *See* PISCITELLO, *supra* note 22, at 12–14.
28. *See id.* at 5.
29. *See id*. at 7.
30. *See id.* at 6.
31. *See* GRIZZARD, *supra* note 5, at 1.
32. *See* THE RENDON GROUP, *supra* note 18, at 16–18.
33. *See* PISCITELLO, *supra* note 22, at 6.
34. *See* THE RENDON GROUP, *supra* note 18, at 7.

Conficker worm originated from the Ukraine,[35] many of the domain names generated in the algorithm were of Chinese denomination.[36] To solve this conundrum of global reach, ICANN took the lead by agreeing: (1) to waive domain name registration fees as far as possible for the Working Group; and (2) to give prior notice to over 100 top-level country domain registrars that certain domain names would be automatically registered by Conficker.[37] Thus, the registries could block the registration of C&C names by Conficker; this coordinated action rendered the botnet unable to communicate with or direct the botnet, effectively disabling it. Reporting on the collaborative effort to takedown Conficker, an ICANN document makes two interesting comments. First, it recognized the ground-breaking nature of the group composition, saying that, "The operational response to Conficker is perhaps as landmark an event as the worm itself."[38] In contrast, however, it also stated that, "The community cannot rely on all contractual matters [such as waiving fees] to be so easily handled for all future incidents."[39]

Although law enforcement engagement with the Conficker Working Group and potential botnet was minimal, its attention to cybercrime was not. Since botnets are the vehicle for accomplishing many types of cybercriminal activity, law enforcement also became directly involved in attempts to disable those threats.

C. The FBI and DoJ

The Coreflood computer virus infected an estimated two million computers globally and was active for at least ten years.[40] When the Coreflood virus installed on a user's computer, it was then possible to enlist it as a bot in a future botnet.[41] In particular, Coreflood could log user keystrokes, obtain account passwords, and facilitate bank fraud and theft.[42]

---

35. *Id*. at 6. But some also hypothesized that the author was a nation–state. *Id.* at 9.

36. *See id*. at 19.

37. *See id.* at 20–21.

38. PISCITELLO, *supra* note 22, at 1.

39. *Id.* at 14.

40. Press Release, U.S. Dep't of Justice, Dep't of Justice Takes Action to Disable Int'l Botnet (Apr. 13, 2011), http://www.fbi.gov/newhaven/press-releases/2011/nh041311.htm.

41. Coreflood is both the name of the virus and the name of the botnet.

42. *See* DoJ Press Release, *supra* note 40.

Not surprisingly, the breadth and depth of Coreflood infections and resulting botnet harms spurred an FBI investigation that resulted in legal action by the U.S. Department of Justice (DoJ); importantly, Coreflood was the first law enforcement and legal action to shut down an active botnet.[43] The initiating complaint described a botnet in general as "inherently a creature of crime,"[44] and "a threat to national security."[45] The specific charges against the unknown Coreflood botnet operators included wire fraud, bank fraud, and unauthorized access to electronic communications.[46] Estimates of Coreflood damages exceeded $20 million.[47]

The Coreflood botnet operated similarly to the previously described Conficker design (except at a simpler level), as the C&C server located at certain IP addresses would change domain names in order to evade disabling.[48] However, domain name changes were programmed in the malware to occur twice per month, and those specific domain names were uncovered by the investigation.[49] The legal action was designed not to arrest and imprison the perpetrators of the botnet, as yet unknown, but to stop the operation of the malicious software installed on unsuspecting user computers. On April 11, 2011, the DoJ announced that under the authority of a temporary restraining order it had seized command and control servers and redirected botnet traffic to substitute servers, disabling the functions of the botnet and giving victims the opportunity to cleanse the Coreflood software from their computers.[50]

---

43. *Id.*

44. Complaint at 3, U.S. v. John Does 1-13, No. 3:1-CV-561 (D. Conn. Apr. 11, 2011) [hereinafter Coreflood complaint].

45. *Id.* at 3–4.

46. *See id.* at 10–12 (alleging violations of 18 U.S.C. §§ 1343, 1344, and 2511, respectively).

47. NAT'L CYBER INVESTIGATIVE JOINT TASK FORCE, FED. BUREAU OF INVESTIGATION, OPERATION CLEAN SLATE 3, *available at* http://www.wpcug.org/Downloads/National%20Cyber%20Investigative%20Joint%20Task%20Force.pdf.

48. *See* Coreflood Complaint, *supra* note 44, at 5–7.

49. *Id.* at 6–7.

50. *See* DoJ Press Release, *supra* note 40. Jurisdiction was granted based on evidence of the large number of computers infected in the United States, allegations of specific instances of bank and wire fraud in the United States and the unauthorized access to computers in interstate commerce under the Computer Fraud and Abuse Act (CFAA). *See* Coreflood Complaint, *supra* note 44, at 3.

In particular, the DoJ seized 29 domain names and 5 servers that were a part of the C&C structure, and concurrently *substituted* FBI-managed servers in the C&C structure.[51] In addition, the TRO granted permission for the substituted servers to send a temporary disabling command to the malware.[52] Sending this "stop" command was authorized "only to computers reasonably determined to be in the United States."[53] The DoJ was prohibited from accessing any content information from the infected computer, its access restricted to data of "originating IP address, network port, and the date and time of transmission."[54] The extraordinary remedy allowing the government to substitute servers in the C&C infrastructure and send electronic instructions to individual computers was based, in part, on the "special needs, including the need to protect the public and to perform community caretaking functions, that are beyond the normal need for law enforcement . . . ."[55]

Meanwhile, security firms continued to work on a lasting patch for the Coreflood vulnerability.[56] In addition, evidence showed that the overall result of the actions rid the Coreflood virus from 90% of infected computers in the United States.[57] Included in this number were private parties, businesses, governments, hospitals, and universities.[58]

Stopping the Coreflood botnet operations would only be a temporary patch, however, if the malware itself were not eliminated from user computers. Victim notification, numbering in the hundreds of thousands, occurred primarily by sharing IP addresses of infected customers with the respective Internet Service Provider (ISP) and requesting that a form notification be delivered to those customers.[59] In arguably a further extension of the extraordinary means taken to disable

51. *See* DoJ Press Release, *supra* note 40.

52. Temporary Restraining Order at 5–6, U.S. v. John Does 1-13, No. 3:11-CV-561 (D. Conn. Apr. 25, 2011) [hereinafter Coreflood TRO].

53. *Id.* at 6.

54. *Id.* at 7.

55. *Id.* at 4.

56. Supplemental Memo. in Support of Prelim. Inj. at 5, U.S. v. John Does 1–13, No. 3:11-CV-561 (D. Conn. Apr. 23, 2011) [hereinafter Supplemental Memo].

57. *Id.* at 10–11.

58. *Coordinated Law Enforcement Action Leads to Massive Reduction in Size of International Botnet*, U.S. DEP'T OF JUSTICE (Apr. 27, 2011), http://www.justice.gov/opa/blog/coordinated-law-enforcement-action-leads-massive-reduction-size-international-botnet.

59. *See* Supplemental Memo, *supra* note 56, at 5–6.

the botnet, the FBI sent *direct* notices to "Identifiable Victims,"[60] including "seventeen state or local government agencies, including one policy department; three airports; two defense contractors; five banks or financial institutions; approximately thirty colleges or universities; approximately twenty hospital or health care companies; and hundreds of businesses"[61] explaining that they could authorize the FBI to delete the Coreflood virus from their computers.[62] With written consent, the government uninstalled the software directly from the user's computer.[63]

Stopping the Coreflood virus involved cross-border action. The botnet servers were located around the world, outside the jurisdictional reach of U.S. courts. In order to disable the botnet, the FBI targeted what it could reach within the United States; it requested and the court ordered the domain name providers to "impose a registry lock on the Internet domain name[s]" including any account associated with it.[64] Stopping with the seizure of domestic C&C computers would not have disabled the botnet for any length of time. The government strategy was effective because it avoided ICANN's participation by using a court order issued to the domain providers to accomplish the same result. Providers were primarily located in the United States, however some were also in Singapore, the United Kingdom, and Australia; voluntary cooperation of the domain name providers in these foreign jurisdictions assisted the takedown.[65]

The Coreflood takedown was subject to criticism from various quarters. The action was labeled "a first in the U.S. . . . that . . . gave law enforcement permission to interfere directly with computers belonging to users who weren't being investigated, or charged with any crime."[66] The Electronic Frontier Foundation (EFF) celebrated the takedown of the botnet, but raised questions about the wisdom of a strategy that included an "extraordinary" governmental intrusion into individual computers; an EFF representative commented that the risk

60. *See id.* at 6.

61. *Id.*

62. *See id.* at 7.

63. *Id.* at 12–13. The government did not request court approval for uninstalling the virus because it did so only upon the user's written permission. *Id.*

64. Coreflood TRO, *supra* note 52, at 6.

65. *See id.* at Schedule A.

66. Chris Paoli, *Feds Move Forward on Coreflood Botnet Removal*, GCN (Apr. 29, 2011), http://gcn.com/Articles/2011/04/28/ECG-Feds-To-Remove-Coreflood.

of harm was too great and that "[i]f nothing horrible comes of this, it will be because of a combination of sheer luck and surprising politeness on behalf of the malware authors."[67] Others questioned the precedent set by such an aggressive posture because "[i]t's getting the FBI involved in an area where they traditionally haven't been involved. What's stopping [the FBI] from going all the way to the extreme and shutting down political discourse they don't like?"[68] On the opposite end of the spectrum, some questioned whether the FBI went far enough. Since the botnet was a threat to the security of the Internet, should the FBI have gone further and cleaned users' computers even without explicit permission? An informal survey, directed at the security community, found support for this more aggressive approach.[69]

Microsoft's first civil lawsuit to dismantle botnets was launched before the Coreflood action, however its strategy can be viewed in contrast to the law enforcement action and the voluntary Conficker collaborative effort, and the inherent difficulties with each. Though MS took the lead as plaintiff in each of the cases discussed, security professionals, academics, and other interested parties were crucial to the takedown efforts.[70] For purposes of much of the following discussion however, based on their lead plaintiff role, the discussion refers only to Microsoft.

67. Dan Kaplan, *Coreflood Takedown May Lead to Trouble*, SC MAG. (Apr. 18, 2011), http://www.scmagazine.com.au/News/254827,coreflood-takedown-may-lead-to-trouble.aspx.

68. *Id.*; *see also* Bruce Schneier, *Hijacking the Coreflood Botnet*, SCHNEIER ON SEC. BLOG (May 2, 2011, 6:52 AM), https://www.schneier.com/blog/archives/2011/05/hijacking_the_c.html (supporting the action as necessary to preserve the Internet, but questioning whether it created a "slippery slope" for more widespread actions).

69. *See* Paul Ducklin, *FBI Takes On Coreflood Botnet—But is This a Step Too Far?*, NAKED SECURITY (Apr. 28, 2011), http://nakedsecurity.sophos.com/2011/04/28/fbi-takes-on-coreflood-botnet-step-too-far/.

70. *See* discussion *infra* Part II.

II. THE FIRST MICROSOFT OFFENSIVE

In February 2010, Microsoft announced the "first of its kind" takedown of a botnet based on collaborative technical and legal action.[71] The Waledac botnet takedown targeted a botnet that could potentially send 1.5 billion unsolicited spam emails per day.[72] Among others, the emails included solicitations for fraudulent products and services, malware that enlisted more computers into the botnet, and the installation of malicious software that stole financial and personal information from the user.[73] In addition, the botnet software modified Microsoft Window's operating system, suspended authentic security updates, and caused users to install fake, injurious "security" software.[74] Waledac owners sold the use of the botnet as a service to third parties, therefore dispersing the various unauthorized and criminal activities across the globe.[75] Microsoft received thousands of complaints[76] from customers, who believed that the malfunction of their computer was due to defects in Microsoft products, and who believed that the spam email originated from Microsoft.[77]

The technical team identified over 200 domain names used in the C&C architecture of the botnet.[78] While a detailed technical description is beyond the scope of this article, a few aspects of the Waledac structure are relevant to understanding how the legal action and court

71. *See* Tim Cranton, *Cracking Down on Botnets*, OFFICIAL MICROSOFT BLOG (Feb. 24, 2010, 6:16 PM), http://blogs.microsoft.com/blog/2010/02/24/cracking-down-on-botnets/ ("This legal and industry operation against Waledac is the first of its kind, but it won't be the last. With this action, done in cooperation with experts from Shadowserver, the University of Washington, Symantec, University of Mannheim, Technical University in Vienna, International Secure Systems Lab, the University of Bonn and others, we're building on other important work across the global security community to combat botnets.").

72. *See* Brief in Support of Application of Microsoft Corp. for an Emergency Temporary Restraining Order and Order to Show Cause RE Preliminary Injunction at 2, Microsoft Corp. v. John Does 1–27, No. 1:10-CV-156 (E.D. Va. Oct. 27, 2010) [hereinafter Waledac Brief]; *see also* Brian Krebs, *Microsoft Ambushes Waledac Botnet, Shutters Whistleblower Site*, KREBS ON SECURITY (Feb. 25, 2010, 11:33 AM), http://krebsonsecurity.com/2010/02/microsoft-ambushes-waledac-botnet-shutters-whistleblower-site/.

73. *See* Waledac Brief, *supra* note 72, at 16–18.

74. *See* Complaint at 8, Microsoft Corp. v. John Does 1–27, No. 1:10-CV-156 (E.D. Va. Oct. 27, 2010) [hereinafter Waledac Complaint].

75. *See* Proposed Findings of Fact and Recommendations at 7, Microsoft Corp. v. John Does 1–27, No. 1:10-CV-156 (E.D. Va. Oct. 27, 2010) [hereinafter Waledac Findings of Fact].

76. *See* Waledac Brief, *supra* note 72, at 3.

77. *Id.* at 8–9.

78. *Id.* at 6.

orders were essential components of disabling the botnet. The Waledac infrastructure was tiered, described by Microsoft as consisting of Spammer Nodes, Repeater Nodes, TSL servers, and at the top-level the Main Command and Control servers.[79] The Spammer Nodes consisted of individual user computers infected with the controlling botnet malware, and situated behind firewalls rather than connected directly to the Internet. Spammer Nodes automatically communicated with and followed the orders of the controller of the botnet through a system that utilized the Repeater Nodes. Repeater Nodes were used for several purposes, including both as a communicating device between the different layers of the botnet, and as DNS servers, which resolve an IP address to a domain name. A third layer consisted of the TSL servers, acting as a wall to obfuscate and protect the identity of the ultimate botnet controller. Communications would pass through the TSL servers to the last layer, the Main Command and Control Servers, which were directly controlled by the owner(s) of the botnet, otherwise known as the bot herder(s).[80] In addition, DNS fast flux servers were utilized to constantly change the domain names associated with IP addresses with the root zone at Internet registrars. In summary, the design of the botnet infrastructure made technical remediation difficult to accomplish.[81]

Microsoft designed an offensive strategy to disrupt the 277 domain names that facilitated communications among the tiers of the botnet. As they explained, "[t]hese 273 [4 were later added] domains continuously control the ability of the computers that make up the Waledac botnet to communicate with each other and to grow the botnet,"[82] and "[t]hese domains have no legitimate purpose. . . . The domains' sole purpose is to await requests from botnet computers and instruct them on how to continue communicating with each other and to infect new user computers."[83] Without a communication structure, the botnet would be unable to operate, even though individual

79. *See* Waledac Complaint, s*upra* note 74.

80. *Id.* at 7.

81. *See id.* at 7–10. It was difficult to reach the spammer node, individual user computers, to stop the infection because they were behind firewalls; difficult to reach the Fast Flux servers because they were routed and hidden behind the Repeater Node computers; difficult to reach the Repeater Node servers because their location was changing due to the continuous action by the Fast Flux servers; and difficult to reach the Command and Control servers because their identity was protected by the Repeater Nodes and the lack of a direct connection to Spammer Nodes.

82. Waledac Brief, *supra* note 72, at 6.

83. *Id.* at 7.

computers would still be infected with malicious software. The adopted strategy involved taking swift and secret action to take the botnet domain names off the Internet before the botnet controllers could change their location.[84] Therefore, Microsoft sued 27 John Doe defendants that were registered as the owners of the domain names, based on allegations of violations of the Computer Fraud and Abuse Act (CFAA), CAN-SPAM Act, Electronic Communications and Privacy Act (ECPA), false designation of origin and trademark dilution under the Lanham Act, trespass to chattels, and unjust enrichment and conversion.[85] Importantly, Microsoft requested an *ex parte* proceeding and a Preliminary Injunction to instruct the domain name registrar, VeriSign, to "lock" the domain names while it attempted to identify the owners of the domains and serve process upon them.[86]

A. Legal Allegations

In general, one of the most often applicable statutes used to pursue prosecution for hacking or the propagation of malicious software is the Computer Fraud and Abuse Act.[87] A criminal statute, the CFAA grants a civil right of action for criminal acts when certain injuries occur.[88] The applicable sections of the CFAA provide a civil remedy of damages, an injunction and equitable remedies when a person intentionally gains unauthorized access, or exceeds authorized access, to a computer used in interstate commerce and either causes aggregate loss of at least $5,000, affects medical treatment of an individual, personal physical injury, or causes a threat to public health or safety.[89] Microsoft alleged that the Waledac botnet accessed its computers and those of its customers intentionally and without authorization, to obtain information, commit fraud, and to cause damage by transferring malicious computer programs and code.[90]

---

84. *See Waledac: The Legal Action Plan*, MICROSOFT SECURITY INTELLIGENCE REPORT, http://www.microsoft.com/security/sir/story/default.aspx#!waledac_legal [hereinafter Legal Action Plan].

85. *See infra* Part III.A.

86. *See* Legal Action Plan, *supra* note 84; *see also infra* Part III.B.

87. 18 U.S.C. § 1030 (2012). *See generally* Lee Goldman, *Interpreting the Computer Fraud and Abuse Act*, 13 U. PITT. J. TECH. L. & POL'Y 1, 2–4, 11–12 (2012) (describing the CFAA as primarily an anti-hacking statute).

88. WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 201 (4th Cir. 2012).

89. 18 U.S.C. § 1030(g). The additional requirements are found in *id.* § 1030(c)(4)(A)(i)(I)–(V).

90. *See* Waledac Complaint, *supra* note 74, at 13.

Waledac sent hundreds of thousands of spam emails to individuals. Microsoft, in its capacity as an Internet service provider, for example a provider of the Hotmail service, was able to file a civil action for violations of the CAN-SPAM Act of 2003[91] based in part on false header and deceptive use of the emails.[92] Microsoft also alleged violations based on the absence of return addresses, opt-out provisions, and the lack of clear indications of the emails' advertising nature.[93]

The Electronic Communications Privacy Act (ECPA)[94] is also a criminal statute that allows for a civil remedy, prohibiting interception of electronic communications without authorization.[95] Microsoft alleged that the Waledac botnet intercepted and interfered with both customer and Microsoft emails in storage at Microsoft, at its customers' computers, and "within Microsoft's licensed operating system."[96]

Trespass to chattels is a common law tort that has been used to pursue remedies for previous electronic intrusion or unauthorized use cases, and the conversion allegation is a related theory.[97] Microsoft alleged trespass to chattels based on the harm caused by the intentional, unsolicited emails sent by the botnets, and the unauthorized access to its computers.[98]

---

91. 15 U.S.C. § 7704 (2006).

92. *See* Waledac Complaint, *supra* note 74, at 13.

93. *Id.*

94. 18 U.S.C. § 2701 (2012).

95. *See* DIRECTV v. Pepe, 431 F.3d 162, 167 (3d Cir. 2005) ("Section 2511 provides in relevant part that '[e]xcept as otherwise specifically provided in this chapter any person who . . . intentionally intercepts . . . any . . . electronic communication' is subject to criminal penalties or civil suit by the federal government. Appearing later in the same chapter, § 2520 expressly authorizes private suits by 'any person whose . . . electronic communication is intercepted . . . in violation of this chapter.' Both sections reference the interception of electronic communications. The linguistic interlock between the two provisions could not be tighter, nor more obviously deliberate: § 2511(1)(a) renders unlawful the unauthorized interception of electronic communications, including encrypted satellite television broadcasts, while § 2520(a) authorizes private suit against those who have engaged in such activities.") (citations omitted).

96. *See* Waledac Complaint, *supra* note 74, at 15.

97. *See* T. Luis de Guzman, *Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges*, 59 CATHOLIC U. L. REV. 527, 531–38 (2010) (reviewing cases under trespass theories and arguing for extension of negligence theory). *See generally* Catherine M. Sharkey, *Trespass Torts and Self-Help for an Electronic Age*, 44 TULSA L. REV. 677 (2009) (discussing trespass to chattels in Internet cases and arguing for a self help right for victims).

98. *See* Waledac Complaint, *supra* note 74, at 17.

The Lanham Act dilution[99] and false designation of origin[100] provisions were used by a business early in the digital era to successfully pursue a civil case when the spammer used false email headers.[101] Microsoft alleged that the Waledac botnet used the trademarks of Microsoft, Windows, and Hotmail in ways that were misleading and caused confusion with customers about the source of the spam email and fake anti-virus software offered as MS antispyware.[102] In addition, the association of Microsoft's famous trademarks with the malicious software caused "blurring and dilution by tarnishment" when it "creat[ed] keys and writing entries under a registry path that include[ed] the Microsoft marks,"[103] all remedies that would prove helpful in later botnet takedowns.[104]

Lastly, Microsoft alleged liability for the botnet's activities based on the general common law conception of unjust enrichment.[105] They argued that botnet operators "profited unjustly"[106] by knowingly using Microsoft computers and customer computers without authorization, and by using Microsoft licensed software without permission. Microsoft appealed to principles of equity to argue for disgorgement of the ill-gotten profits and for payment of damages.[107]

Microsoft's combination of legal theories of civil liability established a legal framework for tackling the takedown of a botnet, a framework that it would use repeatedly to disable subsequent botnets, and upon which it would expand future requests for court permission to take more broad reaching actions. Legal theory alone, however,

---

99. 15 U.S.C. § 1125(c) (2012).

100. *Id.* § 1125(a)(1)(A).

101. America Online v. IMS, 24 F. Supp. 2d 548, 551–52 (E.D. Va. 1998).

102. *See* Waledac Brief, *supra* note 72, at 19.

103. *Id.* at 16–17.

104. Section 1116 of the Lanham Act states:

> [W]ith respect to a violation that consists of using a counterfeit mark in connection with the sale, offering for sale, or distribution of goods or services, the court may, upon ex parte application, grant an order under subsection (a) of this section pursuant to this subsection providing for the seizure of goods and counterfeit marks involved in such violation and the means of making such marks, and records documenting the manufacturer, sale, or receipt of things involved in such violation.

15 U.S.C. § 1116(d)(1)(A) (2013).

105. *See* Waledac Complaint, *supra* note 74, at 18.

106. *Id.*

107. *Id.*

would not be adequate to takedown the botnet; the legal procedure strategy was essential for success.

B. Legal Strategy and Procedure

Microsoft designed a procedural legal strategy described in its *Legal Action Plan*.[108] The legal approach to instituting a takedown included major challenges, as described by Microsoft:

> Cease and desist letters would not force immediate action. Similarly, domain takedown is inexact and somewhat limited under typical ICANN procedures. For example, ICANN's Uniform Domain-Name Dispute-Resolution Policy (UDRP) provides a relatively long window in which bad actors would be able to register new domains, update the botnet code, or take other evasive actions to move the botnet while the ICANN process unfolded.[109]

1. *Ex Parte* Proceeding

Instead of appealing to ICANN and the domain resolution process to freeze the botnet domain names as was done in Conficker, Microsoft asked a District Court for an *ex parte* proceeding without notice to the defendants (for three days), in order to prevent the bot herders from automatically moving their C&C structure and destroying evidence.[110] The precedent cited for the request was the 2009 Federal Trade Commission (FTC) emergency *ex parte* proceeding to dismantle an ISP that hosted extensive criminal activities, including the control of botnets.[111] In the previous case, the FTC was granted an *ex parte* TRO without notice to the ISP because to do otherwise would allow the

---

108. *See* Legal Action Plan, *supra* note 84.

109. *Id.*

110. *See* App. of Microsoft Corp. for an Emergency Temporary Restraining Order and Order to Show Cause Re Prelim. Inj., Microsoft Corp. v. John Does 1–27, No. 1:10-CV-156 (LMB/JFA) (E.D. Va. Feb. 22, 2010); Microsoft Corp.'s Motion for a Protective Order Sealing Documents, Microsoft Corp. v. John Does 1–27, No. 1:10-CV-156 (E.D. Va. Feb. 22, 2010) (citing FED. R. CIV. PROC. 26(c)(1)).

111. FTC v. Pricewert, LLC, No. 09-2407 (N.D. Cal. June 2, 2009); *see also* Press Release, Fed. Trade Comm'n, FTC Permanently Shuts Down Notorious Rogue Internet Service Provider (May 19, 2010), http://www.ftc.gov/news-events/press-releases/2010/05/ftc-permanently-shuts-down-notorious-rogue-internet-service. Microsoft's approach mirrored this case in many procedural ways although the legal theories differed.

defendant to dispose of evidence of wrongdoing and move its operations.[112]

The *Federal Rules of Civil Procedure* allow for *ex parte* hearings, but the court will normally require that the plaintiff first produce evidence of attempted notification to the defendant.[113] Microsoft requested that notification be delayed until after the domains were rendered inoperable; otherwise the botnet would move its location to avoid disruption. Microsoft's legal argument relied on a 1979 case, *In re Louis Vuitton Et Fils S.A.*,[114] in which the court allowed the *ex parte* order without notification because to do otherwise would allow the defendant to dispose of physical evidence. Importantly, Microsoft provided detailed information about how it would satisfy due process and provide notice to the defendants at the later time.[115] MS pledged to utilize all methods of notification possible, including notification by means of:

> (1) [T]he Hague Convention on Service Abroad by sending the Complaint, Summons and all other documents to the Chinese Ministry of Justice; (2) alternative methods, including service and notice by email, facsimile, and by mail; and (3) publication of all relevant pleadings on a website Microsoft set up solely to provide the domain registrants with notice.[116]

Microsoft faced the possibility that at least some of the domain names were "hijacked" by the botnet; thus, they named additional John Doe defendants in order to preserve the rights of any innocent victims.[117] The domain names included Chinese registrants, also likely falsified,

---

112. *See Ex Parte* Temporary Restraining Order and Order to Show Cause at 2–3, FTC v. Pricewert, LLC, No. 09-2407 (N.D. Cal. June 2, 2009).

113. FED. R. CIV. P. 65 provides in pertinent part:

> (1) Issuing Without Notice. The court may issue a temporary restraining order without written or oral notice to the adverse party or its attorney only if:
>
> (A) specific facts in an affidavit or a verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition; and
>
> (B) the movant's attorney certifies in writing any efforts made to give notice and the reasons why it should not be required.

FED. R. CIV. P. 65 (2014).

114. 606 F.2d 1 (2d Cir. 1979).

115. *See* Waledac Brief, *supra* note 72, at 24–27.

116. *See* Legal Action Plan, *supra* note 84.

117. *Id.*

therefore Microsoft also promised service of process via the Chinese Minister of Justice.[118]

2. Emergency Temporary Restraining Order and Preliminary Injunction

In concert with the *ex parte* proceeding, Microsoft requested, and received, an emergency temporary restraining order enjoining the malicious activities by the John Does controlling the botnet, and an order to VeriSign, the domain registry, to shut down the domains at that level.[119] This was the essential action needed to disrupt the communications structure and disable the use of the botnet: targeting the domain names acting in the C&C role. Without receiving updated instructions from the command server, the individual bots would become inactive. Specifically, the preliminary injunction directed VeriSign to "lock" the domains, remove them from the zone file, disallow any changes, hold the domains in escrow, and preserve evidence of misconduct.[120]

The legal strategy included sensitivity to the uniqueness of the lawsuit. Studying precedents of the Eastern District of Virginia, MS crafted its requests for injunction in order to respond to the concerns found in previous decisions involving extraordinary procedures.[121] Microsoft paid attention to its relationship with the court, noting that they, "worked very hard to develop and maintain credibility with the Court by ensuring that its [our] arguments were supported by substantial evidence and law, and also by offering timely submissions, avoiding undue delay, and ensuring that it [we] worked with counsel who was familiar with the Court's practices."[122]

The court granted the preliminary TRO and subsequently the permanent order, on the basis that Microsoft was likely to succeed on violations of the Computer Fraud and Abuse Act, trespass to chattels, unjust enrichment, conversion, and negligence.[123] Microsoft was granted 14 days under the TRO to shut down the botnet, and it was

118. *Id.*

119. *See Ex Parte* Temporary Restraining Order and Order to Show Cause re Prelim. Inj., Microsoft Corp. v. John Does 1–27, No. 1:10-CV-156 (E.D. Va. Oct. 27, 2010) [hereinafter Waledac TRO].

120. *Id.* at 3–4.

121. *See* Legal Action Plan, *supra* note 84.

122. *Id.*

123. *See* Waledac TRO, *supra* note 119, at 2.

ready to act quickly. The domains were shut down within 48 hours, and within the next 24 hours the Chinese defendants were served with notice of the pending lawsuit. Email notices were sent to all addresses of the domain holders listed with the registries, and the takedown action was widely publicized.[124]

Microsoft's attention to the possibility of innocent parties proved prescient. Stephen Paluck, owner of debtbgonesite.com, claimed his innocence, and argued that he had no knowledge that his domain was a part of the botnet.[125] Paluck had transferred control of the domain to a third person, and stated that he did not know who controlled the domain. As a result, Microsoft purchased the domain name from Paluck and assisted him in the cleanup of his computer.[126] Another domain name was used as "name-services.com;" after ensuring that this entity shutoff the domains used in the botnet, Microsoft also dropped this entity from its lawsuit.[127]

C. Default Judgment

The *Ex Parte* Order for an Emergency Temporary Restraining Order, followed by Service of Process and the grant of a Temporary Restraining Order, culminated in a Default Judgment that transferred the domain names to Microsoft.[128] As noted in the Findings of Facts:

> [T]he only way to enjoin effectively the Doe Defendants' operation and propagation of the Waledac Botnet is to permanently deprive them of the Botnet Domains and transfer control of the domains to an entity that will ensure that they are not re-infected and revived as part of the Waledac Botnet. Microsoft is a natural candidate to be the entity in control of these domains because it is willing to bear

---

124. *See* Legal Action Plan, *supra* note 84. The details of how quickly Microsoft acted and the extensive ways in which it sought to identify and give notice to the John Doe defendants are outside the scope of this general article. In brief, documents were translated to Chinese and posted on an approved website. No responses were received, although Microsoft noted that at one point after the takedown became public its noticeofpleadings.com site was probed by entities from Russian IP addresses. *See* Waledac Findings of Fact, *supra* note 75, at 16.

125. Microsoft Corp.'s Status Report at 2, Microsoft Corp. v. John Does 1–27, No. 1:10-CV-156 (E.D. Va. March 5, 2010).

126. *Id.*

127. *Id.* at 3.

128. *R.I.P Waledac: Undoing the Damage of a Botnet*, OFFICIAL MICROSOFT BLOG (Sept. 8, 2010), http://blogs.microsoft.com/blog/2010/09/08/r-i-p-waledac-undoing-the-damage-of-a-botnet/. VeriSign was ordered to transfer 276 domains to a registrar chosen by Microsoft, which would then transfer the domains directly to Microsoft. *Id.*

> the costs associated with ensuring that the domain registrations to not lapse, it has the technical expertise to ensure that the domains are not once again taken over by the Waledac Botnet, and it has no pecuniary interest in controlling those domains.[129]

III. MICROSOFT TAKEDOWNS EVOLVE

Microsoft executed seven more botnet takedowns in the next three years. Five of these were undertaken without law enforcement partnerships, while the two most recent ones in 2013 were collaborative in nature. The five Microsoft led takedowns primarily built upon the legal *procedure* and framework first applied during the Waledac action. A request for an *ex parte* proceeding without notice and a Temporary Restraining Order and Injunction was followed by swift action to serve notice to the defendants. The legal *theories* argued by these cases also built upon the strategy established in the Waledac takedown. Yet each one of these takedowns progressively added to Microsoft's arsenal against malicious botnets by addressing additional issues in each unique case. The following descriptions of the botnet remediations focus on these additional developments, acknowledging that they build upon the previously designed fundamental strategy.

A. Rustock

The Rustock botnet was estimated to have infected over one million individual computers worldwide in 2011, and estimated to produce 20%–60% of worldwide spam.[130] At one point it was estimated to be the largest purveyor of spam in the world, dubbed the "King of Spam."[131] Spam emails generated by the Rustock were primarily used to sell unregulated generic pharmaceuticals, particularly those properly manufactured by Pfizer, but they also targeted Hotmail users with false lottery scams, for example, and caused loss of financial information and associated damages.[132] Rustock was particularly virulent because it infected the user's software so completely, and at such a fundamental

129. *See* Waledac Findings of Fact, *supra* note 75, at 20.

130. Complaint at 7, Microsoft Corp. v. John Does 1–11, No. C11-0222 (W.D. Wash. Feb. 9, 2011) [hereinafter Rustock Complaint].

131. *Id.* at 13.

132. *Id.*

level, that the average user could not detect the infection or clean the malicious software from their computer without technical assistance.[133]

Microsoft identified 96 Rustock C&C servers located in the United States and named 5 data centers that hosted related botnet domains.[134] Similarly to the Waledac botnet takedown, Microsoft requested that the domains be blocked by third parties and removed from the zone root file in order to disrupt the communications of the botnet.[135] Before granting a preliminary injunction, the court requested legal authority for the order to non-party third parties.[136] Microsoft argued the All Writs Act of 1789 as the legal basis for the order, which states: "The Supreme Court and all court established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[137] Courts have used the All Writs Act as the basis for orders to third parties ranging from telephone companies that must participate in wiretaps, to individuals who must stop interfering with school desegregation.[138]

Another new development in the Rustock takedown was the seizure all of the computers, files, and related information from the location of the servers rather than focusing the remedy on the IP addresses; this was necessary because, "the masterminds behind Rustock designed their infected computers to receive instructions from Internet protocol addresses tied to specific command-and-control machines."[139] The court order allowed Microsoft attorneys and experts to accompany U.S. marshals during the seizure to determine the "computers, servers, electronic data storage devices, or media"[140] to be

133. Microsoft Corp.'s Application for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause Re Prelim. Inj. at 10–11, Microsoft Corp. v. John Does 1–11, No. C11-0222 (W.D. Wash. Feb. 9, 2011) [hereinafter Rustock TRO Application].

134. *See* Rustock Complaint, *supra* note 130, at 8.

135. *See* Rustock TRO Application, *supra* note 133, at 2.

136. Microsoft Supp. Brief in Support of Application for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause Re Prelim. Inj. at 1, Microsoft Corp. v. John Does 1–11, No. C11-0222 (W.D. Wash. Mar. 1, 2011) [hereinafter Rustock Supplemental Brief].

137. 28 U.S.C. § 1651(a) (2012).

138. *See* Rustock Supplemental Brief, *supra* note 136, at 2–3.

139. Nick Wingfield, *Spam Network Shut Down*, WALL ST. J. (Mar. 12, 2011, 12:01 AM), http://online.wsj.com/news/articles/SB10001424052748703328404576207173861008758.

140. Order for Prelim. Inj. at 8, Microsoft Corp. v. John Does 1–11, No. C11-0222 (W.D. Wash. Mar. 9, 2011).

seized. The premise for seizing the computers and related physical materials rested upon the "overwhelming risk" that the botnet would move to another location and continue its operation.[141] Importantly, the Lanham Act provided the legal basis for Microsoft's seizure of the offending articles and records because they were products of or related to trademark infringement.[142]

Thus, the Rustock case added legal specificity for court authority to order third parties to botnet takedowns by purging IP addresses and domain names from the Internet, and preserving evidence. Furthermore, it established the Lanham Act as a viable vehicle for Microsoft to seize physical botnet property and increased the ability of Microsoft to pursue the eradication of botnets through the civil system. As a result, security experts found that Rustock produced spam "nosedived,"[143] as the takedown was speculated to be the "largest takedown in the history of the Internet."[144] For example, one entity reported a decrease from one to two thousand Rustock spam emails per second, to merely one to two spam emails per second.[145]

B. Kelihos

In 2011, Microsoft sued an individual and limited liability company located in the Czech Republic, and John Does, in order to disable a botnet known as Kelihos.[146] While both known defendants were located outside of the United States, jurisdiction in the Virginia court was based on the business that they did in Virginia, the malicious code directed at persons in Virginia, and the continued botnet activity involving Virginia-based computers.[147]

---

141. *See* Rustock TRO Application, *supra* note 133, at 28.

142. Temporary Restraining Order and Seizure Order at 6–9, Microsoft Corp. v. John Does 1–11, No. C11-0222 (W.D. Wash. Mar. 9, 2011). Paragraph F of the order states that the seizure is authorized under § 1116(d) of the Lanham Act, however the judge added a handwritten note at the end of the order that "[a]ll actions undertaken under the authority of this Order shall be in strict compliance with 15 U.S.C. 1116," implying that the court was keenly aware of the significance of this action. *Id.* at 11.

143. *See* Brian Krebs, *Rustock Botnet Flatlined, Spam Volumes Plummet*, KREBS ON SECURITY (Mar. 18, 2011, 10:04 AM), http://krebsonsecurity.com/2011/03/rustock-botnet-flatlined-spam-volumes-plummet/.

144. *Id.*

145. *Id.*

146. Complaint at 1, Microsoft Corp. v. Piatti, No. 1:11-CV-1017 (E.D. Va. Sept. 22, 2011) [hereinafter Kelihos Complaint].

147. *Id.* at 6–7.

The owners of the two IP addresses had issued 21 subdomains that were an active part of the Kelihos botnet.[148] The Kelihos structure was similar to the Waledac botnet, and Microsoft used similar legal tactics and court proceedings to disable it, including orders to third parties to freeze and disable the domains and preserve evidence.[149] However, it added a negligence allegation to the action, arguing that the act of hosting subdomains and registering owners imposed a duty on the defendants not to allow the IP addresses and domain names to be used for malicious, botnet purposes; the basis of the duty being, among others, the "domain registration and IP hosting agreements and policies entered into by defendants . . . [in their] domain registration agreements."[150] Additionally, Microsoft alleged that the defendants knew about, assisted, and benefited from the malicious actions of the subdomain holders.[151]

Microsoft and the defendants settled the dispute, agreeing in a Consent Preliminary Injunction that the two defendants would "disable malicious subdomains and [adopt] a process to verify the identities of sub-domain registrants."[152] The Kelihos litigation is instructive in several aspects. First, geographical location of a defendant outside the United States is not necessarily an impediment to an effective legal action when the domain registry (in this case VeriSign), or registrar,[153] is located in the United States and thus subject to the court's jurisdiction. Due to the Internet infrastructure, a registry or registrar

148. *Id.*

149. *See Ex Parte* Temporary Restraining Order and Order to Cause Re Prelim. Inj. at 6–7, Microsoft Corp. v. Piatti, No. 1:11-CV-1017 (E.D. Va. Sept. 22, 2011). A larger number of third parties were subject to the order, including VeriSign (Va.), ARIN (Va.), ATT Internet Services (Tx.), Charter Communications (Mo.), Internet.bs Corp. (Bahamas), and Moniker Online Services (Cal.). *Id.* at app. A.

150. Kelihos Complaint, *supra* note 146, at 22.

151. *Id.* at 5.

152. Consent Prelim. Inj., Microsoft Corp. v. Piatti, No. 1:11-CV-1017 (E.D. Va. Oct. 12, 2011).

153. A registry operates the top-level domain addresses, such as .com in the case of VeriSign. *See .com Registry Agreement*, ICANN (Dec. 1, 2012), http://www.icann.org/en/about/agreements/registries/com. A registrar sells domain names to individuals. For a description of registrar responsibilities, see *Registrant Educational Materials*, ICANN, http://www.icann.org/en/resources/registrars/registrant-rights/educational (last visited Jan. 24, 2015). The Internet Corporation for Assigned Names and Numbers (ICANN), headquartered in the United States, is, in simple terms, the organization that coordinates the workings of Internet communication. *See generally Welcome to ICANN!*, ICANN, http://www.icann.org/en/about/welcome (last visited Jan. 24, 2015).

can take effective action to block the malicious domains or IP addresses from the Internet when ordered by a court of competent jurisdiction. Thus, even though not reaching an out-of-state defendant personally, a private action has the capability to reach the defendant's Internet presence by means of a court order to an in-state registry or registrar. Second, Microsoft served notice to those who facilitate, or turn a blind eye, to botnet activity that they would not be insulated from liability. Assuming that the defendants in the Kelihos case did not directly participate in the illegal activity or botnet structure of the domain holders, they were nonetheless instrumental in facilitating the activity. The Kelihos action was a lesson to those who sell Internet domains that they have a duty to see the obvious, and that they must have procedures to prevent illegal and malicious actors from operating in their domains.

C. Zeus

The Financial Services-Information Sharing and Analysis Center (FS-ISAC) and the National Automated Clearing House Association (NACHA) joined Microsoft as plaintiffs in a legal action in March 2012 to takedown the Zeus botnet.[154] The allegations stated that 13 million computers were involuntarily enlisted into the botnet, which was responsible for the theft of over $100 million in five years.[155] Using a botnet structure, the defendants tricked individuals into interacting with a fake web interface that looked very similar to one that the plaintiffs would ordinarily use.[156] During the interaction, malware would be surreptitiously and fraudulently installed that would steal the user's account logins, especially designed to steal online banking information.[157] The interface would also collect personal and financial information, and the installed malware would secretly and surreptitiously take money from customer bank accounts, even during

154. *See* Complaint, Microsoft Corp. v. John Does 1–39, No. CV12-1335 (E.D.N.Y. March 19, 2012) [hereinafter Zeus Complaint].

155. *Id.* at 1.

156. *Id.* at 13.

157. *Id.* at 20–21, 24–25 ("The websites of nearly every major financial institution, Microsoft and a wide array of other Internet companies have been targeted by the Defendants and the Zeus Botnets in this way."). The general name for this type of activity is phishing. *See Internet Crime Schemes*, INTERNET CRIME COMPLAINT CENTER, http://www.ic3.gov/crime schemes.aspx#item-14 (last visited Jan. 24, 2015). For further discussion about different methods of cyberattacks/weapons, see Gary D. Brown & Andrew O. Metcalf, *Easier Said Than Done: Legal Reviews of Cyber Weapons*, 7 J. NAT'L SECURITY L. & POL'Y 115, 120–27 (2014).

the customer's own online transaction, and wire it to a botnet owner's/agent's account.[158]

Zeus was a global, criminal operation controlled and coordinated by several individual creators[159] who sold the software code in 'builder kits' to other criminals.[160] This botnet as a service could be purchased for an amount between $700 and $15,000 depending on the sophistication of the software code.[161] One security firm called Zeus the "God of DIY [do-it-yourself] botnets" because of its ease-of-use, wide availability, and simple functionality.[162]

In addition to the previously established legal bases for a lawsuit against botnets, Microsoft alleged violations[163] of the Racketeer Influenced and Corrupt Organizations Act (RICO).[164] The interstate and international nature of the Internet was an unmistakable feature of the defendant's actions, and in furtherance of the criminal enterprise, the defendants not only stole financial access information and withdrew money from the victims' bank accounts, they also hired a network of "money mules" in the United States to move and store the stolen money among fraudulent bank accounts.[165]

The court granted an *ex parte* TRO and seizure order directing the US Marshall to seize evidence located in two US states; it also ordered redirection of botnet traffic to a Microsoft site, transfer of unregistered botnet names to Microsoft, disabling of IP addresses, and preservation of evidence.[166] The order to third parties was directed to registries and others in the United States under the All Writs Act.[167] ICANN, located

158. *See* Zeus Complaint, *supra* note 154, at 25.

159. *Id.* at 2–9.

160. *Id.* at 15.

161. *Id.*

162. *See* Doug Macdonald, *Zeus: God of DIY Botnets*, FORTIGUARD, http://www.fortiguard.com/legacy/analysis/zeusanalysis.html (last visited Jan. 24, 2015) (providing a technical description of how a botnet is designed and operates).

163. *See* Zeus Complaint, *supra* note 154, at 35–37.

164. Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(c)–(d) (2006). For an excellent discussion of RICO's international reach, including the necessity to tackle cybercrime through the use of this statute, see Gideon Mark, *RICO's Extraterritoriality*, 50 AM. BUS. L.J. 543, 583–85 (2013).

165. *See* Zeus Complaint, *supra* note 154, at 36.

166. *See Ex Parte* Temporary Restraining Order, Seizure Order and Order to Show Cause Re Prelim. Inj., Microsoft, Corp. v. John Does 1–39, No. CV12-1335 (E.D.N.Y. Mar. 19, 2012) [hereinafter Zeus TRO].

167. *Id.* at 10–11.

in the United States, was directed to forward the Order to identified foreign registries.[168] The Preliminary Injunction more explicitly provided for international cooperation, stating; "This Court respectfully requests, but does not order, that foreign domain registries and registrars take reasonable steps to work with Plaintiffs to ensure that Defendants cannot use the Appendix A domains to control the botnet."[169]

The court added a provision in the order to compensate the registries and associated entities for their actions to block the traffic and preserve evidence, according to "prevailing rates for technical assistance."[170] In addition, the court instructed that the orders be carried out with the "least degree of interference with the normal operation" of the Internet intermediaries as possible.[171]

It is noteworthy in the development of legal precedent that Microsoft cited previous courts' actions in Waledac, Rustock, and Kelihos, in its proposition that; "The requested *ex parte* relief is not uncommon when disabling dangerous botnets."[172] In contrast to the proposition that legal actions to takedown botnets were becoming standard operating procedure, a significant controversy over Microsoft's tactics erupted outside of the courtroom, in at least part of the security community.[173] When Microsoft took control of the identified, compromised domain traffic, it affected some sites maintained by security researchers who were watching and learning from the Zeus operation, in the same way that Microsoft planned to do with its court approved "sinkholing" of the websites.[174] A security firm in the Netherlands also claimed that Microsoft had used information shared on a private security listserv, without permission from its authors, and that its civil action had interfered with ongoing criminal

168. *Id.* at 11–12.

169. Order for Prelim. Inj. at 5, Microsoft Corp. v. John Does 1–39, No. CV12-1335 (E.D.N.Y. Mar. 29, 2012).

170. *See* Zeus TRO, *supra* note 166, at 14.

171. *Id.* at 9. The court also prohibited Microsoft from accessing the content of traffic that was redirected to their servers, except for domain name identification. *Id.* at 10.

172. Brief in Support of Plaintiffs' Application of for [sic] an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause for Prelim. Inj. at 2, Microsoft Corp. v. John Does 1–39, No. CV12-1335 (E.D.N.Y. Mar. 19, 2012).

173. *See* Michael Sandee, *Critical Analysis of Microsoft Operation B71*, FOX IT (Apr. 12, 2012), http://blog.fox-it.com/2012/04/12/critical-analysis-of-microsoft-operation-b71/.

174. *Id.*

investigations.[175] In response, Microsoft's counsel explained the legal necessity of keeping the number of people involved to a minimum in order to obtain an *ex parte* order, and defended its "disruptive" strategy as a beneficial supplement to criminal proceedings that were difficult to pursue.[176] The public debate about Microsoft's legal strategy to takedown Zeus illustrated a rift in the international security community over the role and effectiveness of private civil actions.[177]

D. Nitol

In September 2012, Microsoft targeted the takedown of the Nitol botnet that utilized an Internet domain from China.[178] Through its domain, 3322.org, the defendants hosted subdomains that comprised the Nitol botnet, a botnet that produced spam and fraudulent emails, and precipitated theft and other illegal activities; it was also capable of a large scale [distributed] denial-of-service attack.[179] The software was extremely difficult to remove, and could log user keystrokes as well as turn on the computer's camera to observe the user.[180] Interestingly, Microsoft discovered the operation of the botnet by accident, when it was testing the extent of unlicensed software sold in new computers in China. After buying new computers for testing, it found that one of the computers was infected with malware, right out of the box; as soon as it was turned on it immediately connected to the Internet and automatically started sending communications to the botnet command and control for instructions.[181]

The Nitol botnet was especially damaging to users because it spread by means of physical devices such as thumb drives, as well as through Internet connections.[182] Furthermore, it ran in the background of computer processing, unknown to the user. Analysis of the 3322.org domain found that it hosted a variety of malware, and allowed criminals

175. *Id.*

176. *Id.*

177. *See infra* Part VI.

178. *See* Complaint, Microsoft Corp. v. Peng Yong, No. 1:12-CV-1004 (E.D. Va. filed Sept. 10, 2012) [hereinafter Nitol Complaint].

179. *Id.* at 12, 19.

180. *Id.* at 5.

181. *Id.* at 5–6.

182. *Id.* at 10.

to avoid detection by using the 3322.org as the central place to direct communications to other, changing, domain names.[183]

The complaint contained allegations of violations of the CFAA, trespass to chattels, unjust enrichment, conversion, and negligence.[184] Microsoft alleged that "the massive scale of the problem shows that they [the defendants] are knowingly engaged in such [illegal botnet] activity and/or negligently failing to take reasonable steps to deter such activity."[185] The claim for negligence, similar to Kelihos, argued that the contractual registration agreements obligated the defendants to take reasonable care to avoid illegal actions, and that the breach of that duty was the cause of damages to Microsoft.[186] The court granted the *ex parte* TRO and order that granted Microsoft control over the domain, establishing a server for the purpose of forwarding the illegal traffic (a sinkhole).[187]

The dispute was resolved without further court action, and a release and settlement agreement entered into between Microsoft and the defendants.[188] The defendants agreed "to work in cooperation with Microsoft and the National Computer Network Emergency Response Technical Team Coordination Center of China"[189] (China CERT) to relaunch the domain, and to block the sub-domains identified as belonging to the botnet (provided by Microsoft or the China CERT) by redirecting them to a sinkhole maintained by MS or the China CERT and by adopting a "publicly-published policy of zero tolerance for illegal activities" on the domain.[190] In consideration of those promises, Microsoft agreed to return the control of the domains to the parties.[191]

---

183. *Id.* at 16.

184. *Id.* at 1.

185. *See* Brief in Support of Application of Microsoft Corp. for an Emergency Temporary Restraining Order and Order to Show Cause Re Prelim. Inj. at 3, Microsoft Corp. v. Pen Yong, No. 1:12-CV-1004 (E.D. Va. Sept. 10, 2012).

186. *See* Nitol Complaint, *supra* note 178, at 23.

187. *See Ex Parte* Temporary Restraining Order and Order to Show Cause Re Prelim. Inj. at 5–6, Microsoft Corp. v. Peng Yong, No. 1:12-CV-1004 (E.D. Va. Sept. 10, 2012).

188. *See* Notice of Voluntary Dismissal of Defendants Peng Yong; Changzhou Bei Te Kang Mu Software Tech Co. Ltd; and John Does 1–3 at app. A, Microsoft Corp. v. Peng Yong, No. 1:12-CV-1004 (E.D. Va. Sept. 29, 2012).

189. *Id.* at 1.

190. *Id.* at 2.

191. Non-Confidential Release and Settlement Agreement (Sept. 24, 2012) at 2–3 (on file with the author).

The Nitol botnet action was unique because of its genesis in the supply chain. As the case developed, international cooperation by Chinese authorities and Chinese CERT proved uniquely valuable for settling the case and essential for an effective resolution. While some security commentators questioned whether the settlement would be effective, as criminals would simply move to another dynamic domain name provider,[192] the Nitol lawsuit aimed at a different level—administration within the Internet infrastructure. While MS had control of the domain, it identified 70,000 malicious subdomains operating in connection with 500 strains of malicious software.[193] MS operated a sinkhole for 16 days, during which "it blocked more than 609 million connections from more than 7,650,000 unique IP addresses."[194] Yet at the same time, the domain facilitated almost 35 million valid requests.[195] Thus, the settlement is important not only as part of the fight against criminal activity, but also as a lesson about the responsibility of Internet intermediaries for overall security and safety.

E. Bamital

The primary purpose of the Bamital botnet was click fraud and browser hijacking.[196] Bamital malware enrolled a computer in the botnet and ran without the user's knowledge in the background, clicking on ads in order to earn money per click, and redirecting user search results to unintended websites and ads.[197] The design of the malicious software in a modular fashion meant that the botnet could

192. *See* Paul Ducklin, *Microsoft Settles Lawsuit Against 3322 dot org*, NAKEDSECURITY (Oct. 5, 2012), http://nakedsecurity.sophos.com/2012/10/05/microsoft-settles-lawsuit-against-3322-dot-org/.

193. *See* Kelly Jackson Higgins, *Microsoft Hands Off Nitol Botnet Sinkhole Operation To Chinese CERT*, INFORMATIONWEEK DARKREADING (Oct. 2, 2012, 1:41 PM), http://www.darkreading.com/end-user/microsoft-hands-off-nitol-botnet-sinkhol/240008324.

194. *Id.* "A botnet sinkhole is a target machine used by researchers to gather information about a particular botnet. Sinkholing is the redirection of traffic from its original destination to one specified by the sinkhole owners. The altered destination is known as the sinkhole." *See Botnet Sinkhole*, TECH TARGET (June 2014), http://whatis.techtarget.com/definition/botnet-sinkhole.

195. *See* Higgins, *supra* note 193.

196. *See* Complaint at 15, Microsoft Corp. v. John Does 1–18, No. 1:13-CV-139 (E.D. Va. Jan. 31, 2013) [hereinafter Bamital Complaint].

197. *Id.* at 16.

easily be used for other criminal and malicious purposes.[198] The motivation for taking down this particular botnet related, in part, to the damage that click fraud presents to online advertising platforms, and the Microsoft Bing search and ad business in particular. Bamital was estimated to produce 3 million fraudulent clicks daily, costing Microsoft millions of dollars of damage in lost revenue, as well as incalculable damage to its reputation.[199]

In October, 2013, MS[200] followed its previously established framework for using the legal system to help takedown the Bamital botnet, seeking an *ex parte* proceeding, third party orders, seizures of physical evidence, and preliminary injunctions.[201]

As each botnet takedown was successfully pursued through legal means, the cumulative nature of prior cases built stronger precedent for the requested relief.[202] The Bamital Preliminary Injunction ordered a long list of registered domains in the botnet to be redirected to a server controlled by Microsoft, and another long list of unregistered domains to be directly transferred to Microsoft as the registrant.[203] This allowed Microsoft to take control of Bamital and to thwart its continued spread.

Third parties who were needed to assist in blocking the domains included registries, registrars and subdomain hosting entities. Not only were these third parties, such as VeriSign, located in the United States, but they also included the National Internet Exchange in India, the Public Interest Registry in charge of .org registrations, and administrators/hosts of domains in South Korea, Czech Republic, and

198. *See Bamital Bites the Dust*, SYMANTEC CONNECT BLOG (Feb. 6, 2013, 7:09 PM), http://www.symantec.com/connect/blogs/bamital-bites-dust. For further information about the structure of Bamital, see PIOTR KRYSIUK & VIKRAM THAKUR, TROJAN.BAMITAL (2013).

199. *See id.* at 7.

200. Microsoft partnered with Symantec, whose security software update was affected by the botnet. *See* Richard Domingues Boscovich, *Microsoft and Symantec Take Down Bamital Botnet That Hijacks Online Searches*, OFFICIAL MICROSOFT BLOG (Feb. 6, 2013), http://blogs.technet.com/b/microsoft_blog/archive/2013/02/06/microsoft-and-symantec-take-down-bamital-botnet-that-hijacks-online-searches.aspx.

201. *See* Brief in Support of Application of Microsoft Corporation for an Emergency Temporary Restraining Order, Seizure Order, and Order to Show Cause Re Prelim. Inj. at 3–4, Microsoft Corp. v. John Does 1–18, No. 1:13-CV-139 (E.D. Va. Jan. 13, 2013).

202. *Id.* at 3–5.

203. Prelim. Inj. at 7–8, Microsoft Corp. v. John Does 1–18, No. 1:13-CV-139 (E.D. Va. Feb. 13, 2013). Surrender of computers and evidence held by hosting companies was also ordered. *Id.* at 9.

the Netherlands.[204] Bamital owners, first named as John Does, were eventually identified as Marat Marynskij from either Lithuania or Belarus, and Dmitry Chupkhim of Russia.[205]

Microsoft reported that by working with ICANN, registrars, and international organizations it was able to block over 7,000 domains from being registered for use in Bamital.[206] MS acknowledged the cooperation of the Indian CERT in the cleanup efforts, as they facilitated the user notices so that cleanup tools could be made available.[207] In an important additional extension of the strategy to remediate malicious botnets, Microsoft adopted a proactive cleanup program for user computers; for the first time it notified users *directly*, and provided tools for the user to uninstall the botnet software.[208]

As the above descriptions of the botnet civil cases indicate, Microsoft did not act solely on its own. There was an evolution, however, in the most recent botnet actions, as coordinated, cooperative efforts with law enforcement were featured as a new method for tackling cybercrimes instigated by botnets.

IV. COLLABORATIVE TAKEDOWNS

The Citadel and ZeroAccess botnet actions were distinct from the first five actions led by Microsoft, not because of the legal arguments or basis for the civil lawsuit, but because of the extensive coordination in pursuing the botnet operators. Microsoft called its Citadel case in June 2013, its "most aggressive botnet operation to date,"[209] as it included collaboration with the FBI, financial services entities, and the Financial Services Information Sharing and Analysis Center. The FBI

204. Complaint at 6–7, Microsoft Corp. v. John Does 1–18, No. 1:13-CV-139 (Jan. 31, 2013).

205. Amended Complaint at 2, Microsoft Corp. v. Maznskij, No. 1:13-CV-139 (E.D. Va. June 17, 2013).

206. Microsoft Corporation's Status Report at 2, Microsoft Corp. v. John Does 1–18, No. 1:13-CV-139 (E.D. Va. Mar. 15, 2013).

207. Richard Domingues Boscovich, *Bamital Botnet Takedown is Successful; Cleanup Underway*, OFFICIAL MICROSOFT BLOG (Feb. 22, 2013) http://blogs.technet.com/b/Microsoft_blog/archive/2013/02/22/bamital-botnet-takedown-is-successful-clean-up-underway.aspx.

208. *Id.*

209. *See* Richard Domingues Boscovich, *Microsoft Works With Financial Services Industry Leaders*, OFFICIAL MICROSOFT BLOG (June 5, 2013), http://blogs.technet.com/b/microsoft_blog/archive/2013/06/05/microsoft-works-with-financial-services-industry-leaders-law-enforcement-and-others-to-disrupt-massive-financial-cybercrime-ring.aspx.

acted separately, but in coordination with, the civil action.[210] In addition, the FBI provided communication with foreign law enforcement agencies in order to encourage voluntary worldwide action against the botnet.[211] The FBI touted the collaborative nature of the pursuit of Citadel, stating that:

> Creating successful public-private relationships—in which tools, knowledge, and intelligence are shared—is the ultimate key to success in addressing cyber threats and is among the highest priorities of the FBI. We must ensure that, as cyber policy is developed, the ability of the private sector to coordinate in real time with the FBI is encouraged so that a multi-prong attack on our cyber adversaries can be as effective as possible.[212]

In the second coordinated effort, undertaken at the end of 2013, the collaboration extended across the globe, including European country law enforcement, Europol, and industry partners, among others.[213] These two cases arguably represent the current best practice of cyberdefense against botnets, the culmination of an evolution in legal strategy involving civil and criminal actions.

A. Citadel

In June 2013, Microsoft's coordinated action tackled the Citadel family of botnets, dismantling over 1,400 *unique* botnets.[214] As the FBI explained the timeline of events, "Microsoft exercised its independent civil authorities in this matter. The company then coordinated with the FBI and other private parties."[215] The Citadel botnet stole online banking passwords by employing techniques similar to the Zeus botnet.[216] Also similarly, the creator of the software sold it prepackaged, in "builder kits" for an approximate price of $2,400.[217]

---

210. *FBI Statement on Botnet Operation*, FBI NEWS BLOG (June 5, 2013, 7:00 AM), http://www.fbi.gov/news/news_blog/botnets-101/fbi-statement-on-botnet-operation.

211. *Id.*

212. *Id.*

213. *See* Richard Domingues Boscovich, *Microsoft, Europol, FBI and Industry Partners Disrupt Notorious ZeroAccess Botnet That Hijacks Search Results*, OFFICIAL MICROSOFT BLOG (Dec. 5, 2013), http://blogs.technet.com/b/microsoft_blog/archive/2013/12/05/microsoft-europol-fbi-and-industry-partners-disrupt-notorious-zeroaccess-botnet-that-hijacks-search-results.aspx.

214. *Id.*

215. *FBI Statement on Botnet Operation*, *supra* note 210.

216. Complaint at 7, Microsoft Corp. v. John Does 1–82, No. 3:13-CV-319 (W.D.N.C. May 29, 2013) [hereinafter Citadel Complaint].

217. *Id.* at 8.

The perpetrators of the Citadel botnet were organized in a "single global criminal operation"[218] that managed distribution chains, offered customer services, and sought continual improvement;[219] functions eerily like those of management practices in mainstream organizations. Among other allegations, the RICO charges[220] seemed particularly well suited to the facts.

Two to five million computers were estimated to be infected with the Citadel malware, and the losses from the theft of money from bank accounts was called "staggering."[221] The "particularly sophisticated and destructive botnet enterprise"[222] illustrated that botnet operators could evolve in reaction to defensive actions that sought to disable its reach. Bots checked for instructions every 20 minutes and the botnet controllers could update bots "almost instantaneously."[223] The users' computers in a Citadel botnet were continuously monitored for online banking operations, and whenever the opportunity arose, the malware would steal passwords, account logins, and customer access information.[224] In addition, the malware blocked automated security updates on the user's computer, and prevented the user from manually accessing security websites; the result was an impossible situation for infected users who could not disentangle themselves from the claws of the botnet.[225]

As in past botnet operations, except perhaps with more detailed instructions, Microsoft received an *ex parte* TRO that allowed it to, with orders to third party Internet entities for implementation, take control of currently registered harmful domains and operate them in place of the botnet controller, warehouse unregistered harmful domains, and seize servers and other evidence.[226] Beyond these now well-established procedures, Microsoft took the proactive step of

218. *Id*. at 7.

219. *See id*. at 8–11.

220. *See id.* at 12–14.

221. Brief in Support of Microsoft's Ex Parte Application for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause Re Prelim. Inj. at 1, Microsoft Corp. v. John Does 1–82, No. 3:13-CV-319 (W.D.N.C. May 29, 2013).

222. *Id*. at 2.

223. *See* Citadel Complaint, *supra* note 216, at 22.

224. *Id*. at 7.

225. *Id*. at 22.

226. *See Ex Parte* Temporary Restraining Order and Order to Show Cause Re Prelim. Inj. at 11–17, Microsoft Corp. v. John Does 1–82, No. 3:13-CV-319 (W.D. N.C. May 29, 2013).

obtaining the right for a Microsoft server to send instructions to bots that would "stop the harmful acts of the Citadel botnet malicious software," allow the computer to connect to security anti-virus websites, and direct the bot to a substituted the Microsoft server.[227] After two weeks, Microsoft could implement step two for those computers that continued to be infected with the Citadel malware; when an infected user accessed a browser, it was locked into a curative-notice website for twenty minutes where the only thing that the user could do was stay on that site or go to an anti-virus website.[228] In the case of an obstinate user, step three allowed Microsoft to run the curative website on the user's computer for "up to one twenty minute period every five hours for one twenty-four period once per week, until such time as Microsoft deems it on longer necessary to prompt the owners of such infected end-user computers to take the steps necessary to cleanse them of the Citadel botnet infection."[229] The legal basis for the court order was that the actions were "consistent with the terms of Microsoft's license to its Windows operating system."[230]

The Citadel remediation action was reminiscent of the Coreflood botnet order that substituted a DoJ server for the command server and allowed the FBI to send a notice to infected users that would also uninstall the malware on an individual's computers with express consent. The Microsoft remediation went further; it modified admittedly malicious code on a user's computer without explicit consent and interfered for a short, yet increasingly intrusive, time with the user's access to the Internet. The remediation efforts generally brought praise,[231] however, like the Coreflood operation, it was not without its critics. A segment of the security community decried that Microsoft had included security domain names among the group of harmful names it sinkholed, and questioned Microsoft's methodology

227. *Id.* at 20.

228. *Id.* at 20–21.

229. *Id.* at 21.

230. *Id.* at 19. The court order did not explain further; presumably the reference was to the authority under the license to install updates.

231. *See, e.g.*, Paul Ducklin, *FBI and Microsoft in Massive Takedown of Citadel Botnets*, NAKEDSECURITY (June 6, 2013), http://nakedsecurity.sophos.com/2013/06/06/fbi-and-microsoft-in-massive-takedown-of-citadel-crimeware/.

of inserting a "stop" command into the malware on a user's computer.[232] As explained:

> Microsoft ensures that once a bot connects to their sinkhole it stays there and won't try to reach out to a different C&C. In theory, this is a very good idea and I have to say that many sinkhole operators had the same thought years ago. But unlike Microsoft, most of the sinkhole operators came to a different conclusion: Sending out valid configuration files de facto changes settings of a computer without the consent or knowledge of the user (computer owner). In most countries, this is violating local law.[233]

The weak point in this criticism is that Microsoft did not act unilaterally as the security researcher implies; it obtained prior court approval. It respected the rule of law, was not taking part in unilateral offensive action, and followed established legal procedures. In sum:

> The act of writing up a complaint, backing it up with declarations in support of the plaintiff's motions, and having a federal judge review and grant plaintiff's motions is a very clear, very thorough, and very public justification for taking bold action. This process explains of [sic] who is being harmed, how they are being harmed, what can be done to stop the harm, and why the court should grant the plaintiff's motions.[234]

B. ZeroAccess

The ZeroAccess botnet engaged in click fraud, identity theft, and DoS attacks.[235] Although click fraud might seem to be one of the least harmful actions that a botnet can take, it significantly damages business models for online advertising; criminals can steal millions of dollars a year in this manner.[236] Online advertising amounted to $20.1 billion in the first half of 2013 alone, based in large part on payment for clicks on ads that were delivered, among others, by Microsoft's Bing search

---

232. *See Collateral Damage: Microsoft Hits Security Researchers Along With Citadel*, SWISS SEC. BLOG (June 7, 2013), http://www.abuse.ch/?p=5362.

233. *Id.* No examples were given of what specific laws might be violated. For a study of the legal issues involved from a European Union viewpoint, see VIHUL ET AL., *supra* note 8, at 8–16.

234. David Dittrich, *Thoughts on the Microsoft's "Operation b71" (Zeus Botnet Civil Legal Action)*, HONEYNET PROJECT (Mar. 28, 2012, 4:56 AM), http://www.honeynet.org/node/830.

235. Complaint at 13, Microsoft Corp. v. John Does 1–8, No. A13-CV-1014SS (W.D. Tex. Nov. 25, 2013) [hereinafter ZeroAccess Complaint].

236. *Id.* at 9.

engine.[237] The ZeroAccess botnet hijacked browsers on infected computers to click on ads and fraudulently collect payment for the clicks while uninstalling and blocking security upgrades.[238] In addition, ZeroAccess also interacted with Zeus purveyors from the former botnet so that it was surmised that the Zeus controllers were attempting to restart their botnet by piggybacking on ZeroAccess infections. [239]

ZeroAccess utilized eighteen servers located in Latvia, Luxembourg, Switzerland, the Netherlands, and Germany.[240] Taking down this botnet in November 2013, therefore required global cooperation between public and private entities. While Microsoft was able to file suit in a civil action in Texas due to tens of thousands of compromised computers there,[241] the international reach of the botnet required a coordinated effort with the FBI, Europol's European Cybercrime Centre, and industry partners.[242]

The ZeroAccess botnet architecture differed from some of the previous botnets, as it operated by means of a P2P system whereby each bot communicated directly with other bots in order to update the malware and pass on instructions.[243] Each time a bot connected with another bot it asked for instructions and updates; in that way the viral communications reduced the necessity of continual communication with a central C&C server. Peers did contain a list of IP addresses that changed regularly, which provided further instructions to implement click fraud. In addition, a larger number of domain names were provided as backup locations for instructions should the IP addresses, located with static servers internationally, fail to respond.[244] By not

237. *Id.* at 8–9.

238. *Id.* at 15–16. In addition, ZeroAccess ran silently on a user's computer. Except perhaps for a slowdown in processing, the user would have no idea that the malware was running in the background while he was using the computer for other functions. *Id.* at 15.

239. *See* Brief in Support of Application of Microsoft Corp. for an Emergency Ex Parte Temporary Restraining Order and Order to Show Cause Re Prelim. Inj. at 15, Microsoft Corp. v. John Does 1–8, No. A13-CV-1014SS (W.D. Tex. Nov. 25, 2013) [hereinafter ZeroAccess Brief] ("In spite of these concerted efforts and successes [botnet civil actions] branches of the Zeus botnet live on, and the operators of Zeus are evidently using ZeroAccess-generated traffic to infect more computer in an attempt to rebuild their criminal enterprise.").

240. *See Ex Parte* Temporary Restraining Order and Order to Show Cause Re Prelim. Inj. at 4–5, Microsoft Corp. v. John Does 1–8, No. A13-CV-1014SS (W.D. Tex. Nov. 25, 2013) [hereinafter ZeroAccess TRO].

241. *Id.*

242. Boscovich, *supra* note 213.

243. *See* ZeroAccess Complaint, *supra* note 235, at 12.

244. *Id.* at 14.

employing a C&C infrastructure alone, the ZeroAccess botnet was much more difficult to disarm; as Microsoft explained; "Due to its network architecture, ZeroAccess is one of the most robust and durable botnets on the Internet today."[245] A layered strategy was necessary for an effective takedown. The IP addresses were all maintained on servers outside the United States, therefore the court could only request, not order, that the hosting entities block access and cut off service.[246] In this aspect of the fight against ZeroAccess, the global collaboration with law enforcement agencies and other private parties was key. Secondly, the court ordered domain registries in the United States to redirect active botnet traffic (sinkhole) to Microsoft substitute servers, and to transfer any inactive botnet domain name to Microsoft.[247] The third part of the court order, and a new approach, directed forty-five ISPs in the United States to implement a block on traffic emanating from or directed to the botnet IP addresses.[248] ISPs operate at different levels; they are both the "on-ramp," or user-connection point, and they route Internet traffic from sender-to-destination.[249] ISPs voluntarily undertake website blocking from time-to-time, for example when they implement blacklists of websites that are known to send spam.[250]

When the botnet owners attempted to occupy and use substitute IP addresses and avoid a shutdown, Microsoft coordinated with its partners; "Europol's European Cybercrime Centre (EC3) took immediate action to coordinate with member country law enforcement agencies, led by Germany's Bundeskriminalamt's (BKA) Cyber Intelligence Unit, to quickly track down those new fraud IP addresses."[251] The botnet operators, evidently digitally surrendering, sent a final message to the infected computers simply stating "White Flag."[252]

---

245. *Id.*

246. *See* ZeroAccess TRO, *supra* note 240, at 10.

247. *Id.* at 11–12.

248. *Id.* at 8–9.

249. *See* OLIVER HECKMANN, THE COMPETITIVE INTERNET SERVICE PROVIDER 13 (David Hutchison ed., 2006).

250. *See About Spamhaus*, SPAMHAUS PROJECT, http://www.spamhaus.org/organization/ (last visited Apr. 21, 2014) (describing the organization, its blacklist of spam sites, and the use by ISPs).

251. Richard Domingues Boscovich, *ZeroAccess Criminals Wave White Flag*, OFFICIAL MICROSOFT BLOG (Dec. 19, 2013), http://blogs.technet.com/b/microsoft_blog/archive/2013/12/19/zeroaccess-criminals-wave-white-flag-the-impact-of-partnerships-on-cybercrime.aspx.

252. *Id.*

V. ANALYSIS

Cybersecurity is a complex, dynamic, and thorny problem. As proven by the botnet takedown cases, private entities can proactively use the civil legal system to lead and contribute to cybersafety. One of the goals of this article is to document Microsoft's legal strategy over the course of eight botnet takedowns so that it can be considered for future action by other private entities. Microsoft's civil suits against botnets used legal tools in an innovative way to tackle an intractable and thorny global problem. The legal approach reduced botnet activity, provided a valuable service to users with infected computers, and more broadly increased the level of cybersecurity. Regardless, the wisdom of private civil action is not unanimously praised; as one security expert stated: "The problem with cybercrime is that it can't be solved with doing takedowns. It's only possible to solve this issue by implementing legislation related to cybercrime, enforce them [sic] by getting bad actors arrested and implementing security by design on different layers."[253] Some believe that Microsoft has stepped outside the bounds of its position as a private party,[254] and that it is the role of legislatures and law enforcement to pursue criminals. In contrast, Microsoft proposes that civil lawsuits could be used by many private entities; the resulting increased cost of operating botnets would exert economic pressure on operators and thereby reduce the number of botnets due to those increased costs.[255]

The private sector's role in cybersecurity, and specifically the proactive legal role, deserves detailed analysis. The complex problems of public and private roles, jurisdictional boundaries, international cooperation, limited resources, and the technical sophistication of cyberattacks, will require further research. The outline of the Microsoft's legal suits against botnets provides a springboard for further analysis. To begin this analysis, the following discussion suggests four lenses for future research into understanding the wider impact of the takedowns: crimtorts, governance theory, strategic

253. Zeljka Zorz, *Microsoft Citadel Takedown Ultimately Counterproductive*, HELP NET SECURITY (Oct. 6, 2013), http://www.net-security.org/malware_news.php?id=2514 (result of takedowns is temporary).

254. *See* Collateral Damage, *supra* note 232; *see also supra* text accompanying note 233. The comments and reactions of security researchers to the interview with Richard Boscovich from Microsoft regarding the Zeus takedown were conflicting, and the topic of Microsoft, law enforcement, and the security industry roles was controversial. *See* Brian Krebs, *Microsoft Responds to Critics Over Botnet Bruhaha*, KREBS ON SECURITY (Apr. 16, 2012, 1:49 PM), http://krebsonsecurity.com/2012/04/microsoft-responds-to-critics-over-botnet-bruhaha/.

255. *Id.*

management, and international lenses. Each of these lenses provokes both unique questions and support for the sustainability of civil actions for cybersecurity.

A. Crimtorts Lens

Viewed broadly, the question regarding Microsoft's botnet takedown actions is whether the use of criminal law by means of law enforcement should be the authoritative vehicle for stopping cybercrime, and concurrently, what role if any the private sector should play. Rustad was one of the first scholars to promote a place for private enforcement actions against cybercrime in 2001, arguing that criminal law is "an inadequate institution of social control against cybercrime"[256] because of cybercrime's global reach, the lack of law enforcement resources, and constraints imposed by protecting civil liberties in the electronic environment,[257] reasons that persist today.[258] Rustad argues for a cast of private attorneys general, serving the public interest through private lawsuits that apply established tort law to new situations in cyberspace, punishing the wrongdoer by means of punitive damages rather than criminal penalties.[259] Rustad and his co-author Koenig previously developed the theory of the use of tort law to accomplish wider social benefits under the term "crimtort."[260] More recently, crimtort actions were described as "[c]ivil actions that concurrently fulfill the private function of compensating injured

256. *See* Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, 67 (2001).

257. *See id.* at 96–100.

258. *See* Gregory T. Nojeim, *Cybersecurity: Ideas Whose Time Has Not Come—And Shouldn't*, 8 J.L. & POL'Y FOR THE INFO. SOC'Y 408, 418–19 (2012) (arguing that government should work with the private sector rather than directly alter/impact Internet traffic).

259. *See* Rustad, *supra* note 256, at 104–06. One could argue that early cases against spam and trespass to chattels, and the *ebay v. Bidders Edge* case, would fall into the paradigm of a private attorney general; however, the public interest in those cases is not featured as it was in the botnet documents, and the effect of the actions was more localized and plaintiff-specific than the promotion of overall Internet and consumer safety as was the issue in the botnet cases. For a discussion of these earlier cases and tort law, see Guzman, *supra* note 97, at 534–38; *see also* Michael L. Rustad, *Torts as Public Wrongs*, 38 PEPP. L. REV. 433, 484 ("Tort law not only bridges a regulatory gap, but it also bridges the hiatus left by criminal law that lags well behind technological and social changes, such as Internet-related wrongdoing." (citations omitted)).

260. *See* Thomas Koenig & Michael Rustad, "*Crimtorts" As Corporate Just Deserts*, 31 U. MICH. J.L. REFORM 289, 315 (1998).

claimants while serving the broader public purpose of controlling socially harmful behavior. . . ."[261]

Microsoft's botnet enforcement actions are similar to the private attorney general role envisioned by Rustad. In order for it to gain the extraordinary *ex parte* action without notice, and a preliminary injunction, Microsoft relied on the positive public interest served by its actions, and in contrast, the irreparable harm that would be suffered should the request not be granted.[262] The briefs and court filings are, in fact, replete with references to the specific harms that individuals incur as a result of the botnet operations, from stolen funds, decreased computer functionality, to disabled security and future vulnerability. Undoubtedly, Microsoft's legal actions have benefitted the general public.

Microsoft pursued cybercriminals in the private attorney model, however there are distinctions between the modern pursuit of botnets and the previously envisioned private attorney general function. The concept of a private attorney general anticipates a consumer or environmental champion role, resulting in lawsuits against powerful corporations or institutions,[263] supplementing the effectiveness of but not supplanting government enforcement.[264] Although Microsoft cases evolved to include more explicit prior coordination with law enforcement, the cases turn the concept of the role of the large corporation around. Rather than the target of a private action to coerce publically beneficial behavior, the large corporation, Microsoft, was the leader of lawsuits to protect the public and to promote cybersecurity and safety.

Another difference between traditionally conceived tort remedies that promote the public good and the botnet cases is that Microsoft has evidently not been able to obtain damages from any of the defendants, most of who remain at large and many who remain unidentified. Therefore, cybercriminals will not be deterred by the imposition of either compensatory or punitive damages; a predicate to the theory of

261. Thomas H. Koenig, *Crimtorts: A Cure for Hardening of the Categories*, 17 WIDENER L.J. 733, 733 (2008).

262. *See, e.g.*, ZeroAccess Brief, *supra* note 239, at 23, 31.

263. *See generally* Nicholas DiMascio, *Credit Where Credit is Due: The Legal Treatment of Early Greenhouse Gas Emissions Reductions*, 56 DUKE L.J. 1587 (2007) (discussing impact of private nuisance suits brought against corporations).

264. *See* Gideon Mark, *Private FCPA Enforcement*, 49 AM. BUS. L. J. 419, 490–91 (2012) (discussing application of theory to the Foreign Corrupt Practices Act).

the effectiveness of the private attorney general. Microsoft's strategy to create an economic disincentive to wrongdoers by means of botnet disruptions may substitute in part for damages, but these economic damages are indirect and more difficult effect to measure. The crimtort or private attorney general theory may fit in the case of private civil actions against cybercrime, however further examination of the effect on cybercriminals is necessary. In addition, Microsoft has an inherent motivation to pursue civil actions against botnet operators who damage their reputation and harm their business model. Finding private entities that have as high a stake in the game as Microsoft will be difficult,[265] and the expansion of the private attorney general approach will depend upon attracting private parties who have the incentive to act similarly.

B. Governance Theory Lens

Traditional regulatory, governance theory assumes a top down and centralized system of laws and governmental implementation of those rules of behavior for society,[266] assumptions that are not reflected in Microsoft's leadership of the botnet takedowns. Yet cybercrime in general, and botnet crimes in particular, belong to an ecosystem that is difficult to govern and police, both technically and legally. Traditional governance theory may be insufficient to address the new environment.

Polycentric governance theory may provide a more appropriate lens through which to view cybersecurity actions.[267] The theory

265. Facebook cooperated with the FBI to takedown a botnet that spread through its users, providing users with software to uninstall the malware. However, Facebook did not file a civil suit or otherwise lead the effort in the way that Microsoft did. *See Facebook and the FBI Partner to Take Botnet Offline*, FACEBOOK SECURITY (Dec. 12, 2012, 12:05 PM), https://www.facebook.com/notes/facebook-security/facebook-and-the-fbi-partner-to-take-botnet-offline/10151134554125766.

266. *See* Lance Gable, *Evading Emergency: Strengthening Emergency Responses Through Integrated Pluralistic Governance*, 91 OR. L. REV. 375, 411 (2012). Scholars have distinguished between the traditional modes of *government* regulation and broader *governance*, as explained in Lisa Blomgren Bingham, *Collaborative Governance: Emerging Practices and the Incomplete Legal Framework for Public and Stakeholder Voice*, 2009 J. DISP. RESOL. 269, 274 (2009). However, the terms are used more generally in this article.

267. Other governance theories include new governance and deliberative democracy; a detailed discussion of different governance theories across disciplines is beyond the scope of this article. For a good overview of the theories, see Scott Burris et al., *Changes in Governance: A Cross-Disciplinary Review of Current Scholarship*, 41 AKRON L. REV. 1 (2008). *Compare* Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MINN. L. REV. 342, 344 (2004) ("The new governance model connotes a decentering of legal scholarship, challenging the traditional focus on formal regulation as the dominant locus of change."), *with* Bradley C. Karkkainen, *"New Governance" in Legal Thought*

assumes the devolution of complete state power and governance amid increased governance participation by non-state entities, a movement toward multiple sources of governance, and increased local power.[268] Some scholars cite global Internet governance as an example of this new type of governance.[269] Shackelford uses the lens of polycentric governance to propose a framework for cybersecurity that is approached most successfully by a multi-layered, multi-player, coordinated response.[270] The actions by Microsoft, its interactions with security firms and researchers, and its collaborations with law enforcement, deserve further study as they relate to polycentric governance and other governance theories. Microsoft may be able to play a role that focuses on the safety of the Internet without the need for more exacting criminal proof and criminal arrests. Attribution is a thorny problem[271] for bringing criminal charges, and private rather than criminal actions could be more effective. As is explained:

> Attribution, however, may be more important for government and law enforcement than for private sector organizations. Law enforcement, through their investigations, may strive for attribution so that the actual perpetrator may be prosecuted. Industry organizations, however, may be less concerned and may focus more on damage control and prevention—regardless of the actor or his motivations.[272]

In addition, private sector leadership to secure the Internet, especially when access to individual computers is required, can avoid the stigma and limitation of government access. The federal government's Conficker remediation drew criticism even though the

---

and in the World: Some Splitting as Antidote to Overzealous Lumping, 89 MINN. L. REV. 471 (2004) (asserting a reply to Lobel, taking issue with the consolidation of scholarship).

268. *See* Burris, *supra* note 267, at 15–19. *See also* KRISTIN M. FINKLEA & CATHERINE A. THEOHARY, CONG. RESEARCH SERV., R42547, CYBERCRIME: CONCEPTUAL ISSUES FOR CONGRESS AND U.S. LAW ENFORCEMENT 12 (2012).

269. *See* Burris, *supra* note 267, at 23. Additionally, Froomkin proposes that Internet standard adoption procedures could meet the deliberative discourse theory of Habermas. *See* A. Michael Froomkin, *Habermas@Discourse.Net: Toward a Critical Theory of Cyberspace*, 116 HARV. L. REV. 749 (2003).

270. Scott J. Shackelford, *Toward Cyberpeace: Managing Cyberattacks Through Polycentric Governance*, 62 Am. U. L. Rev. 1273, 1352–60 (2013).

271. For a complete view of attribution from cybercrime to military action, see Duncan B. Hollis, *An E-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 391–406 (2011). For a discussion of the issue of attribution for cyberwarfare, see Collin S. Allan, *Attribution Issues in Cyberspace*, 13 CHI. KENT J. INT'L & COMP. L. 55 (2013).

272. FINKLEA & THEOHARY, *supra* note 268, at 11.

court ordered the FBI not to access any files on computers that were freed from the botnet. More recently, National Security Agency surveillance has likely heightened concerns for government access to personal commuters, even though the circumstances are quite different; privacy from government intrusion is now a hotly contended issue. Whether individuals would trust the government or private entities more to respect their privacy while securing computers from cyberthreats deserves further scrutiny.[273]

More broadly, and related to the polycentric approach, the report of the Conficker virus workgroup showed that local and grassroots actions in the horizontal environment of cybersecurity inherently result in problems with trust, exacerbated by the extremely decentralized governance model.[274] Perhaps Microsoft's leadership was a prerequisite for an effective governance paradigm, although communications between those with security information will always be essential. Microsoft is evidently ready to assume this role, as in 2013 it created the Digital Crimes Unit and the Cybercrime Center, staffed by technical and legal experts, dedicated to tackling cybercrime.[275] Likewise, changing approaches to the botnet takedowns from a solely privately led civil suit, to the Citadel and ZeroAccess collaborations with law enforcement around the world, provide evidence that the governance of cybersecurity and the pursuit of cybercriminals have evolved towards an increasingly networked governance framework. Furthermore, in February of 2014 Microsoft announced that it signed Memorandums of Agreement with the Organization of American States, Europol, and FIS (banking and payment systems) that "establish a framework for collaboration . . . intended to spur collaboration"[276] to pursue cybercriminals.

273. In a recent survey, respondents did not trust large companies to protect their privacy in general; however, they trusted the NSA even less. *See* Jaikumar Vijayan, *Snowden Leaks Erode Trust in Internet Companies, Government*, COMPUTERWORLD (Apr. 4, 2014, 8:23 AM PT), http://www.computerworld.com/s/article/9247441/Snowden_leaks_erode_trust_in_Internet_companies_government.

274. *See infra* II.B.

275. *See Microsoft Unveils State-of-the-Art Cybercrime Center*, MICROSOFT NEWS CENTER (Nov. 14, 2013), http://www.microsoft.com/en-us/news/press/2013/nov13/11-14cybercrimecenterpr.aspx.

276. *See Microsoft Enters Into New Global Partnerships in Fight Against Cybercrime*, MICROSOFT NEWS CENTER (Feb. 12, 2014), http://news.microsoft.com/2014/02/12/microsoft-enters-into-new-global-partnerships-in-fight-against-cybercrime.

C. Strategic Management Lens

A broad definition of the strategic management of a firm is that it is a process by which a strategic plan is adopted, implemented, and revised in order to maintain a competitive advantage in the marketplace.[277] In this process, a company will not only identify its strategic strengths but it will seek to minimize its risks, or weaknesses.[278] Considering Microsoft's actions from a strategic management viewpoint, it makes sense for it to participate in, and it could be strategically astute for it to assume leadership of, efforts to combat the botnet plague. Botnets harm Microsoft's reputation by counterfeiting and mimicking its products, weakening its advertising business model through clickfraud, and creating a lack of trust in the safety of the Internet. Microsoft's competiveness could be hurt as a result.

Microsoft has never denied that its actions were not internally beneficial or proposed that there were no economic motives for its actions. With regards to its civil actions to dismantle botnets, a Microsoft lawyer, Richard Boscovich, explained, "We're not a charitable corporation, obviously. But there are some times when it makes good business sense to actually do good in the community as well. It's one for those intersections where business and being a good corporate citizen actually complements each other."[279] Thus, one could seek to understand Microsoft's actions from a business, strategic management, perspective.

Porter and Kramer's work in "creating shared value"[280] for business and society alike may prove relevant to the analysis. Shared value is conceptualized as distinct from corporate responsibility or philanthropy, as it "recognizes that societal needs, not just conventional economic needs, define markets."[281] A purely economic corporate perspective, on the other hand, leaves societal interests outside of the strategic box, as consumers are viewed only as a source of profit and "societal problems [as] . . . economic costs in the firm's value chain."[282] In comparison, the shared value approach promoted by Porter and

277. *See* Nedelle Grossman, *The Duty to Think Strategically*, 73 LA. L. REV. 449, 455–473 (2013) (relating strategy to the management of risk as well).

278. *Id.* at 459–61.

279. *See* Krebs, *supra* note 254.

280. *See* Michael E. Porter & Mark R. Kramer, *Creating Shared Value*, HARV. BUS. REV., Jan–Feb. 2011, at 62.

281. *Id.* at 65.

282. *Id.* at 68.

Kramer encourages firms to consider societal needs as an integral part of their corporate strategy and as a vehicle for growth. As a general example, the provision of cybersecurity products to consumers would benefit the firm by the sales of its products, but would benefit both the consumer *and* the firm by reducing the risks of online activities and contributing to safety in cyberspace. Furthermore, if the cybersecurity firm also engaged in education about cyber-secure practices, then both the firm and the consumer would share in the value of the cybersafety efforts; the firm may also benefit from a new market for cyberproducts as a result of the consumer awareness.

The Boscovich quote parallels the principle of shared value in some respect; both Microsoft and society in general have a common interest in reducing cybercrime, particularly crime facilitated by botnets. Few companies explicitly adopt the shared value approach, however, and while the societal and business benefit is evident in the pursuit of cybersecurity, it is unclear if Microsoft has reconceived its relationship in this way. Understanding Microsoft's actions, its relationship to corporate responsibility, shared value, and the relevance of its legal strategies for overall strategic management will require additional analysis as its botnet remediation continues to evolve.[283]

D. International Lens

International dimensions have been discussed in the concepts of polycentric governance and strategic management[284] and in the way in which nations across the globe have cooperated with Microsoft to voluntarily dismantle botnet structures.[285] The international questions deserve further analysis as relates to Microsoft's legal strategy and the role of private entities in cybersecurity.

The significant extent of cooperation by foreign courts and foreign law enforcement with Microsoft and US court requests correlates with the magnitude of the problem and the difficulty of resolution. While not impossible, it is difficult and time consuming for law enforcement to follow criminals across international boundaries. Criminals who

283. The use of law for strategic management purposes has been addressed by Constance E. Bagley, *Winning Legally: The Value of Legal Astuteness*, 33 ACAD. MGMT. REV. 378 (2008); Robert C. Bird, *Pathways of Legal Strategy*, 14 STAN. J.L. BUS. & FIN. 1 (2008); George J. Siedel & Helena Haapio, *Using Proactive Law for Competitive Advantage*, 47 AM. BUS. L.J. 641 (2010).

284. *See* discussions *infra* Parts VI.B–C.

285. For example, China's CERT cooperated in the Nitol case and the ZeroAccess case involved several countries' law enforcement agencies. *See* discussion *infra* Parts IV.D., V.B.

prey on individual consumers in foreign countries are particularly unlikely to be arrested, or followed, across international jurisdictional boundaries.[286] The resources and expertise are simply not available to the local entities who otherwise would be the ones most appropriately protecting the public.[287] U.S. courts also recognize their jurisdictional limitations; the Microsoft injunctions and orders included deferential requests for foreign cooperation to stop the spread of harmful botnets.[288] International criminal coordination between law enforcement could be viewed through a different lens, especially in the current environment of suspicion raised by National Security Agency surveillance.[289]

Whether Microsoft can continue its aggressive actions against cybercrime could depend on the international evolution of Internet governance, a complex issue with many different sides.[290] On March 14, 2014, the United States indicated that it would transfer to ICANN the U.S. Commerce Department/National Telecommunications and Information Administration's role in the functioning of the domain name system.[291] Public debate intensified around the announcement, and future developments are uncertain.[292] As the botnet cases show, Microsoft's strategy depends in part on the location of ICANN in the United States as a California incorporated entity. U.S. courts can exert jurisdiction and order ICANN to take measures to block and transfer domain names and IP addresses that are used for criminal purposes. If the Internet infrastructure changes more broadly so that major

286. *See* Danny Yadron, *Grappling With Cybercrime*, WALL ST. J., Apr. 21, 2014, at A3.

287. *Id.*

288. For example, see the discussion of the Nitol case *infra* Part IV.D.

289. *See* Tom Brewster, *Has the NSA's Mass Spying Made Life Easier for Digital Criminals?*, THE GUARDIAN (Mar. 7, 2014, 7:37 AM EST), http://www.theguardian.com/technology/2014/mar/07/nsa-spying-harmed-digital-crime-fight.

290. For a concise historical background to some of the changes in governance, see Jonathan Weinberg, *Governments, Privatization, and "Privatization": ICANN and the GAC*, 18 MICH. TELECOMM. & TECH. L. REV. 189 (2011).

291. *See* Press Release, Nat'l Telecomm. & Info. Admin., NTIA Announces Intent to Transition Key Internet Domain Name Functions (Mar. 14, 2014), *available at* http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions; *see also* Loretta Chao et al., *U.S. Hopes to Soothe Cyberspying Tensions as Web Summit Looms*, WALL ST. J., Apr. 22, 2014, at B3 (reporting that international distrust based on NSA surveillance led to a U.S. proposal to transfer control of Internet addressing).

292. *See, e.g.*, Denver Nicks, *Republicans Don't Want America to Give Up Control of Web Addresses*, TIME (Apr. 10, 2014), http://time.com/58277/republicans-dont-want-america-to-give-up-control-of-web-addresses/.

structural entities, such as ICANN or VeriSign, are not located in the United States then Microsoft will effectively lose its legal strategy to dismantle botnets.[293] The relationship between ICANN, the United States, and the international community will continue to evolve; the Microsoft botnet cases illustrate one reason why Internet governance and infrastructure decisions are important to the future of cybersecurity.

CONCLUSION

This article contributes to an understanding of the role of the private sector in cybersecurity by chronicling civil lawsuits brought by Microsoft to takedown botnets, and by comparing the evolution of these takedowns to two different efforts, by law enforcement and an informal security group. The botnet takedowns by Microsoft have been subject to both praise and criticism, and some charged that Microsoft has acted as a "vigilante."[294] Microsoft's efforts have evolved, however, to be significantly integrated with law enforcement efforts, as the most recent Citadel and ZeroAccess lawsuits illustrate. Microsoft heralded its Citadel operation as a success, and as the emergence of a new framework, describing the action as "a real world example of how public-private cooperation can work effectively within the judicial system, and how 20th-century legal precedent and common law principles dating back hundreds of years can be effectively applied toward 21st-century cybersecurity issues."[295] The FBI also recognizes the heightened importance of public private partnerships and international coordination. [296]

"Going it alone," as Microsoft did in the series of cases before the Citadel and ZeroAccess botnet takedowns, has its risks. In takedown efforts occurring after this article was in production, Microsoft obtained an *ex parte* order allowing it to take control of 22 domains of

293. *See supra* note 153 and accompanying text describing the relationship of registries and domain names, and how this relates to the takedown of botnets.

294. *See* Dittrich, *supra* note 234; John Leyden, *Microsoft Botnet Smackdown 'Caused Collateral Damage, Failed to Kill Target,'* THE REGISTER (June 13, 2013, 12:59 PM), http://www.theregister.co.uk/2013/06/13/ms_citadel_takedown_analysis.

295. *See* Boscovich, *supra* note 209.

296. *See* Richard P. Quinn, Nat'l Sec. Assistant Special Agent In Charge, FBI, Statement Before the House Homeland Security Committee, Subcommittee on CyberSecurity, Infrastructure Protection, and Security Technologies (Apr. 16, 2014), *available at* http://www.fbi.gov/news/testimony/the-fbis-role-in-cyber-security.

No-IP, based on evidence that subdomains were involved in botnet activity. Microsoft was unable, however, to handle the traffic of innocent users, and reportedly blocked 5 million valid users.[297] Days later, Microsoft and Vitalwerks, the parent of No-IP, announced that the domains had been restored and the dispute was settled.[298] Criticism of Microsoft's failure ensued, tempered by praise for the results of the takedown, and spurring debate about private entities' proper role in addressing cybercrime.[299]

In the ultra-connected, electronically dependent world, botnets threaten the security of countries, people, and industries, because they are the vehicle for criminals, and potentially nation states, to disrupt society, harm privacy, commit fraud and theft, and seed distrust of the marketplace and Internet communications. Because of their commodification, botnets are easy to launch, and proliferate easily. Yet botnet defensive technology continues to strengthen, making them difficult to defeat through only technical counter measures. The evolution of a combination of technical methods, international collaborations, and legal strategies to defeat botnets shows promise for success. The active leadership of the private sector, using the legal system, will certainly be a component of future cybersecurity frameworks; understanding the dynamics and coordination of these relationships, and the limits of the applicable laws, will deserve future examination. For the present, the addition of a civil legal strategy to disrupt botnets to the many technical efforts by public and private parties to do the same strengthens cybersecurity and is becoming a powerful tool to fight cybercrime globally.

297. Nate Cardozo, *What Were They Thinking? Microsoft Seizes, Returns Majority of No-IP.com's Business*, ELECTRONIC FRONTIER FOUNDATION (July 10, 2014), http://www.eff.org/deeplinks/2014/07/microsoft-and-noip-what-were-they-thinking.

298. Natalie Goguen, *Vitalwerks and Microsoft Reach Settlement*, NO-IP.COM (July 9, 2014), http://www.noip.com/blog/2014/07/09/vitalwerks-microsoft-reach-settlement.

299. Tim Ring, *MS No-IP Takedown Hits 25% of APT Attackers*, SC MAGAZINE UK (July 2, 2014), http://www.scmagazineuk.com/ms-no-ip-takedown-hits-25-of-apt-attackers/article/359021.