Why Botnets Persist:

Designing Effective Technical and Policy Interventions

IPRI(2019)02
https://internetpolicy.mit.edu/publications-ipri-2019-02.

Author: Wajeeha Ahmad

Why have botnets remained a key feature of network attacks and exploitations? Why have years of interventions by security researchers, private actors and law enforcement agencies been unable to effectively tackle this seemingly persistent feature of networks? This article analyzes the multiple technical and socio-economic factors contributing to the barriers in mitigating botnet-based attacks and exploitations in an attempt to determine weaknesses in the botnet attack model and areas for effective interventions. The lesson to be drawn is that a mix of varied technical and policy interventions along with greater collaboration between key stakeholders are needed in the fight against botnets.

Internet Policy Research Initiative
Massachusetts Institute of Technology

https://internetpolicy.mit.edu

1. Introduction

Botnets, networks of malware-infected machines controlled by an adversary, are the root cause of a large number of security problems on the Internet. The term botnet, an amalgamation of the words "ro*bot*" and "*net*work", refers to collections of bots – compromised or "zombie" computers – that are remotely controlled by a human operator. A bot is a malicious piece of software that runs on a compromised computer system, without its owner's knowledge, and in cooperation with other bots, accomplishes certain tasks. Often referred to as the 'plague of the internet',[i] botnets have been used for illegal activities on a scale large enough to jeopardize the operation of private and public services in several countries around the world. As early as 2007, experts believed that approximately 16–25% of the computers connected to the internet are part of botnets.[ii][1] Today, botnets continue to generate as much as 30% of all internet traffic.[2] Moreover, the FBI estimated in 2014 that 500 million computers are annually infected by botnets, incurring global losses of approximately $110 billion.[3]

Broadly, the lifecycle of a botnet consists of three stages: infection, communication between the infected bots, and finally, application or execution. While botnets infect vulnerable machines using similar methods as other classes of malware such as remotely exploiting software vulnerabilities or social engineering, etc., their defining characteristic is using a command and control (C&C) infrastructure for communication between the attackers' - also called botmasters or bot-herders – and their bot armies. The botmaster must ensure that their C&C infrastructure is sufficiently robust to manage numerous distributed bots across the globe apart from being able to resist any attempts to shut down the botnet. The execution stage consists of attackers controlling the bots using a C&C channel to accomplish various tasks, such as information or identity theft, extortion, click fraud, email spam, distributed denial of service (DDoS) attacks, manipulating online games

[i] A phrase used in many of the Microsoft civil suit court documents.
[ii] In 2006, researchers showed that botnets represent a major contributor to unwanted Internet traffic with 27% of all malicious connection attempts observed from the distributed darknet being directly attributed to botnet-related activity. See: Abu Rajab et al., "A Multifaceted Approach to Understanding the Botnet Phenomenon."

or surveys, and distributing malicious software such as Trojan horses, spyware, and key loggers to name a few.[4]

After more than a decade since Vint Cerf's dire warning of a botnet "pandemic", this threat has only intensified.[5] Despite a handful of successful operations that have taken down botnets over the years, there is no sign of the "zombie apocalypse" waning.[6] As a result of improvements in the speed and volume of data transmission, both botnet infection rates and the monetary damaging power of botnets are continuously increasing with staggering numbers of devices joining botnet armies. Botnets have now started conscripting mobile phones and smart devices, such as refrigerators and surveillance cameras to spam and mine cryptocurrencies.[7] While the types of threats posed by botnets are not new, they have magnified significantly and are expected to grow as innumerable insecure Internet of Things (IoT) devices enter the market. Thus, given the apparent avenue for continued growth in the market as well as the massive costs to both individuals and society as a whole, there is dire need to both prevent the spread of botnets and mitigate their harmful effects.

This paper is structured as follows. The first part examines the incentives that cause botnets to exist and tracks the history of botnet evolution (Sections 2 and 3). The second part presents an overview of botnet mitigation approaches adopted by various stakeholders such as security researchers, private corporations and law enforcement agencies, and highlights the key features, successes and failures of their efforts (Sections 4 and 5). Finally, the article analyzes the full botnet attack model to explain why botnets have remained a persistent part of networks, and identifies weaknesses in the attack model to direct the future implementation of technical and policy interventions to effectively tackle the threats posed by botnets (Section 6).

2. Why botnets exist

Operating botnets has two distinct advantages. First, the botmaster is hard to trace because the actual attacks are launched by bots that are distributed both on the network and geographically. This separation of attacker from attacking devices makes it especially hard to determine the botmaster's location or shut down their command-and-control server. Second, the distributed network of bots allows the botmaster to instigate large-scale automated attacks. Botnets made up of thousands of computers allow attackers to send a vast number of emails, collect massive amounts of information, or disrupt access to a website quickly and efficiently. Thus, the same characteristics that made the Internet economy grow successfully – such as the ability for every node to run arbitrary code – are being abused by botmasters, to commit illegal activities on a vast scale. Many of these attacks and exploitations have specific targets motivated by various financial or political goals.

2.1 Financial harms and incentives

Distributed bot networks are used to execute numerous financial crimes, such as online payment account and bank account cracking, spamming, distributed denial of service

attacks, etc.[iii] These may be financially-motivated criminal attacks targeting individual computer users by recording their Internet banking details and other financial services. Other attacks may be commercially motivated, involving companies targeting their competitors' infrastructure to prevent regular users from accessing certain services and harming the victim company's reputation in their customers' eyes.

Today, botnets represent a blossoming economic market where botmasters offer a menu of services for either purchase or rental. "Rent a botnet" and "DDoS for hire" services are commonplace, allowing malicious actors to rent a whole network of infected computers and use it to perform their attacks.[8] The marketplace is replete with advertisements offering botnets at various hourly or daily rates depending on the number of infected users, their geographical location, and the botnets' ability to evade detection.[iv] Typically, customers rent a botnet from an intermediary, a non-technical entrepreneur who is usually independent of the developer. While botmasters may use the botnet directly to make money through various scams, their primary job is marketing i.e. renting their services via chat and email.

Botnets are particularly attractive and lucrative tools for criminals because they are effective, easy to propagate, and cheap.[v] They have a relatively low cost of entry, the marginal cost to maintain them is low, and the potential profits grow exponentially as more computers are infected. Although they take many forms and use a wide range of tools, a common theme among such botnets is the desire to generate a profit for the botnet operators. As an example of some of the economic incentives of a few of the most malicious botnets, Zeus, a family of financial botnets responsible for identity theft, caused more than $100 million in financial losses since its discovery in 2007 through the targeting of financial websites.[9]

However, criminal incentives are only one side of the problem. Another crucial aspect relates to the incentives of the owners of the infected machines. Botnets typically attack third parties, not the owners whose machines are used for an attack. This reduces the odds that owners will discover the infection and, more importantly, undermines their incentive to better secure their machines since the damage is borne by others or society at large. At the same time, the benefits of investment in security partially accrue to other users. Bauer et al. found that the incentives under which end users and ISPs operate explain the emergence of botnets generating information security problems for society at large.[vi] This

[iii] According to a former researcher at Arbor Networks, which tracks and defends against botnets, "bots are at the center of the undernet economy. Almost every major crime problem on the Net can be traced to them." (Berinato, "Attack of the Bots."). It is estimated that over 80% of spam messages originate from botnet activity. (Silva et al., "Botnets: A survey").

[iv] Broersma, "Botnet Price for Hourly Hire on Par with Cost of Two Pints."; IoT botnets are even cheaper, ranging from anywhere between $0.25 to $1 per host with minimum orders of around 50-100. See: "The Cost of Renting an IoT Botnet."

[v] For example, Symantec reported an advertisement on an underground forum in 2010 promoting a botnet of 10,000 bots for US $15. See: Fossi et al., "Symantec Internet Security Threat Report – Trends for 2010."

[vi] The authors posit that the proximate source of the problem is end users since "in sum, end users in the aggregate spend too little on security; their decisions therefore enable the growth of botnets, which

divergence between private and social costs represents a classic form of an economic externality or market failure, where the direct effect of the activity of one actor on the welfare of another is not compensated by a market transaction.

2.2 Political harms and incentives

The same attributes that make botnets well suited for financial crimes readily translate to politically motivated applications. For instance, a botnet capable of DDoS attacks can be exploited as a mechanism of unfair competition or cyberterrorism.[10] In some cases, CrowdStrike has observed state actors piggybacking on traditional criminal botnet infrastructure, searching compromised hosts for information or access of potential interest, sometimes only in highly localized areas.[11] The political goals of botnet-based attacks may include conflict instigation, revenue generation, service disruption, intelligence exfiltration and chaos instigation.[12] In 2007, distributed denial-of-service attacks launched by botnets targeted IT assets belonging to Estonian banks, newspapers and parliament. Although the attacks were not directly attributed to a nation state, they illustrate the impact that botnets can have on a nation's security. In addition to country-sponsored attacks to disable critical services or collect intelligence, botnets may be exploited by "hacktivist" groups or terrorist organizations.[13] In such cases, average Internet users could partake in a collaborated botnet attack without requiring any skill or expertise by donating their regular computer equipment to the attack. For example, the Anonymous "hacktivist" group attacks have displayed the power of distributed computational contribution to botnet-powered attacks.[14]

In such cases, botnet activity succeeds in part because the actual source of the attack, the botmaster or client who has rented the botnet from the botmaster, is hidden.[vii] Tracing back through the attacking machines to find the actual source of an attack may involve several stages through multiple machines in different jurisdictions, which adds complexity and delay. To avoid attribution, botmasters may deliberately use intermediate services that do not demand or log identity, thereby ensuring that they are several hops removed from the machines performing the attacks. The attack may also involve falsified source addresses, making traceback very difficult or even impossible. The fact that attribution remains a significant challenge further complicates deterrence and retaliatory measures. For instance, in the July 2009 botnet attacks on South Korean and US websites, the South Korean intelligence services stated through the press that they suspected North Korean hackers were behind the attacks.[15] A few days later, this was used as a call for retaliation on North Korea by a US lawmaker,[16] which shows that such politically motivated attacks may spiral into significant diplomatic incidents.

In summary, botnets exist because they enable cybercrime, which is profitable for botmasters and their clients. The old adage that success begets success seems to apply

---

impose costs on virtually every other actor in the network." See: Eeten and Bauer, "Emerging Threats to Internet Security."

[vii] Former U.S. Deputy Secretary of Defense, William Lynn, summarizes this problem as: "Whereas a missile comes with a return address, a computer virus generally does not." See: William J. Lynn, "Defending a New Domain."

to botnet-based attacks and exploitations. This is exacerbated by the fact that the owners of the infected machines used for botnet-based attacks and exploitations may lack both sufficient awareness and incentives to take defensive actions. Additionally, since botnet-based attacks and exploitations have multiple stages, where an attacker infiltrates a computer to use as a platform to attack a second computer, and so on, they pose significant challenges for attribution and hence, deterrence. Thus, botnets are also an especially attractive tool since they allow politically motivated actors to achieve their ends without the perception of direct involvement.

3. Tracing the history of botnet evolution: Increasing stealth and resilience

The development of botnets can be better understood when placed in the broader context of the Internet. Since its inception, the Internet was meant to allow decentralized private communities to self-organize, invent and create with a limited, if any, role for government interventions in the form of regulation or liability. The increase in online transactions and the decrease in the cost of abusing vulnerabilities motivated profit-driven criminals to enter the scene and rapidly expand their activities.[17] Criminals discovered various business models to monetize the infected machines, spurring an increase in specialization for roles such as malware authors and botmasters, the emergence of markets for attack tools and services, and a new complex system of monetizing online crime. This section outlines the main technological developments exploited by botnets, organized by means of conducting C&C communications. Figure 1 shows the main stages in the technical evolution of botnets over time.

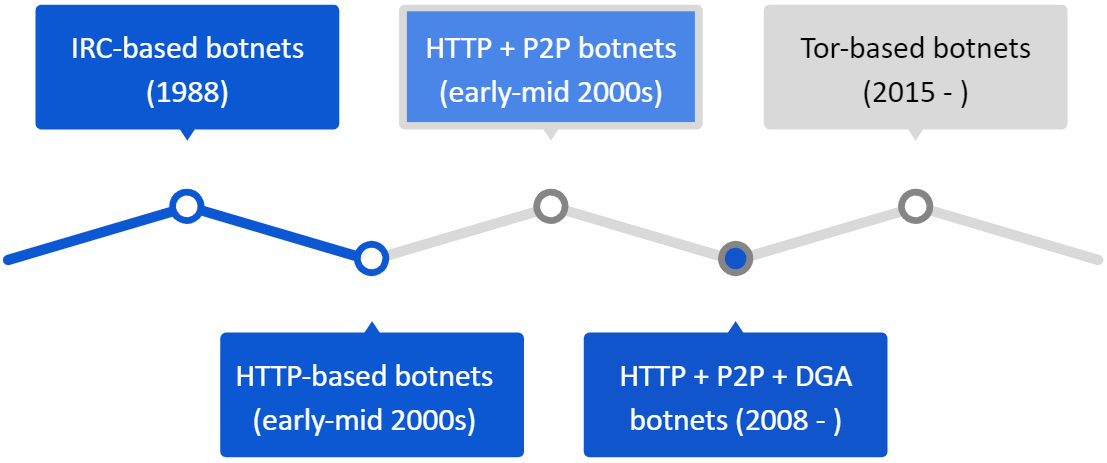

Figure 1: The technical evolution of botnet command-and-control (C&C) architecture.

3.1 IRC-based botnets

Historically, botnets originated from Internet Relay Chat (IRC), a text-based chat-system that organized communication in channels.[18] The concept of bots did not necessarily include harmful behavior, and the original idea behind botnets was to control interactions in IRC chat rooms. Each 'infected' computer connected to the IRC server (master) indicated

in the body of the bot program, and waited for commands from its master on a certain channel. They were able to interpret simple commands, provide administration support, offer simple games and other services to chat users, and retrieve information about operating systems, logins, email addresses, aliases, etc. The first botnet was invented in August of 1988 by Jarkko Oikarinen of the University of Oulu, Finland.[19] In 1989, Greg Lindahl, an Internet Relay Chat (IRC) server operator, created the benevolent bot called GM, which would play a game of Hunt the Wumpus with IRC users.[20] One notable example of a non-malicious botnet is Eggdrop created by Jeff Fisher for assisting IRC channel management in 1993 and developed further thereafter.[21]

Next, malicious IRC bots appeared that were developed by adopting the same basic idea, but were created for the primary purpose of attacking other IRC users or servers. The first malicious bot was GT-Bot, which developed in April 1998 and had at least a hundred variants.[22] Shortly thereafter, new bots evolved that used complex mechanisms for communication with the botmaster, exploited other available protocols and integrated new, powerful methods of attack, all of which made botnets more sophisticated and robust. They could propagate like worms, remain hidden as viruses and could launch large, coordinated attacks. Some examples of these bots include AgoBot and SDBot. The development of AgoBot and its variants is considered as the point from which botnets became a major threat to the Internet.[23]

These first generation of IRC-based botnets, including Agobot, SDBot, and SpyBot (observed in 2002-03), were relatively easy to take down because they used centralized channels for communication.[24] The botmaster hardcoded the IRC server and channel details into the bot executable prior to deployment so that once infected, the bots could log on to the specified chatrooms for instructions. This method has numerous advantages: the IRC protocol is widely used across the Internet, there are several public servers that botnets can use, and communication is in real-time. However, the network signature of IRC traffic is easily distinguishable and security devices can be configured to block IRC traffic.[25] More critically, this C&C architecture is centralized, allowing researchers to reverse-engineer bots, eavesdrop in C&C chatrooms, identify the bots and track the botmaster. Researchers also regularly coordinate with law enforcement to take down C&C chatrooms, crippling the entire botnet in a single step. According to some insider accounts, two thirds of IRC botnets are shut down within 24 hours.[26]

3.2 HTTP-based botnets

Botnets subsequently moved to HTTP-based C&C infrastructures, using webservers to issue instructions and receive uploads from infected machines. This involves bots connecting to predefined web servers (masters), receiving commands from it and transferring data to it in response using the HTTP protocol. Examples of this second generation of botnets that upgraded to HTTP-based C&C communications include Rustock, Zeus and Asprox (observed in 2006-2008). Since HTTP is ubiquitous on most networks, bot communications blend in with legitimate user traffic. However, web domains

can be blocked at the Domain Name System (DNS) level and C&C webservers, which serve as the single point of failure, can be located and seized.

More recently, botnets have experimented with esoteric C&C mechanisms, including social media and cloud services. The Flashback Trojan retrieved instructions from a Twitter account.[27] Whitewell Trojan used Facebook as a rendezvous point to redirect bots to the C&C server.[28] Makadocs Trojan and Vernot used Google Docs and Evernote respectively as proxies to the botmaster.[29] The results have been mixed. Network administrators rarely block these services because they are ubiquitously used, and C&C traffic is therefore harder to distinguish. On the other hand, C&C channels are again centralized and companies like Twitter and Google are quick to crack down on them.

With time, botnets have used more robust techniques to perform attacks on larger scales. However, the fatal weak point for botnets is the C&C infrastructure, the central nervous system of the botnet. Downstream communication comprises instructions and software updates sent by the botmaster, whereas upstream communication from bots includes information such as financial data, login credentials, etc. Security researchers usually reverse engineer a bot, infiltrate the C&C network, trace the botmaster and disrupt the botnet. The overwhelming majority of successful takedown operations to date have relied heavily on exploiting or subverting botnet C&C infrastructures.[30] However, these infrastructures are centralized with a single point of failure for the botmasters. Domain registrars, hosting companies and social networks can kill the accounts used to control the botnets by controlling the C&C infrastructure. Some innovations that have made HTTP-based botnets more resilient over time are summarized below.

3.2.1 Decentralized peer-to-peer architecture

Decentralized peer-to-peer (P2P) botnets aim at removing or hiding the central C&C server, which was the main vulnerability or central point of failure of the centralized model. Under the P2P architecture, bots maintain individual routing tables, and every bot actively participates in routing data in the network, making it very difficult to identify C&C servers. Some P2P botnets that operate in a completely decentralized manner allow a botnet operator to inject a command into any of the bots, and have it be broadcasted to specified node(s). Since P2P botnets usually allow commands to be injected at any node in the network, the authentication of commands becomes essential to prevent other nodes from injecting incorrect commands. The first known botnet that utilized the P2P model was Slapper worm that appeared in 2003.[31] Other famous P2P botnets include the Conficker, Nugache and Storm botnets that emerged in 2005-2007.[32]

The use of P2P structures means that botnet takedowns are considerably harder, and require interfering with communications between many infected machines. This may involve detecting P2P traffic signatures, successfully crawling P2P networks to enumerate the botnet, and poisoning bot routing tables to disrupt the botnet. As an example, Symantec researchers took down the ZeroAccess botnet in a concerted effort by flooding

routing advertisements that overwhelmed bot routing tables with invalid or sinkhole entries, isolating bots from each other and crippling the botnet.[33]

3.2.2 Domain-generation algorithms

The Domain Name System or DNS, which maps domain names to IP addresses, serves as the address book of the Internet. Most modern botnets make frequent use of domain names to support their C&C communications.[34] Additionally, bots are no longer hard-coded with a web address prior to deployment, but with a Domain Generation Algorithm (DGA) that takes factors such as date and time as seed values to generate custom domain names at a very rapid rate.[viii] Generating numerous domain names and registering only the relevant one(s) "just in time" before an attack allows a botnet to shift their C&C domains on the fly and remain inconspicuous for longer.[ix] This is because the reputation of a domain over time can be used to identify malicious behavior.[35] While it is very costly and time-consuming for defenders to reverse-engineer a DGA and seize the large number of algorithmically generated domains to eliminate C&C activity, the botmaster has to register only one to communicate with other bots in a given time-window.[x] This economic asymmetry makes the problem of finding a domain used for C&C communications equivalent to trying to find a needle in a haystack. Thus, the use of DGAs to general massive numbers of domains is used to both hide real botnet C&C servers and overwhelm traditional blacklisting solutions.

3.2.3 Fast-flux Service Networks

Another technology for implementing the DNS protocol within C&C communications is a Fast-flux Service Network. A fast-flux botnet rapidly changes the mapping of IP addresses to its domain names, which allows a botmaster to link several hundreds of destination IP addresses with a single domain name in a DNS record. Mapping a domain name to a number of IP addresses rather than a single IP address increases the productivity and extends the lifetime of domain names linked to the bots. Moreover, to obscure the link between a domain name and the IP addresses of available bots, fast-flux botnets also often employ a strategy that resolves a domain name to different sets of IP addresses over time. These IP addresses are swapped with very high frequency (as often as every 3 minutes), so that different parties connecting to the same domain within minutes of each other are redirected to different locations.[36] Yet another layer of confusion can be added by similarly concealing the Authoritative Name Servers for the domain within this constantly changing fast flux cloud. In 2007, Storm botnet creators used such service networks for the first time, and today cyber-criminals engaged in illegal activities commonly use fast flux techniques.[37]

[viii] As an example, Conficker-C generated up to 50,000 domain names daily, distributed over 116 Top Level Domains (TLDs), which proved nearly impossible to block. See: M. Bowden, "Worm: the First Digital World War."

[ix] Plohmann et. al also show that attackers seem to register domains very shortly before their validity or use. See: Plohmann et al., "A Comprehensive Measurement Study of Domain Generating Malware."

[x] The domains wait for commands from C&C servers and help relay instructions on how bots can continue communicating with each other and infect new devices.

3.3 Botnets exploiting anonymous networks

Botnets have increasingly exploited privacy infrastructures and anonymous services.

3.3.1 Tor-based botnets

Some examples of botnets that have used the Tor anonymity network to host and hide their C&C servers include the Skynet botnet, Sefnit botnet and variants of the Zeus botnet.[38] Although these early botnets exploiting the Tor network posed a challenge in locating the real IP addresses of the C&C servers, analyzing their C&C traffic was still possible since the infected bots were hosted outside the Tor network. However, researchers have come up with a proof-of-concept construction of a botnet hosted entirely within the Tor network i.e. all C&C communication is carried out exclusively via Tor hidden services.[39] This would allow such botnets to evade current techniques for detection, measurement, scale estimation, observation, and mitigation since the Tor traffic is encrypted, non IP-based, and no conventional DNS queries exist to resolve the .onion addresses.

3.3.2 Blockchain-based botnets

Researchers have also proposed botnet constructions based on blockchain technology, including one that uses bitcoin transactions to embed C&C information.[40] Bitcoin, in particular, has been touted as an "ideal C&C dissemination mechanism for botnets".[41] This is because it eliminates the need for a botnet operator to create their own C&C mechanism, and provides built-in anonymity and security that makes both the detection and disruption of C&C communication exceptionally difficult without significantly affecting legitimate Bitcoin users.[42]

There have also been cases of botnets exploiting bulletproof domain providers for additional anonymity and resilience.[43] Given that the next wave of botnets may further subvert privacy infrastructures, there is a need to develop novel detection and mitigation techniques to prevent botnet attacks and exploitations.

In short, since 1988, botnets have evolved from being harmless initial assistant tools to one of the predominant threats facing the Internet. The aforementioned overview of developments in botnet infrastructures shows that they have adopted the fundamental traits of networks and have incorporated more resilient and stealthy features over time. It can be argued that the generality of the Internet favors the attacker over the defender. The Internet was meant to allow multiple different patterns of communication – a feature that affords attackers ample flexibility for exploitation: the attacker must build a C&C system to communicate with bots, but can accomplish this in several ways using diverse C&C protocols and structures, whereas defenders must secure all channels to thwart attacks. The next part of this article focuses on the steps taken by the technical community, private actors and law enforcement to combat malicious botnet activity.

4. Technical mitigation methods: legal and ethical challenges

Since as early as 2005, the security community has been working to understand, mitigate, and disrupt botnets.[44] Various studies have analyzed the structure, behavior, and evolution of particular botnets.[xi] Bailey et al. note that each technique for understanding botnets has a unique set of tradeoffs, and only by combining perspectives can we fully analyze the entire picture.[45] However, despite being well studied, botnet mitigation remains a difficult problem since botnets often evolve to avoid disruption. A defense to one attack often spurs botmasters to find new styles of attack to defeat that defense. Consequently, protecting against botnets at scale has been described as "a game of chess against an opponent that is constantly changing the rules."[46] While innovative features have constantly increased the resiliency of botnets, there remain weaknesses that can be exploited by defenders. This section reviews the main technical mitigation methods used against botnets in increasing levels of aggressiveness using the categories of action introduced by Dittrich (2012).[47]

4.1 Passive Monitoring

This involves analyzing network traffic patterns to detect botnet activity. For example, Zand et al. proposed a detection method based on identifying command and control signatures, and Gu et al. focused on analyzing network traffic to aid in detection and mitigation.[48] However, using this method, it may be impossible to find all compromised hosts by monitoring C&C traffic alone since only a subset of infected hosts may be actively communicating simultaneously.[xii] In many cases, knowing the full size of the botnet from passive observation alone is practically impossible.[xiii] Moreover, obfuscated host identities can prevent their direct and unique identification. Other factors significantly reducing the utility of passive observation include the use of heavy encryption to conceal the content of communications, and possibly a peer-to-peer (P2P) infrastructure for C&C communications.[49] Thus, while still used today, this means of identifying botnet activity is becoming less and less viable over time.

In many countries, the routine technical action of inspecting internet traffic is surrounded by a number of legal concerns, most notably those of personal data protection,

[xi] Some examples: Barford and Yegneswaran, "An Inside Look at Botnets."; Holz et al., "Measurements and Mitigation of Peer-to-Peer-Based Botnets."; Porras, Saïdi, and Yegneswaran, "A Foray into Conficker's Logic and Rendezvous Points."; Sinha et al., "Insights from the Analysis of the Mariposa Botnet."

[xii] For instance, it took a week of observation to see a few hundred nodes of the Nugache P2P botnet since its random topology limited the number of connections to remote peers to no more than a dozen or so per day. See: "Global Network Service Providers: Securing a Position to Challenge the Botnet."

[xiii] However, commands can typically propagate across a botnet at a much faster pace. For instance, research simulations have shown that mobile WiFi botnets can support rapid command propagation, with commands typically reaching over 75% of the botnet only 2 hours after injection, within as little as 30 minutes at times. Moreover, those bots able to receive commands usually have ≈40-50% probability of being able to do so within a minute of the command being issued. See: Knysz et al., "Open WiFi Networks."

unauthorised surveillance and confidentiality of communications.[xiv] Thus, based on legal requirements in some countries, passive monitoring may require proper permission to conduct surveillance activities and may only be allowed as part of official criminal proceedings.

4.2 Infiltration and Manipulation

Infiltration of the botnet by a defender involves executing malware in a sandbox environment, such as a virtual machine, and analyzing the results. However, sandboxes do not fully mimic human behavior since running malware in an automated fashion involves no human interaction: information on keystrokes, passwords or webpage visits is not obtained. Manipulation, on the other hand, involves actively controlling the botnet and causing bots to do things, which is similar to how BBC reporters interacted with the botnet they leased in 2009.[50]

4.3 Takeover

This involves a third party taking control of a botnet after its full command set and capabilities along with valid credentials for gaining administrative access to its C&C mechanism are known with a sufficiently high degree of certainty. If carefully executed, this can successfully expose the attackers without their knowledge. However, takeovers require a significant investment in reverse engineering and data analysis from real intrusion events. This carries the risk of being detected and counter-attacked. For instance, in January 2009, about three years after the first discovery of the Torpig botnet, researchers at University of California Santa Barbara used information from reverse engineering the C&C server selection protocol to identify as-yet unregistered domains that the bots would use for depositing their keylog files. They registered these domains before the attackers could, set up their own servers in a provider known to be unresponsive to complaints, and temporarily took control of the botnet for approximately 10 days.[51] The attackers noticed the takeover, updated their botnet to resist this weakness, and took back control.

Researchers have proposed the use of Sybil attacks to takeover P2P botnets.[xv] However, there remain open ethical and legal questions regarding the right to launch such attacks.[52] Moreover, apart from potential privacy issues relating to violating the rights to confidential

[xiv] As an example, monitoring traffic for botnet fighting purposes in Estonia might be regarded as illegal surveillance under the respective criminal law provisions of the Estonian Penal Code. In the German Penal Code, IP addresses are covered by telecommunications secrecy as well, and the surveillance of packet and traffic data can be punishable if it constitutes a violation of telecommunications secrecy (§ 206 of the German Penal Code, § 88 of the Telecommunications Code, § 7(2) of the Telemedia Code). See: Vihul et al., “Legal Implications of Countering Botnets.”

[xv] Sybil attacks involve infiltrating a botnet with large number of fake nodes or sybils in order to disrupt C&C communication between bots. See: Davis et al., “Sybil Attacks as a Mitigation Strategy against the Storm Botnet.”

communications or personal data protection, taking over the botnet using its infrastructure could also have implications under criminal law in various jurisdictions.[53]

4.4 Takedown

Taking down a botnet involves identifying weaknesses in the C&C structure and fall-back mechanisms in order to completely disrupt any new infections, any connections with the C&C infrastructure, and any means of the attacker countering these actions. A takedown of C&C servers can be achieved by disconnecting the identified C&C servers by deleting their domain names, making the C&C servers unavailable by sinkholing the traffic directed to it, physically seizing the C&C servers, or disconnecting the C&C servers by the ISP or the cloud service provider hosting it. The legal aspects of taking down C&C servers depend on the authorities ordering and implementing the takedown and on the location of the C&C servers.[xvi]

The decision to takedown a botnet is not always straightforward since botmasters are adept at transitioning their infrastructure to other hosts when their operations are partially, rather than completely, disrupted. Thus, partial takedowns may actually prolong botnets' ability to continue operating core infrastructure since when a takedown is not successful, the botnet operators "take a break and revise their code to be smarter, faster, and stealthier."[54] This was apparent when the Federal Trade Commission (FTC) obtained a court order to shut down the spamming Ozdok botnet in 2008, which caused the botnet to simply move and return in 2009 to again become one of the top sources of spam.[55] In another case, when a Crowdstrike engineer sinkholed an earlier variant of the Kelihos botnet live onstage during a security conference in 2012, it re-emerged to be even more sophisticated and resilient later on.[56] Interestingly, operators of the Mariposa botnet were able to evade a full takedown by bribing a registrar to return domain control to the malicious operators, thereby emphasizing that barriers to successful takedowns are not only technical ones.[57]

Moreover, there is the risk of collateral damage stemming from larger efforts to cut off networked criminal activity. Therefore, despite noble intentions, taking down sophisticated and decentralized criminal networks such as P2P botnets has proven difficult in practice. As a consequence, the decision to engage in a takedown rests on striking a balance between risk and reward. Nadji et al. quantified these tradeoffs by balancing the cost of collateral damage, visibility into criminal activity, and long-term economic benefit.[58]

4.5 Eradication

Eradication involves using captured C&C capabilities or remotely exploitable vulnerabilities found in the botnet infrastructure or its host operating system to control

[xvi] For example, if a C&C server were located in Estonia, the Estonian Computer Emergency Response Team (CERT-EE) would normally contact the relevant ISP and ask it to disconnect the server. Should the server be based elsewhere, the relevant CERT would contact either the foreign ISP or the national CERT of the respective state. See: Vihul et al., "Legal Implications of Countering Botnets." p. 35.

infected nodes and clean up the malicious software on those nodes on command. Apart from demanding extensive technical capability, planning, and execution, this can be a risky endeavor with significant legal and ethical implications.[59] In cases where eradication efforts have involved modifying malicious code on users' computers and interfering with users' access to the Internet without explicit consent, there has been criticism of the methods used. For instance, the eradication efforts associated with the takedown of the Coreflood botnet, the first botnet takedown by U.S. law enforcement, were criticized as "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."[60] The Electronic Frontier Foundation (EFF), which celebrated the takedown of the botnet, also expressed concerns about a "dangerous" governmental intrusion into individual computers.[61]

In summary, the various technical methods to counter botnets tend to pose increasingly thorny legal and ethical dilemmas with increasing intrusiveness and invariably involve certain tradeoffs. As an example, Clark and Landau suggest that since ISPs are better poised to observe network traffic than users, regulation could permit or require that the serving ISP log the network traffic of machines infested with malware as opposed to more stringent alternatives such a total disconnection or quarantine, resulting in a system whereby poor system maintenance leads to a loss of user privacy.[62] While technical remedies for stopping botnet attacks and exploitations remain an ongoing area of research and practice, technical solutions alone are inadequate because botnets continue to regularly resurrect, often with new strategies or mechanisms for garnering profit or exfiltrating data. Clearly, the scourge of botnets cannot be understood as merely a technical issue. Rather, the underlying incentives - economic or otherwise - of all actors involved must also be addressed. The next section elaborates on the challenges involved in coordinating botnet takedowns in practice.

5. Coordinating botnet takedowns: a game of whack-a-mole?

Those involved in the fight against botnets include security researchers, law enforcement and corporations. This section evaluates the key characteristics and challenges associated with botnet takedown attempts in practice using two methods: voluntary takedowns by decentralized groups of security researchers and court-authorized takedowns by both law enforcement and corporations.

5.1 Takedowns by voluntary working groups

Given the decentralized and cross-boundary architecture of the Internet, it is not surprising that self-organization and voluntary action are at the heart of responding to botnet-related crime. Botnet fighters tend to consist of small groups of security researchers and engineers — self-proclaimed "internet janitors" — who work to keep networks running smoothly. Incidents evolve rapidly and so do the necessary actions of the players involved.[63]

In tackling some of the more prominent botnets, defenders have had to collaborate to have a chance of being effective. This was evident in the establishment of the Mariposa Working

Group, which was formed in May 2009 as an informal group with the goal of exterminating the Mariposa botnet.[xvii] At one point, one of the leaders of the criminal group made the mistake of attempting to connect to a C&C server without using the anonymous VPN, exposing his personal IP address and identifying him. This information was handed over to Spanish law enforcement, who subsequently arrested the suspect.[64] Another example of a collaborative effort between various private actors is that of the Conficker Working Group, which coordinated the preemptive shutdown of the Conficker botnet by registries of domain names used to control the large botnet. The fundamental problem in dealing with distributed attacks is that of coordinating a response involving data collection, analysis, and countermeasures, across a heterogeneous population that is not formally organized as a single team, nor under any obligation or requirement to behave as one. The Conficker Working Group presents an interesting case study to understand the dynamic of collaborative botnet takedown efforts.

5.1.1 Resource constraints

One of the first collaborative large-scale efforts was aimed at thwarting Conficker, which was poised to become a huge international botnet.[65] Those involved included security firms, antivirus vendors, university researchers, and various private entities who shared information with each other based on personal trust to develop mitigation methods and inform the public about patches.[66] After a DNS security symposium in February 2009, a coordinated effort began by means of the informal Conficker Working Group (CWG).[67] The involvement of representatives from the Internet Corporation for Assigned Names and Numbers (ICANN), which is responsible for coordinating the DNS among other critical Internet infrastructure, became fundamental to the botnet takedown given the fraudulent use of domain names to direct bots to a control server.[68]

After decrypting the algorithm used for the botnet's dynamic communications, members of the Working Group sought to buy the domains from Internet registrars before they were utilized by Conficker in order to block its commands and updates to individual computers.[69] However, this proved to be difficult since the domains used different country codes, which complicated the mitigation efforts.[70] Additionally, the large volume of domains was too costly to purchase in bulk, even for a resource rich entity such as Microsoft, which was involved in the effort. This problem of global reach was ultimately resolved by ICANN, which agreed to both waive domain name registration fees as far as possible for the Working Group and give prior notice to over 100 top-level country domain registrars that certain domain names would be automatically registered by Conficker.[71] However, obtaining similar exceptions may prove difficult in the future as noted in an ICANN document that states, "The community cannot rely on all contractual matters [such as waiving fees] to be so easily handled for all future incidents."[72] Moreover, due to the long-

[xvii] The group consisted of Defence Intelligence, the Georgia Tech Information Security Center and Panda Security, along with additional unnamed security researchers and law enforcement agencies. See: Panda Security Mediacenter, "Mariposa Botnet."

term nature of the volunteer effort, several members of the group cited burnout as a key reason for why the effort could not maintain momentum indefinitely.[73]

5.1.2 Problems of coordination

While personal motivations and commercial competition may play a role in how well groups function, the Conficker Working Group shows that differences can be overcome to cooperate against a threat. An ICANN document recognizes the ground-breaking nature of the group composition, stating that, “The operational response to Conficker is perhaps as landmark an event as the worm itself.”[74] However, given the ad-hoc nature of collaboration among a group of volunteers, there were certain difficulties in tasking and accountability of group members as well as glitches in management, communications and transparency within the group. The single most common recommendation emerging from this effort was about maintaining a collaborative infrastructure to help the private sector counter emerging threats in cyberspace.[75] While no member recommended a standing organization to manage all threats citing that "every threat is different" and "competition is good”, the formation of small working groups within a large architecture of collaboration was the preferred model.[76]

Several members also pointed to uncoordinated communication between the Working Group and ISPs as a weakness, and argued for more systematic coordination with ISPs to aid with clean-up efforts. There have also been earlier suggestions in literature for researchers and law enforcement to cultivate working relationships with registrars and ISPs to enable rapid response time to botnet threats.[77] Moreover, the group’s ability to remediate infected computers had limited success due to insufficient financial incentives for remediation efforts.

The CWG also shows that there is a need to clarify the role of private sector cooperation with law enforcement, which remains a vital part of cybersecurity efforts led by governments. While several CWG researchers communicated with various intelligence and law enforcement agencies through their own social networks, these agencies were unable or unwilling to make formal contributions to the group.[78] The inability to attribute Conficker to an individual or group remained a key failure of the effort to combat and eliminate Conficker, but several members of the CWG stated that the responsibility for identifying and capturing criminals should fall to law enforcement agencies.[79] While the CWG expressed a willingness to assist law enforcement, some members raised concerns about the nature and limitations of such assistance, including concerns about becoming embroiled in potential future court cases over chain of evidence issues. Nonetheless, there was a consensus that law enforcement activity is essential to combating threats like Conficker, with some members stating that it might be the only effective method of eliminating such threats permanently.[80]

In summary, the Conficker Working Group illustrated that the availability of resources as well as public-private sector collaboration and information sharing are among the many urgent requirements of protecting against impending botnet threats. However, it is

generally easier and cheaper for botmasters to invest resources to maintain attack infrastructures than it is for a large number of uncoordinated and competitive entities to do expensive reverse engineering necessary for effective takedowns or countermeasures. As illustrated in this section, the application of significant resources by a single entity does not sustainably scale. Corporations and university research labs may have reputational risks limiting the aggressiveness of their actions whereas individuals with limited resources may act based on partial information or with inadequate planning, putting innocent third parties at risk. Moreover, fewer and fewer entities have had the necessary resources to definitively take down the most sophisticated botnets by themselves.

5.2 Court-authorized takedowns

While takedowns coordinating the civil and/or criminal legal process with technical methods (Waledac, Rustock, Coreflood, and Kelihos) have succeeded on the first try, those using only the civil legal process (the first attempt at taking down Ozdok) or only technical means (Torpig, Ozdok, and Pushdo) did not.[81] Some of the most sophisticated botnets could not have been fully taken down without using the legal process to remove all of the domains used for fall-back and secondary C&C. These efforts suggest that compelled action via court orders may be an important feature of successful botnet takedowns.

Court-authorized botnet takedowns typically involve seizures of domain names, many of which act as botnet C&C servers, based on violations of a number of U.S. statutes such as the Computer Fraud and Abuse Act and the Electronic Communication Privacy Act. This methodology of death by domain name seizures disrupts bots' ability to communicate with its peers and C&C servers, thereby allowing defenders to eliminate the threat without immediately having to seize malicious resources located in various countries. Lerner (2014) and Hiller (2015) provide a detailed background on the legal theory and procedure used in past court proceedings involving botnet takedowns.[82]

5.2.1 Takedowns motivated by national security concerns

While law enforcement agencies such as the Federal Bureau of Investigation (FBI) and the US Department of Justice (DoJ) are active in tracking the criminal activities of botnets, the number and sophistication of the attackers often overwhelm their capacity. Given the high costs of investigating and prosecuting globalized cybercrime perpetuated by botnets, approaches via criminal law have been used only sparingly against a number of high-profile targets. Rather than prosecuting the botmaster, law enforcement agencies have pursued seizing and disabling a botnet in some cases.[83]

Coreflood was the first law enforcement action to shut down an active botnet.[xviii][84] The breadth and depth of Coreflood infections and resulting botnet harms spurred an FBI investigation in 2011 that resulted in legal action by the DoJ, where Coreflood was

[xviii] The Coreflood botnet was active for at least ten years and infected approximately two million computers globally, causing estimated damages exceeding $20 million.

described as a threat to national security in the initiating complaint.[xix] The government initiated and won a civil suit in federal court, seeking a temporary restraining order (TRO) allowing it to replace servers, collect IP addresses, and deliver a disabling command.[xx] Instead of aiming to arrest and imprison the as yet unknown perpetrators of the botnet, this action was designed to stop the operation of the malicious software installed on unsuspecting user computers. Using the TRO, the government seized C&C servers and redirected botnet traffic to substitute servers, disabling botnet functions and enabling victims to remove the Coreflood software from their computers.[85] In dealing with subsequent botnet cases, the FBI and DOJ have often relied on corporate assistance in executing operations while the judicial actions and mitigation techniques have typically been implemented by the government.

5.2.2 Takedowns motivated by corporate interests

Before the Coreflood action, Microsoft announced the "first of its kind" takedown based on collaborative technical and legal action targeting the Waledac botnet in February 2010.[86] Apart from being able to send 1.5 billion unsolicited spam emails per day, the botnet software modified the Microsoft Windows operating system, suspended authentic security updates, and caused users to install fake, injurious "security" software.[87] Consequently, Microsoft received thousands of complaints from customers, who attributed their computers' malfunctioning to defects in Microsoft products.[88] In response, Microsoft pursued an offensive strategy as part of its Operation b49 to disrupt the 277 domain names that were used for communications among the tiers of the botnet.[89] This involved taking swift and secret action to take the botnet domain names off the Internet before the botnet controllers could change their location.[90]

This was the first time in history that a court had granted an ex parte TRO forcing a domain registrar to take 277 domains used as C&C entry points for the Waledac bots out of service.[91] 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, CAN-SPAM Act, Electronic Communications and Privacy Act, false designation of origin and trademark dilution under the Lanham Act, trespass to chattels, and unjust enrichment and conversion. Additionally, 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.[92] The technical sinkholing followed methods described in published analyses of Waledac.[93] In the next three years, Microsoft undertook seven additional takedowns both with and without law enforcement partnerships by building upon legal framework of

[xix] Alleging violations of 18 U.S.C. §§ 1343, 1344, and 2511, respectively. The specific charges against the unknown Coreflood botnet operators included wire fraud, bank fraud, and unauthorized access to electronic communications. See: Hiller, "Civil Cyberconflict."

[xx] Sending a temporary disabling "stop" command was authorized "only to computers reasonably determined to be in the United States." See: Hiller, "Civil Cyberconflict."

the Waledac takedown.[94] These civil lawsuits have created the legal precedent for suing botnet operators and dismantling botnets.

5.2.3 Challenges involved in court-authorized takedowns

This section describes the challenges associated with court-authorized botnet takedowns using particular cases as examples.

5.2.3.1 Establishing local jurisdiction

In 2011, Microsoft sued an individual and limited liability company located in the Czech Republic, and John Does, in order to disable the Kelihos botnet.[95] Despite both known defendants being outside of the U.S., jurisdiction was established in a Virginia court based on their business activities in Virginia, the malicious code directed at persons in Virginia, and botnet activity involving Virginia-based computers.[96] Thus, the litigation illustrated that the geographical location of a defendant outside the U.S. is not necessarily an impediment to legal action when the domain registry (in this case VeriSign), or registrar, is located in the U.S. and thus subject to the court's jurisdiction. As the takedown cases show, the location of ICANN in the U.S. as a California incorporated entity has been helpful since U.S. courts could exert jurisdiction and order ICANN to take measures to block and transfer domain names and IP addresses used for criminal purposes.

However, this also illustrates the jurisdictional limitations of U.S. courts. Court-authorized botnet takedowns depend on the location of major structural entities of the Internet infrastructure such as ICANN and VeriSign in the United States. The significant extent of cooperation by foreign courts and law enforcement with Microsoft and U.S. court requests showed that while not impossible, it is difficult and time consuming for law enforcement to follow criminals across international boundaries. Criminals who prey on consumers in foreign countries are particularly unlikely to be arrested, or followed, across international jurisdictional boundaries.[97] The resources and expertise are simply not available to the local entities who otherwise would be the ones most appropriately protecting the public.[98]

5.2.3.2 Requesting the cooperation of foreign domain registries and registrars

Disabling the Coreflood botnet, the first law enforcement takedown attempt, involved cross-border action. This is because the seizure of domestic C&C computers alone would not have disabled the botnet for any length of time given that many botnet servers were located around the world, outside the jurisdictional reach of U.S. courts. While the FBI targeted U.S.-based servers, the court ordered the domain name providers to "impose a registry lock on the Internet domain name[s]" including any account associated with it.[99] This strategy effectively avoided ICANN's participation using a court order issued to the domain providers. Domain providers were mainly located in the U.S. with some in Singapore, the U.K., and Australia, whose voluntary cooperation assisted the takedown.[100]

Many of Microsoft injunctions and orders have also included deferential requests for foreign cooperation to stop the spread of harmful botnets. As part of the legal action

against the Zeus botnet, ICANN was directed to forward the court order obtained by Microsoft to specified foreign registries. In requesting international cooperation, the Preliminary Injunction stated: "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."[101] Similarly, the takedown of the Nitol botnet, which utilized an Internet domain (3322.org) from China for its C&C communications, was assisted by cooperation from Chinese authorities and Chinese CERT. Third parties including registries, registrars and subdomain hosting entities also assisted Microsoft in blocking over 7,000 domains from being registered for use in the Bamital botnet.[xxi] However, if botnet operators had used foreign domain name registrars in jurisdictions that are not cooperative to US law enforcement, court takedown orders would likely be delayed or ignored.[102]

5.2.3.3 The existence of safe havens in law enforcement

In more recent botnet cases, Microsoft has adopted increasingly coordinated efforts with law enforcement to pursue botnet operators in addition to taking down botnets. As the company launched Operation b54 to tackle the Citadel family of botnets in 2013, the FBI coordinated with Europol and law enforcement counterparts in more than eighty nations to encourage voluntary worldwide action against the botnet.[103] While the coordinated effort did not lead to the arrest of Aquabox, the alleged Citadel master, it did result in the disruption of almost 90% of the Citadel botnet.[104] 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."[105] The FBI also recognized the heightened importance of public private partnerships and international coordination.[106]

In the case of the ZeroAccess botnet, the botnet's international reach necessitated a coordinated effort with the FBI, Europol's European Cybercrime Centre, and industry partners.[xxii] When the botnet owners attempted to use substitute IP addresses to 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."[107] The changing approaches to the botnet takedowns from a solely privately led civil suit, to the Citadel and ZeroAccess

[xxi] Some third parties such as VeriSign were located in the United States, while others 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 the Netherlands. See: Complaint at 6–7, Microsoft Corp. v. John Does 1–18, No. 1:13-CV-139 (Jan. 31, 2013).

[xxii] The ZeroAccess botnet engaged in click fraud, identity theft, and DoS attacks using eighteen servers located in Latvia, Luxembourg, Switzerland, the Netherlands, and Germany. 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)

collaborations with law enforcement around the world, provide evidence that the fight against botnets and botmasters has evolved towards an increasingly networked framework that depends on cooperation from a range of global partners.

However, in cases where botnet infrastructure or operators are located in unfriendly jurisdictions or traditionally uncooperative regimes, coordinating a takedown or bringing the botmaster to justice becomes exponentially more challenging, if not impossible. For instance, although the individual in charge of the Kelihos botnet, a man named Peter Yuryevich Levashovman who was known as "one of the world's most notorious criminal spammers",[108] was indicted in 2009 for his operation of the Storm botnet, he remained outside the reach of US law enforcement for more than a decade. A resident of St. Petersburg, Russia, Levashov was arrested by authorities in Spain, a strong U.S. ally on cybercrime, while he was on vacation with his family.[109]

Some nations are alleged to let botnet operators attack foreign entities with impunity, in some instances because the cybercriminal outfits are paying off corrupt officials and in other cases because the government views such actors as national assets and actively sponsors such tactics.[xxiii] Russia, for instance, does not even allow for offenders to be extradited to the country where the offence has been committed under any circumstances.[110] As a result, much botnet activity is directed from outside of Western countries and often, US law enforcement can target botmasters and their clients only when they travel outside of the borders of an uncooperative jurisdiction.[111] Kim et al. suggest that to avoid increased risk of punishment in the US, attackers may strategically situate the botnet infrastructure in regions where the risk of punishment is perceived to be lower.[112]

Consequently, there exist safe havens where botnet operators are free to use the Internet to commit crimes affecting victims in multiple jurisdictions but highly unlikely to face arrest and punishment for these crimes. While law enforcement authorities must respect international borders in their pursuit of justice, botnet-based attacks and crimes have no such restrictions on their destructive reach. There is thus a need for improved country-to-country collaboration to minimize the existence of safe havens for botnet operators.

5.2.3.4 Slow multi-jurisdictional law enforcement investigations

Based around specific jurisdiction, law enforcement is at best unwieldy across national boundaries given the long-winded procedures U.S. cyber investigators have to follow even when collaborating with close allies. Mutual Legal Assistance Treaties (MLATs) govern data exchanges across jurisdictions. MLAT requests must travel through multiple levels of diplomatic and legal bureaucracy, and are answered at the discretion of the country that receives the request. However, the MLATs process was developed in the 1970s and was not designed to accommodate complex cyber investigations. It takes an average of 10 months for the U.S. to respond to another nation's MLAT request – and when the U.S.

[xxiii] Historically, when the U.S. would approach countries like Russia to seek help with investigating an individual, it appeared at times that the regime would use the tip "as a way to recruit for its own law enforcement or intelligence agencies". See: Bradley Barth, "Cybercriminals Find Many Safe Havens."

requests information from a foreign entity, a 10-month response time is a "best case-scenario."[xxiv] While botnet operators often move quickly to erase traceable records of their actions online, such delays can severely damage the effectiveness of an investigation. Speaking on the DoJ's fight against botnets, Assistant Attorney General Caldwell identified the slow MLAT process as a factor that has "harmed our relationships with foreign law enforcement agencies".[113]

Additionally, countries have mismatched legal assistance treaties, conflicting laws, and differing norms with no comprehensive framework for navigating cross-border jurisdictional disputes. Such a patchwork of laws and rules impedes law enforcement action against botnets, even when the source of an attack is well identified. Some of these legal challenges were first broadly identified in the Budapest Convention on Cybercrime that came into force in 2004 and was developed to address many of these jurisdictional issues, but it is uncertain whether the treaty has led to a greater degree of cooperation between law enforcement agencies and governments.[xxv] The present cooperation in detection, investigation, and prosecution both domestically and internationally, including the Convention, is insufficient for relieving the global threats posed by botnets. Therefore, agreements between countries are needed to prosecute cyber-crime in a consistent and coordinated way.

5.2.3.5 Finding motivated plaintiffs

The aggressive civil actions by Microsoft highlight the proactive role of the private sector in addressing a thorny and seemingly intractable global problem. The legal approach used by Microsoft reduced botnet activity and helped users with infected computers apart from generally increasing the level of cybersecurity. Although similar civil lawsuits could be used by many private entities to exert economic pressure on botnet operators, it is important to note that Microsoft was incentivized to act against actors who damaged its reputation and competitiveness by counterfeiting and mimicking its products, as well as weakening its advertising business model through click fraud. This led the company to not be complacent in its attempt to mitigate the problem and develop the most cost-effective solution.[xxvi]

[xxiv] A 2013 study found that the average "turnaround" time for an MLAT request is ten months, "with some requests taking considerably longer." See: Clarke, Richard, et. al. "Liberty and Security in a Changing World." p. 227; David Bitkower, "International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests."

[xxv] These include: "Recognising the need for cooperation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies; (and) Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international cooperation in criminal matters". See: Council of Europe, "Convention on Cybercrime."

[xxvi] Concerning 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." See: Brian Krebs, "Microsoft Responds to Critics Over Botnet Bruhaha."

However, finding other private entities with similarly high stakes in the fight against botnets could prove difficult.[xxvii]

5.2.3.6 The long-term ineffectiveness of domain name takedowns

In its offensive against the Strontium botnet launched by a cyber-espionage hacking group known as Fancy Bear or APT28 that has been connected to attacks related to the 2016 U.S. presidential election among other high-profile attacks,[114] Microsoft sought to temporarily seize 22 Fancy Bear domains, including the ActBlues[.]com address used in an attack on the Democratic Congressional Campaign Committee.[xxviii] However, almost as soon as Microsoft began sinkholing the domains, Fancy Bear responded by registering another batch of names that sent Microsoft back to court for a supplemental order to seize the new addresses. The cat-and-mouse game has continued unabated with Microsoft painstakingly analyzing Fancy Bear's choices of domain names, registrars and webmail providers, and even developing a list of 140 words most likely to appear in a Fancy Bear domain. By March 2017, Microsoft had been back five times for supplemental orders, and grabbed a total of 70 domains from the Russians.[115] Although Microsoft has concluded in court filings that its efforts have had "significant impact" on Fancy Bear's operations[116] and has streamlined the takedown process such that a new domain can be challenged and seized in as little as 24 to 48 hours,[117] the only response from Strontium operators so far has been to calmly register more command-and-control domains with each wave of takedowns.[xxix]

This shows that despite having the resources of a well-equipped corporation, domain name takedowns can only represent part of the approach in botnet mitigation. Other factors such as successful criminal prosecutions of botmasters remain valuable measures because "systems don't rebuild themselves without the master".[118] In fact, arrests of two botnet masters in the past three years "led to a huge and almost immediate halt in the use of those malicious creations."[119] One security researcher has argued that takedowns are ineffective and trigger countermeasures, comparing botnet takedowns to seizing the

---

[xxvii] 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 Security, "Facebook and the FBI Partner to Take Botnet Offline."

[xxviii] Instead of registering generic domains for its cyber espionage operations, Fancy Bear often picked domain names that look-alike Microsoft products and services, such as livemicrosoft[.]net and rsshotmail[.]com, in order to carry out its hacking and cyber espionage campaigns. This inadvertently gave Microsoft an opportunity to drag the hacking group with "unknown members" into the court of justice by alleging that Strontium has created command-and-control domains "designed to cause harm to Microsoft, its customers and licensees, and the public." See: Microsoft Corp. v. John Does 1–2, Civil Action No: 1:16-CV-993 (E.D. Va.). (For unsealed court documents, see: "Strontium." August 6, 2016. Accessed July 24, 2018. https://www.noticeofpleadings.com/strontium/#)

[xxix] As part of streamlining the domain takedown process, a retired judge has been appointed to serve as an independent "court monitor" overseeing the takedown requests. Additionally, Microsoft has sought an order to prospectively seize a list of none thousand other Microsoft-themed domains from Fancy Bear that have never been registered, but which the company's algorithms suggest might be used in the future. See: Microsoft Corp. v. John Does 1–2, Civil Action No: 1:16-CV-993 (E.D. Va.).

baseball bat from a habitual home invader.[120] He argues that the criminal will just buy a new bat, or even worse, buy a gun, making him more dangerous in the future, stating that "[I]t's obvious that the criminals using Citadel won't stop doing cybercrime."[121] While effective for short-term disruption, domain seizures and takedowns would merely result in attackers updating their software and improving their defense mechanisms, thereby making proactive measures the only viable means of mitigating botnets in the long term.[122]

As illustrated in this section, botnet takedowns are analogous to playing a game of whack-a-mole in that they represent a highly reactive approach to defense against persistent adversaries. The ability of botnet operators to move attacks across national borders in an agile manner while defenders face a myriad of jurisdictional and coordination challenges further boosts the benefit–cost ratio for botnet operators pursuing an expanding range of attacks and exploitations. The next section discusses measures to more proactively address the root causes of the emergence of botnets.

6. Potential interventions along the botnet attack chain: A way forward

The above discussion shows that the emergence of botnets and corresponding ad-hoc takedown efforts thus far have been ineffective for long-term and sustainable botnet mitigation. As security researchers and law enforcement engage in more botnet takedowns, botmasters implement more resilient features, resulting in endless cat-and-mouse escalation. As explained in Section 2, botnets are a classic example of an economic externality. Since market forces cannot sufficiently tackle this phenomenon, intervention is required. Given the interplay of moves and counter-moves by botmasters and defenders, it is apparent that technical interventions alone are insufficient to curb the spread and use of botnets that continue to adopt increasingly sophisticated methods to achieve malicious ends.

Botnets will continue to operate and spread unless proactive steps are taken to address the factors that enable botnet attacks and exploitations rather than only mitigating its symptoms. However, comprehensive and effective interventions are difficult because operating a botnet involves a number of stages, and each stage can be accomplished in multiple different ways. First, a botnet must infect machines by exploiting technical insecurities or via social engineering. Second, it must establish communications between the C&C servers and infected bots to carry out C&C commands. Finally, it must perform the task it was developed or rented for, i.e. take money or data back to the botmaster, or disrupt a particular service or website via a DDoS attack. Analyzing each of these stages core to the functionality of a botnet can help explain why botnets persist, and aid in finding effective interventions. Consequently, no one solution exists. Instead, a multitude of steps and policy interventions are needed to holistically tackle threats posed by botnets by exploiting weaknesses in the botnet attack model as well as reducing the safe havens in which they operate.

6.1 Preventing and Tracking Botnet Infections

The first challenge in building a botnet is that of infecting machines at scale. Since bots are recruited to be part of a botnet by exploiting vulnerabilities in insecure devices, a first line of defense could be the widespread enforcement of certain minimum security standards for manufacturers. However, this can prove to be difficult in practice since the incentives of users and market players not aligned with the public goal of better security as discussed in Section 2. What exacerbates the challenge of coordinating technical fixes and promulgating new policy to safeguard consumers is that botnets can exploit insecure devices from any part of the world to attack victims located anywhere. A recent case study is that of the Mirai botnet that had the bulk of its infections (41.5%) stemming from IoT devices located in Brazil, Colombia, and Vietnam, whereas the botnet's victims were distributed across 85 countries and heavily concentrated in the U.S. (50.3%), France (6.6%), and the U.K. (6.1%) among others.[xxx] Mirai's reach extended across borders and legal jurisdictions, and it infected devices with little infrastructure to effectively apply security patches in regions considered by the black market to have ample low-quality hosts used for proxies and DDoS attacks.

While many vulnerabilities can be avoided using existing security tools and practices, adoption remains a significant challenge given the lack of awareness, expertise or market incentives. The case of the Mirai botnet illustrates the need for globally accepted security standards and practices in the development of Internet-connected devices. To achieve this, a recent U.S. government report recommends that industry should establish internationally applicable standards and the federal government should "promote international adoption of best practices and relevant tools through bilateral and multilateral international engagement".[123]

However, even if the majority of obvious security vulnerabilities were removed by IoT device and other manufacturers via market or regulatory incentives and pushback, there would still be room for botnet infestations via social engineering attacks.[xxxi] Even users with heightened awareness of security risks and solutions remain vulnerable to attacks involving social engineering, which continues to be notoriously difficult to counter given the shifting tactics adopted by attackers in response to their targets' security behaviors.[xxxii] Nevertheless, the widespread adoption of baseline security tools and practices would have a significant impact in reducing botnet activity resulting from increasingly available

[xxx] Mirai's infection patterns could possibly have been strongly influenced by the market shares and design decisions of certain consumer electronics manufacturers in those regions. See: Antonakakis et. al., "Understanding the Mirai Botnet."

[xxxi] Such attacks typically involve some form of psychological manipulation, causing unsuspecting victims to reveal sensitive information, click a malicious link, or open a malicious file to trick users into downloading malicious software.

[xxxii] Research has shown that attackers shift tactics in response to targets' security behaviors. For instance, targets who employed two-factor authentication received specially designed phishing crafted to capture both passwords and authorization codes. See: Kleemola et al., "London Calling: Two-Factor Authentication Phishing From Iran."

unsecured devices.[xxxiii] Additionally, a move from optional to mandatory baseline security features on user devices and accounts causing minimal inconvenience to users could help mitigate some of the security concerns associated with low user adoption.[xxxiv]

6.2 Disrupting Botnet Communications

The aforementioned discussion shows that botnets significantly rely on utilizing domain names to support agile C&C infrastructures (Section 3), and that domain name takedowns remain the predominant means of stopping botnet attacks and exploitations (Section 5). This highly-reactive approach where botnet operators continue to register domains and defenders must continue to take them down is not sustainable for mitigating botnet attacks and exploitations over the long term. Furthermore, by analyzing seven years of data on the C&C servers of botnets that have engaged in attacks on financial services, Tajalizadehkhoob et al. show that the speed with which providers take down C&C domains has only a weak relation with C&C occurrence rates, concluding that attackers have little to no preference for providers who allow long-lived C&C domains.[124] This suggests that pro-actively mitigating botnet-related DNS abuse rather than reactive domain name takedowns could be helpful for addressing the source of the problem. While past work in this area has focused on building DNS reputation systems to distinguish legitimate domains from malicious ones and adding malicious domains to blacklists, this does not prevent botmasters and their clients from registering new malicious domains even as their old domains become blacklisted. In this regard, proactive reputation systems that can accurately and automatically identify malicious domains before they start to appear on blacklists or at time-of-registration rather than later at time-of-use could contribute towards preventing botnet attacks and exploitations.[xxxv]

Additionally, requiring greater scrutiny to identify malicious domains could have a potential deterrent effect on the use of such domains for botnet infestations and communications. Liu et al. showed that there was flight of domain registrations from .cn to .ru in the use of domains for spam messages after significant new regulations by the China Internet Network Information Center in December 2009 that included requirements for formal paper documentation and validation, and limitations on individual registrations.[125] Although

---

[xxxiii] IoT-based botnets saw a massive growth of 140% over the course of 2017 with no indication of any let-up coming soon. See: "Spamhaus Botnet Threat Report 2017."

[xxxiv] Aatif Sulleyman, "Gmail Two-Step Verification: Less than 10% of Google Users Have Its Most Important Security Feature Enabled."; Marczak et al. showed that a significant number of subjects with specialized awareness of security risks did not enable optional security features on their devices or online accounts. See: Marczak and Paxson, "Social Engineering Attacks on Government Opponents: Target Perspectives."

[xxxv] One approach that has been developed uses only time-of-registration features to establish domain reputation and predict malicious domains when they are registered at a 70% detection rate. See: Hao et al., "PREDATOR.";

Another approach relies on analyzing the unique characteristics of malicious use of DNS and distinguishing it from legitimate and professional uses of DNS services. Antonakakis et al. developed a dynamic reputation system using passive DNS data to classify domains and assign a reputation score to the new domains to identify malicious domains significantly before they appear on public blacklists. See: Antonakakis et al., "Building a Dynamic Reputation System for DNS."

it is plausible that more stringent identification requirements for domain registration may correlate with lower abuse rates, such policies may not be desirable for groups who rely on safe anonymous registration to exercise free speech and expression.[xxxvi] Similarly, price and registration restrictions appear to affect which registrars and registries cybercriminals choose for DNS abuse, making low priced domain names with easy registrations attractive attack vectors.[126] Nonetheless, the same qualities may be appealing for registrants with legitimate interests and the overarching goal of a free and open Internet. However, registries that do not impose registration eligibility restrictions can still reduce technical DNS abuse through proactive means such as identifying repeat offenders, monitoring suspicious registrations, and actively detecting abuse instead of merely waiting for complaints to be filed.

DNS abuse is not random. To ensure that counter-abuse efforts do not adversely affect non-malicious users, proactive botnet mitigation efforts should be focused on domain registrars and registries that enable high levels of abuse. Hao et al. observed that 46% of the spam domains come from just two registrars.[127] A report by ICANN's Competition, Consumer Trust, and Consumer Choice Review Team (CCT) also concluded that: "Certain registries and registrars appear to either positively encourage or at the very least willfully ignore DNS abuse."[128] Additionally, an ICANN-commissioned study found that two specific registrars had overwhelming rates of abuse and highlighted certain behaviors, such as spontaneous and bulk domain registration features, that appear to enable abuse and harm consumer trust.[xxxvii]

The high levels of DNS abuse concentrated in a relatively small number of registries, registrars and geographic regions that appears to have gone on unremedied for an extended amount of time in some cases suggest that focused counter-abuse efforts could increase costs for botnet operators. Currently, registrars and registry operators associated with extremely high rates of technical DNS abuse continue operating and face little incentive to prevent technical DNS abuse. While registrars oppose having more requirements placed on them, ICANN, as a non-profit organization with direct contractual relationships with registrars and registries, can use its authority to encourage proactive steps against DNS abuse. This is especially important since local interventions on a registry or registrar level are likely to be ineffective given that malicious actors appear quite resilient to localized efforts; such policy changes can in fact lead to displacements in

[xxxvi] A report from an ICANN Expert Working Group on gTLD Directory Services acknowledges that certain groups have legitimate needs for heightened privacy protection such as religious minorities under threat, journalists operating in hostile territory, free political speech, etc. See: ICANN Expert Working Group Final Report, "A Next-Generation Registration Directory Service (RDS)."

[xxxvii] More than 93% of the new gTLD registrations sold by China's Nanjing Imperiosus Technology appeared on blacklists. ICANN eventually suspended Nanjing in January 2017, citing its failure to comply with the RAA for reasons than its sustained high abuse rates. Another registrar, Alpnames Ltd., based in Gibraltar, was associated with a high volume of abuse. The study notes that this registrar used price promotions that offered domain name registrations for $1 USD or sometimes even free. Moreover, Alpnames permitted registrants to randomly generate and register 2,000 domain names in 27 new gTLDs in a single registration process. See: Korczynski´ et al., "Statistical Analysis of DNS Abuse in gTLDs Final Report."

domain use between registrars or TLDs but not to appreciable reductions in overall malicious activity.[129] Thus, any such intervention would need to be scaled globally by ICANN and country-level entities to effectively increase the costs of domain registration for malicious actors.

ICANN should prioritize its attention to compliance matters relating to parties that exhibit consistently higher rates of abuse, and incentivize the implementation of proactive anti-abuse measures by such registry operators. In this regard, the CCT report recommends that registries and registrars with over 10% of their names used for abusive purposes should be tasked by ICANN with proactively cleaning up their zones.[130] Those that fail to do so should be subject to a new Domain Abuse Dispute Resolution Process, and should have their contracts suspended when they are "associated with unabated, abnormal and extremely high rates of technical abuse".[131] Other options for encouraging proactive anti-abuse measures include financial incentives such as fee reductions for registries that screen registrations to detect malfeasance. There exists precedent for ICANN adjusting its fee price structure to address harmful behavior, such as abolishing the automatic fee refund for domain tasters that seriously restricted registrars' ability to get registry refunds.[132] Simultaneously, the CCT Review Team proposes strengthening the consequences for culpable or complacent conduits of technical DNS abuse. This is because although ICANN's current Registrar Accreditation Agreement requires registrars to take "reasonable and prompt steps to investigate and respond appropriately to any reports of abuse" and publish abuse-handling procedures, there are no explicit enforcement mechanisms for preventing DNS abuse.[133]

Although it is unlikely that any set of the aforementioned measures will completely stamp out DNS abuse, these proactive measures can make it appreciably more costly for botnet operators to use the domains essential to their botnet-controlling activities. Additionally, since there exists the possibility of botnets adopting new modes of C&C communication to become more stealthy and resilient (See Section 3.3), there is a need to complement DNS anti-abuse efforts with research on detecting and disrupting botnet abuse in privacy-enhancing and anonymity-providing networks in ways that do not compromise anonymity and usability for other users.

6.3 Following the Monetary Trail

One effective way of tackling botnet-related financial crime is attacking its Achilles heel i.e. disrupting the economic incentives by "following the money". While useful for tracking financially motivated botnets, this mitigation strategy does not apply in cases where botnets are used for purposes other than making money such as for data exfiltration by a foreign government.

Many cyber criminals using botnets for phishing are motivated by profit. Examining Internet bank phishing in Australia led one researcher to conclude that focusing on the activity of Internet money mules and wire transfer agents, such as Western Union, would be more impactful than a sole reliance on technical controls since without these payment platforms

and facilitators, the botnet operators obtain no benefit.[xxxviii] While payment platforms typically operate within the law and have worked with industry to warn users of being used as Internet money mules, a review of the material Western Union supplied to customers showed they could be more explicit in warning customers and potentially more proactive in identifying fraudulent transactions.[134] McCombie and Pieprzyk (2010) proposed a strategy that places more law enforcement focus on financial transactions to detect such money laundering to significantly impact the success of the phishing attack model.[135]

Additionally, email spam continues to exist several years after Bill Gates' optimistic prediction that spam would be eradicated in only two years because it fuels a profitable enterprise.[136] In a study on the use of botnets to send spam, Levchenko et al. investigate the full structure of the spam enterprise, providing the first strong evidence of payment bottlenecks in the spam value chain.[xxxix] The researchers found that 95% of the credit card transactions for the spam-advertised products were handled by just three financial companies with significant sharing and concentration of payment infrastructure.[xl] Similar to the phishing case study by McCombie, the researchers found that the weak link in the spam network was the Visa payment system handling transactions between banks. By blocking the transactions at the point where the consumer uses a credit card, it would be possible to shift the cost burden to the spammers. In such cases, the defenders can identify which banks the spammers are using faster than the spammers can get new banks, and for virtually zero cost whereas the cost of finding and switching to new banks would be high for spammers. Therefore, if a few payment companies refused to authorize online credit card payments to such merchants, it would cut off the money supporting the entire spam enterprise. Additionally, security researchers could aid financial companies in improving detection methods to identify the payment accounts used for botnet-based exploitations.

In analyzing a search engine optimization (SEO) botnet, Wang et al. found that undermining monetization was a much more effective intervention against the botnet as opposed to targeting the botnet infrastructure directly.[xli] [137] A study of a payment intervention regarding botnet-based DDoS-for-hire services, also known as booters, found a similar

[xxxviii] After identifying the various activities supporting phishing (i.e. the construction of infrastructure such as botnets, the acquisition of spam lists, research and development of content to trick users, development of malware to capture passwords, DDoS attacks on response organisations and the recruitment and management of Internet money mules), McCombie determined that the money laundering aspects of the phishing attack model are its greatest weakness. See: McCombie, "Phishing the Long Line: Transnational Cybercrime from Eastern Europe to Australia."

[xxxix] The researchers looked at nearly a billion messages and spent several thousand dollars on about 120 purchases of spam-advertised products. See: Levchenko et al., "Click Trajectories: End-to-End Analysis of the Spam Value Chain."

[xl] For instance, most herbal and replica purchases cleared through the same bank in St. Kitts, while most pharmaceutical affiliate programs used two banks (in Azerbaijan and Latvia), and software was handled entirely by two banks (in Latvia and Russia).

[xli] An SEO botnet can manipulate search engine rankings for key search terms, ultimately directing users to sites promoting some kind of scam e.g., fake antivirus.

conclusion.[xlii][138] Karami et al. empirically demonstrated that payment interventions that undermine the accessibility of convenient payment methods such as PayPal could potentially reduce the scale of DDoS-for-hire services by increasing their costs.[139] After an intervention that reduced the availability of PayPal, the researchers found that the percentage of active booters dropped significantly while several booters shut down their business or switched to alternative payment methods, such as Bitcoin. However, these new payment methods did result in reduced customer bases for booters that could not directly accept credit card payments. Thus, an increased effort to locate and blacklist low-cost hosting services that cater to DDoS attacks could be effective.

The aforementioned studies offer evidence that the payment tier is the most concentrated and valuable asset for mitigating botnet abuse in the phishing, spam, SEO and DDoS-for-hire ecosystems. Since botnet operators rely on just a few banks and an even smaller number of credit card processors, this business is highly vulnerable to disruption by regulators and law enforcement agencies. Levchenko et al. conclude that a "financial blacklist" could be updated far more quickly than the turnaround time to acquire new banking resources—a rare asymmetry favoring botnet fighters and one for which effective intervention through public policy action is possible.[140] Specific legislation that increases the burden on organisations and individuals that transfer money across national boundaries to establish they are not the proceeds of crime could also have the desired effect. Furthermore, as botnet operators switch to cryptocurrencies to retrieve the proceeds of their crimes, this may also open additional avenues for "following the money", which remains an area of active research and careful deliberation.[141]

6.4 Improving the Collaboration Model to Streamline Botnet Mitigation

Since botnets span the globe, it is paramount that different network players and administrative entities take cooperative actions. Presently, the majority of cyber criminals go unpunished, with their capabilities often exceeding those of the authorities responsible for stopping them.[142]

As discussed in Section 5, botnet mitigation is a highly collaborative exercise that depends on the cooperation of various entities, including security researchers, corporations and law enforcement agencies. However, uncoordinated groups of defenders face several challenges. First, Section 4 shows that the spectrum of actions that can be taken by private actors to tackle botnets are mired in a number of legal and ethical challenges. Therefore, while private sector efforts demonstrate an eagerness to tackle the public threats posed by botnets, such efforts must be accompanied by appropriate policy and legal interventions to be effective and sustainable. Second, although security researchers and other private actors play a vital role in the fights against botnets, this decentralized approach faces significant coordination and jurisdictional hurdles apart from a lack of incentives to engage in long-term clean-up efforts. This is especially true in the absence

[xlii] DDoS-for-hire services or booters have commoditized DDoS attacks and enabled abusive subscribers of these services to cheaply extort, harass and intimidate businesses and people by knocking them offline.

of a motivated and resourceful party that has suffered substantial damages to its competitiveness and reputation as a result of botnet activity. Finally, law enforcement collaborations to take down botnets are often impeded by long investigative procedures as well as the existence of safe havens for botnet operators.

One means of being proactive in this case is to build long-term sustainable mechanisms for public-private cooperation as well as streamlining collective action among law enforcement agencies. Some measures for spurring decentralized collaboration are described below.

6.4.1 Clarifying the rules of engagement between private and public sectors

The work of the Conficker Working Group shows that security researchers willing to combat botnets were at a loss as to how to engage with law enforcement authorities to share information in addition to facing concerns over the potential liability of their actions. While various private sector entities such as ISPs and security firms have the expertise and means to respond to botnets, they may not have the undisputed legal authority to do so in certain cases.[xliii] In this regard, the existence of clear and transparent guidelines on the types of legitimate countermeasures, rules for data exchanges with public authorities, and how different forms of cooperation may translate into liability would allow private sector entities to take a more active role in the fight against botnets.[143]

Nadji et al. suggest the adoption of a standard DNS-takedown policy administered by ICANN similar to the "Uniform Dispute Resolution Policy" or URDP, an ICANN policy that specifies independent arbitrators to oversee the process of trademark dispute resolution as it relates to domain names, and make quick and inexpensive decisions relative to courts.[144] However, even with such a policy in place, there would remain room for more comprehensive guidelines that clarify how various entities may cooperate against non-DNS-based botnet C&Cs or non-ICANN administered DNS-based botnet C&Cs. Additionally, clarifying the terms of cooperation between private and public sectors would enable third parties to scrutinize botnet mitigation efforts, thereby reducing potential spillover effects on Internet users and furthering the development of solutions that do not negatively impact fundamental rights such as the rights to privacy, data protection and freedom of speech.

6.4.2 Developing long-term and sustainable collaborations

As mentioned in Section 2 and elaborated in Section 5.1, private sector efforts also face resource constraints and insufficient incentives to act in the public interest against persistent botnet threats in the long term. Asghari et al. suggest that instead of one-time C&C takedowns, "bot remediation needs the mindset of a marathon runner, not a sprinter", giving the example of Finland as a country that has been in the marathon for a longer time

[xliii] As an example, European Union Law does not require Internet intermediaries, let alone manufacturers and software developers, to detect malicious botnets operating in their networks. See: Karine K. e Silva, "How industry can help us fight against botnets: notes on regulating private-sector intervention."

than others have.[145] Such long-term efforts can be made cost-effective by the adoption of automated recommender systems that comprehensively analyze past takedowns to ensure complete and effective future takedowns.[146] Thus, national and international anti-botnet initiatives should support, and perhaps fund, the long-term sustainability of sinkholes in addition to identifying best practices for decentralized working groups and working in tandem with law enforcement to clarify any legal implications of their work.[xliv]

6.4.3 Building collaborations among law enforcement agencies

A recent development regarding cross-border data flows is the passage into law of the Clarifying Lawful Overseas Use of Data Act (CLOUD) Act by the US Congress on March 23, 2018.[147] The CLOUD Act allows the establishment of Executive Agreements allowing law enforcement agencies reciprocal access to data held in each other's countries in order to investigate and prosecute certain crimes. This will enable foreign governments seeking the data of foreigners outside the US to make direct demands to US technology companies under their own laws instead of using existing MLATs. Conversely, those governments must commit to ensuring that US law enforcement can directly request communications content from their local providers. However, bilateral agreements under the Act will only remove legal impediments and potential conflicts of law pursuant to a long list of substantive and procedural safeguards.[xlv] This will encourage interested countries to undertake necessary reforms to adopt privacy-protective standards to facilitate entering into an agreement.[xlvi] Scholars have argued that this will both streamline investigations in light of the unsustainable MLAT system and provide a better alternative in terms of privacy protections to the data localization laws being pursued by foreign governments in the absence of such a development.[148]

While the CLOUD Act has the potential to streamline law enforcement requests between the US and other countries, it remains to be seen whether the Act's provisions could be applied in the context of a high-profile botnet investigation. Additionally, it might be difficult for technology companies - especially, small and medium-sized enterprises - to verify and assess various requests. Thus, there remains room for further streamlining implementation, such as by appointing specific agencies to act as control points to verify, determine lawfulness, and route requests made under the Act. The CLOUD Act presents an

---

[xliv] While in the case of Conficker, ICANN was able to waive the cost of domain registration by security researchers who identified the malicious domains prior to its use by the botnet, one potential use case of public funds established to thwart botnets in the future could be funding the registration costs of domains that have been identified via reverse engineering to soon be used by botnets.

[xlv] The Act permits the U.S. to enter into an Executive Agreement with a foreign government only if the Attorney General and the Secretary of State certify to Congress that, among other things, the foreign government provides "robust substantive and procedural protections for privacy and civil liberties" and that it has adopted procedures to "minimize the acquisition, retention, and dissemination of information concerning United States persons." Congress is afforded 180 days to disapprove any agreement. See: CLOUD Act § 105.

[xlvi] The UK made changes to its laws to ensure compliance with the CLOUD Act's requirements. See: "Associate Deputy Attorney General Sujit Raman Delivers Remarks to the Center for Strategic and International Studies."

opportunity for increasing the efficiency of high-stakes botnet investigations by making cross-border data requests less time-consuming. It will also allow the U.S. to encourage other countries to make privacy-protective adjustments to their own laws and procedures in order to enter into a bilateral agreement, thereby reducing safe havens where botnets may operate without consequences.

7. Conclusion

Why have botnets remained a persistent feature of networks since their inception? Although there is extensive literature on various aspects of botnet attacks and exploitations, this article presents an overview of the full botnet attack model to identify gaps and deficiencies in existing interventions. From the perspective of the attackers, the increasing availability of unsecured Internet-connected devices that can be exploited with cheap and lucrative botnets, as well as the ability of politically motivated actors to exploit botnet infrastructures to their ends without the perception of direct involvement have led to the widespread use of botnets (Section 2). An examination of the technical evolution of botnets shows that the generality of Internet architecture favors the attacker over the defender, as evidenced by the development of peer-to-peer structures and domain generation algorithms among other innovations (Section 3). Regarding the technical development of botnets, the study of new detection and mitigation techniques to subvert botnets exploiting privacy infrastructures such as anonymous networks remains an area of future study. From the defenders' standpoint, technical mitigation methods involve a number of complex tradeoffs with legal and ethical considerations and are insufficient against persistent botnet operators, who continue to constantly evolve their tactics (Section 4). An analysis of past botnet takedown attempts shows that ad-hoc takedowns remain ineffective in the long run in the presence of jurisdictional limitations and safe havens for botnet operators (Section 5).

Proactive interventions at each step of the botnet attack chain along with long-term collaborations among key stakeholders are needed. First, the development and widespread adoption by industry of baseline built-in security standards for Internet-connected devices is paramount to reduce the vulnerabilities that botnets prey on. Concerning user devices and accounts, minimum security standards should be accompanied with mandatory security features that cause minimal inconvenience to users to counter the effects of low user adoption. Second, since present-day botnets predominantly rely on DNS-based C&C communications to function, pro-actively mitigating botnet-related DNS abuse by focusing on the domain name registrars and registries that enable a high level of abuse could be fruitful for addressing the source of the problem instead of a sole reliance on reactive domain name takedowns. Such steps may include identifying domain registration policies that would increase operational costs for botmasters, making botnet attacks and exploitations more difficult and costly to execute without incurring unreasonable inconvenience for non-malicious users. Third, since financially-motivated botnet attacks and exploitations leave a monetary trail and remain lucrative only as long as their payments cannot be traced back, the approach of "following the money" can be more effective in tracking such botnets than technical measures alone.

In this case, closer collaboration between payment providers, security researchers and law enforcement to identify illicit money flows associated with botnet-based activity followed by a refusal by the payment providers to authorize payments to such merchants could help ensure that botmasters do not reap the benefits of their activities. Finally, clarifying the rules of engagement between private actors and public authorities, and setting up long-term working partnerships would promote and streamline both law enforcement botnet takedowns and other private remediation efforts.

8. References

[1] AsSadhan et al., “Detecting Botnets Using Command and Control Traffic.”;

[2] Zeifman, “2015 Bot Traffic Report.”

[3] A. Stevenson, “Botnets Infecting 18 Systems per Second, Warns FBI.”

[4] Ianelli et al., “Botnets as a Vehicle for Online Crime.”; D. Dittrich, “So You Want to Take over a Botnet.”

[5] Weber, “Criminals ‘May Overwhelm the Web.”

[6] Zetter, “Hacker Lexicon: Botnets, the Zombie Computer Armies That Earn Hackers Millions.”

[7] “Android Smartphones ‘Used for Botnet’, Researchers Say.”; Vincent, James. “Could Your Fridge Send You Spam? Security Researchers Report ’Internet.”

[8] Gilbert, “The Evolution of the Botnet.”

[9] Riccardi et al., “Titans’ Revenge.”

[10] Nazario, “Politically Motivated Denial of Service Attacks.”

[11] Crowdstrike Solution Brief, “Promoting Stakeholder Action against Botnets and Other Automated Threats.”

[12] Koziel et al., “Botnets as an Instrument of Warfare.”

[13] Wilson, “Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.”

[14] Scanlon et al., “The Case for a Collaborative Universal Peer-to-Peer Botnet Investigation Framework.”

[15] The Guardian, “North Korea Launched Cyber Attacks, Says South.”

[16] Zetter, “Lawmaker Wants ‘Show of Force’ Against North Korea for Website Attacks.”

[17] van Eeten, “Patching Security Governance.”

[18] Silva et al., “Botnets: A Survey.”

[19] Zang et al., “Botnet Detection through Fine Flow Classification.”

[20] Ibid.

[21] Silva et al., “Botnets: A Survey.”

[22] Li et al., “Botnet: Survey and Case Study.”

[23] Grizzard et al., “Peer-to-Peer Botnets.”

[24] Barford and Yegneswaran, “An Inside Look at Botnets.”

[25] Li et al., “Botnet: Survey and Case Study.”

[26] Robert Westervelt, “Botnet Masters Turn to Google, Social Networks to Avoid Detection.”

[27] Brian Prince, “Flashback Botnet Updated to Include Twitter as C&C.”

[28] Andrea Lelli, “Trojan.Whitewell: What’s Your (Bot) Facebook Status Today?”

[29] Katsuki, “Malware Targeting Windows 8 Uses Google Docs.”; Gallagher, “Evernote: So Useful, Even Malware Loves It.”

[30] D. Dittrich, “So You Want to Take over a Botnet.”

[31] Arce and Levy, “An Analysis of the Slapper Worm.”

[32] Zeidanloo and Manaf, “Botnet Command and Control Mechanisms.”

[33] A. Neville and R. Gibb, “ZeroAccess Indepth”.

[34] Truong and Cheng, “Detecting Domain-Flux Botnet Based on DNS Traffic Features in Managed Network.”

[35] Hao, Feamster, and Pandrangi, “Monitoring the Initial DNS Behavior of Malicious Domains.”

[36] Jamie Riden, “How Fast-Flux Service Networks Work.”

[37] Borgaonkar, “An Analysis of the Asprox Botnet.”

[38] Constantin, “Cybercriminals Are Using the Tor Network to Control Their Botnets.”; Constantin, “Tor Network Used to Command Skynet Botnet.”; Dennis Fischer, “Huge Botnet Found Using Tor Network for Communications.”; Dmitry Tarakanov, “The Inevitable Move - 64-Bit ZeuS Enhanced With Tor.”

[39] Sanatinia and Noubir, “OnionBots: Subverting privacy infrastructure for cyber attacks.”

[40] Frkat et al., “ChainChannels: Private Botnet Communication over Public Blockchains.”

[41] Ali et al., “ZombieCoin 2.0.”

[42] Ibid.

[43] “.Bit - The next Generation of Bulletproof Hosting.” Abuse.ch (blog), September 25, 2017. Accessed August 6, 2018. https://abuse.ch/blog/dot-bit-the-next-generation-of-bulletproof-hosting/.

[44] Cooke, Jahanian, and McPherson, “The Zombie Roundup.”

[45] Bailey et al., “A Survey of Botnet Technology and Defenses.”

[46] Google (blog), “Booting the Bots: New Botnet Protections across Our Ads Systems.”

[47] Dittrich, David. “So You Want to Take over a Botnet.”

[48] Zand et al., “Extracting Probable Command and Control Signatures for Detecting Botnets.”; Gu et al., “BotMiner.”

[49] Ibid.

[50] Eleanor Mills, “BBC buys, uses botnet to show dangers to PCs.”

[51] Stone-Gross et al., “Your Botnet Is My Botnet.”

[52] Dittrich, Leder, and Werner, “A Case Study in Ethical Decision Making Regarding Remote Mitigation of Botnets.”

[53] Vihul et al., “Legal Implications of Countering Botnets.” p. 42-44.

[54] Dittrich, “So You Want to Take over a Botnet.”

[55] Ibid.

[56] Garrett M. Graff, “How the FBI Took down Russia’s Spam King - And His Massive Botnet.”

[57] B. Krebs, “Mariposa Botnet Authors May Avoid Jail Time.”

[58] Nadji et al., “Beheading Hydras.”

[59] Dittrich, Leder, and Werner, “A Case Study in Ethical Decision Making Regarding Remote Mitigation of Botnets.”

[60] Chris Paoli, “Feds Move Forward on Coreflood Botnet Removal.”

[61] Dan Kaplan, “Coreflood Takedown May Lead to Trouble.”

[62] Clark and Landau, “The Problem Isn’t Attribution: It’s Multi-Stage Attacks.”

[63] Graff, “Inside the Hunt for Russia’s Most Notorious Hacker.”

[64] McMillan, “Spanish Police Take Down Massive Mariposa Botnet.”

[65] The Rendon Group, “Conficker Working Group: Lessons Learned.”

[66] Dave Piscitello, “Conficker Summary and Review.”

[67] The Global DNS Security, Stability, & Resiliency Symposium, “Summary, Trends, and Next Steps.”

[68] Dave Piscitello, “Conficker Summary and Review.”

[69] The Rendon Group, “Conficker Working Group: Lessons Learned.”

[70] Ibid.

[71] Hiller, “Civil Cyberconflict.”

[72] A. Neville and R. Gibb, “ZeroAccess Indepth”.

[73] The Rendon Group, “Conficker Working Group: Lessons Learned.”

[74] Dave Piscitello, “Conficker Summary and Review.”

[75] Ibid.

[76] Ibid.

[77] Stone-Gross et al., “Your Botnet Is My Botnet.”

[78] A. Neville and R. Gibb, “ZeroAccess Indepth”.

[79] The Rendon Group, “Conficker Working Group: Lessons Learned.”

[80] Ibid.

[81] D. Dittrich, “So You Want to Take over a Botnet.”

[82] Zach Lerner, “Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets.”; Hiller, “Civil Cyberconflict.”

[83] Zach Lerner, “Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets.”

[84] U.S. Department of Justice Press Release, “Department of Justice Takes Action to Disable International Botnet.”

[85] U.S. Department of Justice Press Release, “Department of Justice Takes Action to Disable International Botnet.”

[86] Tim Cranton, “Cracking Down on Botnets.”

[87] Hiller, “Civil Cyberconflict.”

[88] Ibid.

[89] Tim Cranton, “Cracking Down on Botnets.”

[90] Microsoft Security Intelligence Report,“Waledac: The Legal Action Plan.”

[91] D. Dittrich, “So You Want to Take over a Botnet.”

[92] Microsoft Security Intelligence Report,“Waledac: The Legal Action Plan.”

[93] Borup, “Peer-to-peer botnets: A case study on Waledac”.

[94] Hiller, “Civil Cyberconflict.”

[95] Microsoft Corp. v. Piatti, No. 1:11-CV-1017 (E.D. Va. Sept. 22, 2011).

[96] Ibid.

[97] Yadron, “Police Grapple With Cybercrime.”

[98] Ibid.

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

[100] Zach Lerner, "Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets."

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

[102] John P. Mello Jr., "FBI Declaws Russian Fancy Bear Botnet."

[103] James Vincent, "$500 Million Botnet Citadel Attacked by Microsoft and the FBI."

[104] Lucian Constantin, "Microsoft: Almost 90 Percent of Citadel Botnets in the World Disrupted in June."

[105] Richard D. Boscovich, "Microsoft Works With Financial Services Industry Leaders."

[106] Richard P. Quinn, "The FBI's Role in Cyber Security."

[107] Richard D. Boscovich, "ZeroAccess Criminals Wave White Flag, Official Microsoft Blog."

[108] U.S. v Levashov, Case No. 3: 17-cv-00074 (Alaska 2017).

[109] Garrett M. Graff, "How the FBI Took down Russia's Spam King---And His Massive Botnet."

[110] Ibid.

[111] Jeff Roberts, "Russian Hackers Are Afraid to Travel after U.S. Arrests Spam King."

[112] Kim, Wang, and Ullrich, "A Comparative Study of Cyberattacks."

[113] Department of Justice, "Assistant Attorney General Leslie R. Caldwell Testifies Before the Senate Committee on the Judiciary Subcommittee on Crime and Terrorism."

[114] Schwartz, "Tainted Leaks: Researchers Unravel Cyber-Espionage Attacks."

[115] Kevin Poulsen, "Putin's Hackers Now under Attack—From Microsoft."

[116] Microsoft Corp. v. John Does 1–2, Civil Action No: 1:16-CV-993 (E.D. Va.).

[117] Shaun Nichols, "Microsoft: The Kremlin's Hackers Are Already Sniffing, Probing around America's 2018 Elections."

[118] Alastair Stevenson, "Arresting Hackers More Effective than Botnet Takedowns for Tackling Cybercrime."

[119] Ibid.

[120] Abuse.ch, "Collateral Damage: Microsoft Hits Security Researchers Along with Citadel."

[121] Ibid.

[122] Ibid.

[123] Dept. of Commerce and Dept. of Homeland Security "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats." The Secretary of Commerce and The Secretary of Homeland Security, May 22, 2018.

Accessed August 1, 2018.
https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf

[124] Tajalizadehkhoob et al., "The Role of Hosting Providers in Fighting Command and Control Infrastructure of Financial Malware."

[125] Liu et al., "On the Effects of Registrar-Level Intervention."

[126] Sood and Zeadally, "A Taxonomy of Domain-Generation Algorithms."

[127] Hao et al., "Understanding the Domain Registration Behavior of Spammers."

[128] ICANN, "Competition, Consumer Trust and Consumer Choice (CCT): New Sections."

[129] Liu et al., "On the Effects of Registrar-Level Intervention."

[130] ICANN, "Competition, Consumer Trust and Consumer Choice (CCT): New Sections."

[131] Ibid.

[132] Brian Krebs, "New Policy Aims to Curb Web Site Name Abuse."

[133] Section 3.18, ICANN 2013 Registrar Accreditation Agreement.

[134] McCombie and Pieprzyk, "Winning the Phishing War."

[135] Ibid.

[136] John Leyden, "We'll Kill Spam in Two Years – Gates."

[137] Wang et al., "Juice: A longitudinal study of an SEO botnet."

[138] Karami, Park, and McCoy, "Stress Testing the Booters."

[139] Ibid.

[140] Levchenko et al., "Click Trajectories: End-to-End Analysis of the Spam Value Chain."

[141] Bohannon, "Why Criminals Can't Hide behind Bitcoin."; Meiklejohn et al., "A Fistful of Bitcoins."

[142] Kim, Wang, and Ullrich, "A Comparative Study of Cyberattacks."

[143] Ibid.

[144] Nadji et al., "Beheading Hydras."

[145] Asghari, Ciere, and Van Eeten, "Post-Mortem of a Zombie."

[146] Nadji et al., "Beheading Hydras."

[147] H.R.4943 - 115th Congress (2017-2018): CLOUD Act.

[148] Daskal and Swire, “Why the CLOUD Act Is Good for Privacy and Human Rights.”

9. Full Bibliography

".Bit - The next Generation of Bulletproof Hosting." Abuse.ch (blog), September 25, 2017. Accessed August 6, 2018. https://abuse.ch/blog/dot-bit-the-next-generation-of-bulletproof-hosting/.

"A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats." The Secretary of Commerce and The Secretary of Homeland Security, May 22, 2018. Accessed August 1, 2018. https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf

"Android Smartphones 'Used for Botnet', Researchers Say." BBC News, July 5, 2012. Accessed August 4, 2018. https://www.bbc.com/news/technology-18720565;

"Booting the Bots: New Botnet Protections across Our Ads Systems." Inside AdWords (blog), February 9, 2016. Accessed February 17, 2018. https://adwords.googleblog.com/2016/02/booting-bots-new-botnet-protections.html.

"Conficker Working Group: Lessons Learned." The Rendon Group, January 2011. Accessed August 4, 2018. http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf

"Facebook and the FBI Partner to Take Botnet Offline." Facebook Security, December 12, 2012. Accessed August 4, 2018. https://www.facebook.com/notes/facebook-security/facebook-and-the-fbi-partner-to-take-botnet-offline/10151134554125766.

"Global Network Service Providers: Securing a Position to Challenge the Botnet." Level 3 Communications, 2014. Accessed August 5, 2018. http://www.level3.com/-/media/files/white-paper/en_secur_wp_botnet_white_paper.pdf

"International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests." Statement of David Bitkower, Principal Deputy Assistant Attorney General, Criminal Division, Department of Justice, Before the Committee on the Judiciary, US House of Representatives, February 25, 2016.

"Mariposa Botnet." Panda Security Mediacenter (blog), March 3, 2010. Accessed August 4, 2018. https://www.pandasecurity.com/mediacenter/malware/mariposa-botnet/.

"North Korea Launched Cyber Attacks, Says South." The Guardian, July 11, 2009. Accessed August 4, 2018. http://www.theguardian.com/world/2009/jul/11/south-korea-blames-north-korea-cyber-attacks.

"Spamhaus Botnet Threat Report 2017." Spamhaus Malware Labs, January 8, 2018. Accessed August 1, 2018. https://www.spamhaus.org/news/article/772/spamhaus-botnet-threat-report-2017.

"The Cost of Renting an IoT Botnet." Nuvias Blog (blog), September 19, 2017. Accessed August 5, 2018. https://www.nuviasblog.com/main-category/security/cost-renting-iot-botnet/.

A. Neville and R. Gibb. "ZeroAccess Indepth". White paper, Symantec, Oct. 4 2013. Accessed August 6, 2018. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/zeroaccess-indepth-13-en.pdf.

A. Stevenson. "Botnets Infecting 18 Systems per Second, Warns FBI." V3, July 16 2014. Accessed February 16, 2018. https://www.v3.co.uk/v3-uk/news/2355596/botnets-infecting-18-systems-per-second-warns-fbi.

Aatif Sulleyman, "Gmail Two-Step Verification: Less than 10% of Google Users Have Its Most Important Security Feature Enabled." The Independent, January 22, 2018. Accessed August 4, 2018. https://www.independent.co.uk/life-style/gadgets-and-tech/news/gmail-two-step-verification-2fa-google-account-users-security-feature-cyber-crime-a8172391.html.

Abu Rajab, Moheeb, Jay Zarfoss, Fabian Monrose, and Andreas Terzis. "A Multifaceted Approach to Understanding the Botnet Phenomenon." In *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*, 41–52. IMC '06. New York, NY, USA: ACM, 2006. https://doi.org/10.1145/1177080.1177086.

Abuse.ch, "Collateral Damage: Microsoft Hits Security Researchers along with Cit…." archive.is, June 19, 2013. Accessed August 4, 2018. http://archive.is/F2yWw.

Alastair Stevenson. "Arresting Hackers More Effective than Botnet Takedowns for Tackling Cybercrime." V3, Feb. 10, 2014. Accessed August 4, 2018 www.v3.co.uk/2327200.

Ali, Syed Taha, Patrick McCorry, Peter Hyun-Jeen Lee, and Feng Hao. "ZombieCoin 2.0: Managing next-Generation Botnets Using Bitcoin." International Journal of Information Security 17, no. 4 (August 1, 2018): 411–22. https://doi.org/10.1007/s10207-017-0379-8.

Andrea Lelli, "Trojan.Whitewell: What's Your (Bot) Facebook Status Today?" Symantec Security Response, October 31, 2009. Accessed February 16, 2018. http://www.symantec.com/connect/blogs/trojanwhitewell-what-s-your-bot-facebook-status-today.

Antonakakis et. al., "Understanding the Mirai Botnet", 26th USENIX Security Symposium, August 2017.

Antonakakis, Manos, Roberto Perdisci, David Dagon, Wenke Lee, and Nick Feamster. "Building a Dynamic Reputation System for DNS." In Proceedings of the 19th USENIX Conference on Security, 18–18. USENIX Security'10. Berkeley, CA, USA: USENIX Association, 2010. http://dl.acm.org/citation.cfm?id=1929820.1929844.

Arce, Iván, and Elias Levy. "An Analysis of the Slapper Worm." IEEE Security and Privacy 1, no. 1 (January 2003): 82–87. https://doi.org/10.1109/MSECP.2003.1177002.

Asghari, Hadi, Michael Ciere, and Michel J. G. Van Eeten. "Post-Mortem of a Zombie: Conficker Cleanup After Six Years." In Proceedings of the 24th USENIX Conference on Security Symposium, 1–16. SEC'15. Berkeley, CA, USA: USENIX Association, 2015. http://dl.acm.org/citation.cfm?id=2831143.2831144.

AsSadhan, B., J. M. F. Moura, D. Lapsley, C. Jones, and W. T. Strayer. "Detecting Botnets Using Command and Control Traffic." In *2009 Eighth IEEE International Symposium on Network Computing and Applications*, 156–62, 2009. https://doi.org/10.1109/NCA.2009.56.

B. Krebs. "Mariposa Botnet Authors May Avoid Jail Time." March 4, 2010. Accessed August 5, 2018. https://krebsonsecurity.com/2010/03/mariposa-botnet-authors-may-avoid-jail-time/.

Bailey, M., E. Cooke, F. Jahanian, Y. Xu, and M. Karir. "A Survey of Botnet Technology and Defenses." In 2009 Cybersecurity Applications Technology Conference for Homeland Security, 299–304, 2009. https://doi.org/10.1109/CATCH.2009.40.

Barford, Paul, and Vinod Yegneswaran. "An Inside Look at Botnets." In Malware Detection, 171–91. Advances in Information Security. Springer, Boston, MA, 2007. https://doi.org/10.1007/978-0-387-44599-1_8.

Barford, Paul, and Vinod Yegneswaran. "An Inside Look at Botnets." In Malware Detection, 171–91. Advances in Information Security. Springer, Boston, MA, 2007. https://doi.org/10.1007/978-0-387-44599-1_8.

Berinato, Scott. “Attack of the Bots.” Wired, November 1, 2006. Accessed August 5, 2018. https://www.wired.com/2006/11/botnet/.

Borgaonkar, Ravishankar. “An Analysis of the Asprox Botnet.” In Proceedings of the 2010 Fourth International Conference on Emerging Security Information, Systems and Technologies, 148–153. SECURWARE ’10. Washington, DC, USA: IEEE Computer Society, 2010. https://doi.org/10.1109/SECURWARE.2010.32.

Borup, L. T. “Peer-to-peer botnets: A case study on Waledac”. Master’s thesis, Technical University of Denmark, 2009. Accessed August 4, 2018. http://etd.dtu.dk/thesis/241876/ep09_24_net.pdf

Bradley Barth. “Cybercriminals Find Many Safe Havens.” SC Media, November 1, 2016. Accessed August 4, 2018. https://www.scmagazine.com/cybercriminals-find-many-safe-havens/article/569177/.

Brian Krebs, “Microsoft Responds to Critics Over Botnet Bruhaha”, Krebs On Security, April 16, 2012. Accessed August 4, 2018. http://krebsonsecurity.com/2012/04/microsoft-responds-to-critics-over-botnet-bruhaha/.

Brian Prince. “Flashback Botnet Updated to Include Twitter as C&C.” SecurityWeek.Com, April 30, 2012. Accessed February 16, 2018. https://www.securityweek.com/flashback-botnet-updated-include-twitter-cc.

Broersma, Matthew. “Botnet Price for Hourly Hire on Par with Cost of Two Pints.” ZDNet, May 25, 2010. Accessed April 21, 2018. https://www.zdnet.com/article/botnet-price-for-hourly-hire-on-par-with-cost-of-two-pints.

C. Wilson. “Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress”, CRS Report for Congress, RL32114, Congressional Research Service, Washington, DC, 2008. Accessed August 6, 2018. https://fas.org/sgp/crs/terror/RL32114.pdf.

Chris Paoli. “Feds Move Forward on Coreflood Botnet Removal.” GCN, April 29, 2011. Accessed August 5, 2018. http://gcn.com/Articles/2011/04/28/ECG-Feds-To-Remove-Coreflood.

Clark, David D., and Susan Landau. “The Problem Isn’T Attribution: It’s Multi-Stage Attacks.” In Proceedings of the Re-Architecting the Internet Workshop, 11:1–11:6. ReARCH ’10. New York, NY, USA: ACM, 2010. https://doi.org/10.1145/1921233.1921247.

Clarke, Richard, et. al. “Liberty and Security in a Changing World”. Report and Recommendation of the President’s Review Group on Intelligence and Communications Technologies, December 12, 2013. Accessed August 4, 2018. https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

Collins, Doug. “H.R.4943 - 115th Congress (2017-2018): CLOUD Act.” February 6, 2018. Accessed August 4, 2018. https://www.congress.gov/bill/115th-congress/house-bill/4943/text.

Cooke, Evan, Farnam Jahanian, and Danny McPherson. “The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets.” In Proceedings of the Steps to Reducing Unwanted Traffic on the Internet on Steps to Reducing Unwanted Traffic on the Internet Workshop, 6–6. SRUTI’05. Berkeley, CA, USA: USENIX Association, 2005. http://dl.acm.org/citation.cfm?id=1251282.1251288.

Council of Europe, “Convention on Cybercrime”, Budapest, November 23, 2001. Accessed August 4, 2018. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

Crowdstrike Solution Brief, “Promoting Stakeholder Action Against Botnets and Other Automated Threats”, National Telecommunications and Information Administration, U.S. Department of Commerce, July 13, 2017. Accessed August 6, 2018. https://www.crowdstrike.com/wp-content/brochures/datasheets/Solution_Brief_CrowdStrike_Falcon_and_the_NTIA_Botnet.pdf.

Dave Piscitello. “Conficker Summary and Review” ICANN Securities Team, May 7, 2010. Accessed August 4, 2018. https://www.icann.org/en/system/files/files/conficker-summary-review-07may10-en.pdf

Davis, C. R., J. M. Fernandez, S. Neville, and J. McHugh. “Sybil Attacks as a Mitigation Strategy against the Storm Botnet.” In 2008 3rd International Conference on Malicious and Unwanted Software (MALWARE), 32–40, 2008. https://doi.org/10.1109/MALWARE.2008.4690855.

Davor Frkat, Robert Annessi, and Tanja Zseby. “ChainChannels: Private Botnet Communication Over Public Blockchains.” In IEEE International Conference on Blockchain (Blockchain), 2018.

Dennis Fischer, “Huge Botnet Found Using Tor Network for Communications,” Threatpost (blog), September 2013. Accessed July 31, 2018. https://threatpost.com/huge-botnet-found-using-tor-network-for-communications/102179/

Department of Justice Press Release. “Department of Justice Takes Action to Disable International Botnet.” FBI Archives, April 13, 2011. Accessed August 4, 2018. https://www.fbi.gov/newhaven/press-releases/2011/nh041311.htm.

Department of Justice. “Assistant Attorney General Leslie R. Caldwell Testifies Before the Senate Committee on the Judiciary Subcommittee on Crime and Terrorism,” July 15, 2014. Accessed August 4, 2018. https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-testifies-senate-committee-judiciary.

Department of Justice. “Associate Deputy Attorney General Sujit Raman Delivers Remarks to the Center for Strategic and International Studies,” May 31, 2018. Accessed August 4, 2018. https://www.justice.gov/opa/speech/associate-deputy-attorney-general-sujit-raman-delivers-remarks-center-strategic-and.

Dittrich, David, Felix Leder, and Tillmann Werner. “A Case Study in Ethical Decision Making Regarding Remote Mitigation of Botnets.” In Proceedings of the 14th International Conference on Financial Cryptograpy and Data Security, 216–230. FC’10. Berlin, Heidelberg: Springer-Verlag, 2010. http://dl.acm.org/citation.cfm?id=1894863.1894883.

Dittrich, David. “So You Want to Take over a Botnet.” In Proceedings of the 5th USENIX Conference on Large-Scale Exploits and Emergent Threats, 6–6. LEET’12. Berkeley, CA, USA: USENIX Association, 2012. http://dl.acm.org/citation.cfm?id=2228340.2228349.

Dmitry Tarakanov, “The Inevitable Move - 64-Bit ZeuS Enhanced With Tor,” Securelist, December 11, 2013. Accessed July 31, 2018. https://securelist.com/the-inevitable-move-64-bit-zeus-enhanced-with-tor/58184/.

Eeten, Michel Van, and Johannes M. Bauer. “Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications.” Journal of Contingencies and Crisis Management 17, no. 4 (December 1, 2009): 221–32. https://doi.org/10.1111/j.1468-5973.2009.00592.x.

Eeten, Michel van. “Patching Security Governance: An Empirical View of Emergent Governance Mechanisms for Cybersecurity.” Digital Policy, Regulation and Governance 19, no. 6 (September 11, 2017): 429–48. https://doi.org/10.1108/DPRG-05-2017-0029.

Eleanor Mills. “BBC buys, uses botnet to show dangers to PCs.” CNET, March 13, 2009. Accessed August 5, 2018. https://www.cnet.com/au/news/bbc-buys-uses-botnet-to-show-dangers-to-pcs/

Gallagher, Sean. “Evernote: So Useful, Even Malware Loves It.” Ars Technica, March 27, 2013. Accessed August 5, 2018. https://arstechnica.com/information-technology/2013/03/evernote-so-useful-even-malware-loves-it/.

Garrett M. Graff. "How Russian Spam King Peter Levashov Was Arrested, and His Kelihos Botnet Dismantled." WIRED, April 11, 2017. Accessed August 4, 2018. https://www.wired.com/2017/04/fbi-took-russias-spam-king-massive-botnet/.

Garrett M. Graff. "How the FBI Took Down Russia's Spam King---And His Massive Botnet." WIRED, April 11, 2017. Accessed January 30, 2018. https://www.wired.com/2017/04/fbi-took-russias-spam-king-massive-botnet/.

Gilbert, David. "The Evolution of the Botnet." International Business Times UK, February 14, 2013. Accessed August 4, 2018. https://www.ibtimes.co.uk/evolution-botnets-justin-bieber-fans-435301.

Graff, Garrett M. "Inside the Hunt for Russia's Most Notorious Hacker." Wired, March 21, 2017. Accessed August 4, 2018. https://www.wired.com/2017/03/russian-hacker-spy-botnet/.

Grizzard, Julian B., Vikram Sharma, Chris Nunnery, Brent ByungHoon Kang, and David Dagon. "Peer-to-Peer Botnets: Overview and Case Study." In Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets, 1–1. HotBots'07. Berkeley, CA, USA: USENIX Association, 2007. http://dl.acm.org/citation.cfm?id=1323128.1323129.

Gu, Guofei, Roberto Perdisci, Junjie Zhang, and Wenke Lee. "BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection." In Proceedings of the 17th Conference on Security Symposium, 139–154. SS'08. Berkeley, CA, USA: USENIX Association, 2008. http://dl.acm.org/citation.cfm?id=1496711.1496721.

Hao, Shuang, Alex Kantchelian, Brad Miller, Vern Paxson, and Nick Feamster. "PREDATOR: Proactive Recognition and Elimination of Domain Abuse at Time-Of-Registration." In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 1568–1579. CCS '16. New York, NY, USA: ACM, 2016. https://doi.org/10.1145/2976749.2978317.

Hao, Shuang, Matthew Thomas, Vern Paxson, Nick Feamster, Christian Kreibich, Chris Grier, and Scott Hollenbeck. "Understanding the Domain Registration Behavior of Spammers." In Proceedings of the 2013 Conference on Internet Measurement Conference, 63–76. IMC '13. New York, NY, USA: ACM, 2013. https://doi.org/10.1145/2504730.2504753.

Hao, Shuang, Nick Feamster, and Ramakant Pandrangi. "Monitoring the Initial DNS Behavior of Malicious Domains." In Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference, 269–278. IMC '11. New York, NY, USA: ACM, 2011. https://doi.org/10.1145/2068816.2068842.

Hiller, Janine. "Civil Cyberconflict: Microsoft, Cybercrime, and Botnets." Santa Clara High Technology Law Journal 31, no. 2 (January 1, 2014): 163.

Holz, Thorsten, Moritz Steiner, Frederic Dahl, Ernst Biersack, and Felix Freiling. "Measurements and Mitigation of Peer-to-Peer-Based Botnets: A Case Study on Storm Worm." In Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats, 9:1–9:9. LEET'08. Berkeley, CA, USA: USENIX Association, 2008. http://dl.acm.org/citation.cfm?id=1387709.1387718.

ICANN Expert Working Group Final Report, "A Next-Generation Registration Directory Service (RDS)", June 6, 2014. Accessed August 4, 2018. https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf.

ICANN. "2013 Registrar Accreditation Agreement." Accessed July 25, 2018. https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en.

ICANN. "Competition, Consumer Trust and Consumer Choice (CCT): New Sections". Review Team, November 27, 2017. Accessed August 1, 2018. https://www.icann.org/en/system/files/files/cct-rt-draft-recs-new-sections-27nov17-en.pdf.

J. Scott-Railton and K. Kleemola. “London Calling: Two-Factor Authentication Phishing From Iran.” The Citizen Lab, August 27, 2015. Accessed: August 4, 2018. https://citizenlab.org/2015/08/iran_two_factor_phishing/.

James Vincent. “$500 Million Botnet Citadel Attacked by Microsoft and the FBI.” The Independent, June 6, 2013. Accessed August 4, 2018. http://www.independent.co.uk/life-style/gadgets-and-tech/news/500-million-botnet-citadel-attacked-by-microsoft-and-the-fbi-8647594.html.

Jamie Riden. “How Fast-Flux Service Networks Work.” The Honeynet Project, August 16, 2018. Accessed February 16, 2018. https://www.honeynet.org/node/132.

Jeff Roberts, “Russian Hackers Are Afraid to Travel After U.S. Arrests Spam King,” Fortune, April 11, 2017. Accessed February 20, 2018, http://fortune.com/2017/04/11/russian-hackers-levashov-arrest/.

Jennifer Daskal and Peter Swire. “Why the CLOUD Act Is Good for Privacy and Human Rights.” Lawfare, March 14, 2018. Accessed August 4, 2018. https://www.lawfareblog.com/why-cloud-act-good-privacy-and-human-rights.

John Bohannon. “Why Criminals Can’t Hide behind Bitcoin” Science, March 9, 2016. Accessed August 4, 2018. http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin.

John Leyden. “We’ll Kill Spam in Two Years – Gates.” The Register, January 26, 2004. Accessed January 30, 2018. https://www.theregister.co.uk/2004/01/26/well_kill_spam_in_two/.

John P. Mello Jr. “FBI Declaws Russian Fancy Bear Botnet.” TechNewsWorld, May 25, 2018. Accessed August 4, 2018. https://www.technewsworld.com/story/85356.html.

Kaplan, D. “Coreflood Takedown May Lead to Trouble.” April 18, 2011. Accessed August 5, 2018. http://www.scmagazine.com.au/News/254827,coreflood-takedown-may-lead-to-trouble.aspx.

Karami, Mohammad, Youngsam Park, and Damon McCoy. “Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services.” In Proceedings of the 25th International Conference on World Wide Web, 1033–1043. WWW ’16. Republic and Canton of Geneva, Switzerland: International World Wide Web Conferences Steering Committee, 2016. https://doi.org/10.1145/2872427.2883004.

Karine K. e Silva. “How industry can help us fight against botnets: notes on regulating private-sector intervention.” International Review of Law, Computers & Technology, 31:1, 105-130, 2017. DOI: 10.1080/13600869.2017.1275274.

Kevin Poulsen. “Putin’s Hackers Now Under Attack—From Microsoft.” Daily Beast, July 20, 2017. Accessed July 23, 2018. https://www.thedailybeast.com/microsoft-pushes-to-take-over-russian-spies-network.

Kim, Seung Hyun, Qiu-Hong Wang, and Johannes B. Ullrich. “A Comparative Study of Cyberattacks.” Commun. ACM 55, no. 3 (March 2012): 66–73. https://doi.org/10.1145/2093548.2093568.

Knysz, M., Xin Hu, Yuanyuan Zeng, and K. G. Shin. “Open WiFi Networks: Lethal Weapons for Botnets?” In 2012 Proceedings IEEE INFOCOM, 2631–35, 2012. https://doi.org/10.1109/INFCOM.2012.6195668.

Korczynski´ et al., “Statistical Analysis of DNS Abuse in gTLDs Final Report”, August 2017. Accessed August 1, 2018. https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf

Koziel, Eric & Robinson, David. “Botnets as an Instrument of Warfare”. Chapter 2 from book “Critical Infrastructure Protection V” (pp.19-28). 2011. DOI: 10.1007/978-3-642-24864-1_2.

Krebs, Brian. “New Policy Aims to Curb Web Site Name Abuse,” January 30, 2008. Accessed August 4, 2018. http://www.washingtonpost.com/wp-dyn/content/article/2008/01/30/AR2008013002178.html.

Levchenko, Kirill, Andreas Pitsillidis, Neha Chachra, Brandon Enright, Márk Félegyházi, Chris Grier, Tristan Halvorson, et al. "Click Trajectories: End-to-End Analysis of the Spam Value Chain." In Proceedings of the 2011 IEEE Symposium on Security and Privacy, 431–446. SP '11. Washington, DC, USA: IEEE Computer Society, 2011. https://doi.org/10.1109/SP.2011.24.

Li, C., W. Jiang, and X. Zou. "Botnet: Survey and Case Study." In 2009 Fourth International Conference on Innovative Computing, Information and Control (ICICIC), 1184–87, 2009. https://doi.org/10.1109/ICICIC.2009.127.

Liis Vihul, Christian Czosseck, Dr. Katharina Ziolkowski, Lauri Aasmann, Ivo A. Ivanov, Dr. Sebastian Brüggemann, M.A. "Legal Implications of Countering Botnets." Joint report from the NATO Cooperative Cyber Defence Centre of Excellence and the European Network and Information Security Agency (ENISA), 2012.

Liu, He, Kirill Levchenko, Márk Félegyházi, Christian Kreibich, Gregor Maier, Geoffrey M. Voelker, and Stefan Savage. "On the Effects of Registrar-Level Intervention." In Proceedings of the 4th USENIX Conference on Large-Scale Exploits and Emergent Threats, 5–5. LEET'11. Berkeley, CA, USA: USENIX Association, 2011. http://dl.acm.org/citation.cfm?id=1972441.1972448.

Lucian Constantin, "Tor Network Used to Command Skynet Botnet." Computerworld, December 7, 2012. Accessed July 31, 2018. https://www.computerworld.com/article/2493980/malware-vulnerabilities/tor-network-used-to-command-skynet-botnet.htm

Lucian Constantin. "Cybercriminals Are Using the Tor Network to Control Their Botnets." PCWorld, July 25, 2013. Accessed August 4, 2018. https://www.pcworld.com/article/2045183/cybercriminals-increasingly-use-the-tor-network-to-control-their-botnets-researchers-say.html

Lucian Constantin. "Microsoft: Almost 90 Percent of Citadel Botnets in the World Disrupted in June." July 26, 2013. Accessed August 4, 2018. https://www.pcworld.com/article/2045282/microsoft-almost-90-percent-of-citadel-botnets-in-the-world-disrupted-in-june.html.

M. Bowden. "Worm: the First Digital World War". Atlantic Monthly Press, 2011.

M. Fossi, G.Y. Egan, K. Haley, E. Johnson, T. Mack, T. Adams, J. Blackbird, M.K. Low, D. Mazurek, D. McKinney, P. Wood, "Symantec Internet Security Threat Report – Trends for 2010", Technical Report Volume 16, Symantec, 2011.

Marczak, W. R., and Paxson, V. "Social Engineering Attacks on Government Opponents: Target Perspectives." In Proceedings on Privacy Enhancing Technologies, pp. 152–164, 2017.

Mathew J. Schwartz. "Tainted Leaks: Researchers Unravel Cyber-Espionage Attacks." Accessed July 24, 2018. https://www.databreachtoday.com/tainted-leaks-researchers-unravel-cyber-espionage-attacks-a-9955.

McCombie, S., and J. Pieprzyk. "Winning the Phishing War: A Strategy for Australia." In 2010 Second Cybercrime and Trustworthy Computing Workshop, 79–86, 2010. https://doi.org/10.1109/CTC.2010.13.

McCombie, Stephen James. "Phishing the long line: transnational cybercrime from Eastern Europe to Australia." Macquarie University, 2011.

McMillan, R. "Spanish Police Take Down Massive Mariposa Botnet." PCWorld, March 2, 2010. Accessed August 4, 2018. https://www.pcworld.com/article/190634/article.html.

Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names." In Proceedings of the 2013 Conference on Internet Measurement Conference, 127–140. IMC '13. New York, NY, USA: ACM, 2013. https://doi.org/10.1145/2504730.2504747.

Microsoft Security Intelligence Report."Waledac: The Legal Action Plan." In "Battling Botnets for Control of Computers," Volume 9, 2010. p. 46-50. Accessed August 5, 2018. http://download.microsoft.com/download/8/1/B/81B3A25C-95A1-4BCD-88A4-2D3D0406CDEF/Microsoft_Security_Intelligence_Report_volume_9_Battling_Botnets_English.pdf.

N. Ianelli and A. Hackworth. "Botnets as a Vehicle for Online Crime." Coordination Center, CERT cMellon University, Carnegie CERT, 2005. https://resources.sei.cmu.edu/asset_files/WhitePaper/2005_019_001_51249.pdf

Nadji, Yacin, Manos Antonakakis, Roberto Perdisci, David Dagon, and Wenke Lee. "Beheading Hydras: Performing Effective Botnet Takedowns." In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, 121–132. CCS '13. New York, NY, USA: ACM, 2013. https://doi.org/10.1145/2508859.2516749.

Nazario, Jose. "'Politically Motivated Denial of Service Attacks'". In The Virtual Battlefield, 2009. Edited by: Czosseck, Christian and Geers, Kenneth. 163–81. Amsterdam/Washington, DC: IOS Press.

Plohmann, Daniel, Khaled Yakdan, Michael Klatt, Johannes Bader, and Elmar Gerhards-Padilla. "A Comprehensive Measurement Study of Domain Generating Malware." In Proceedings of the 25th USENIX Conference on Security Symposium, 263–278. SEC'16. Berkeley, CA, USA: USENIX Association, 2016. http://dl.acm.org/citation.cfm?id=3241094.3241115.

Porras, Phillip, Hassen Saïdi, and Vinod Yegneswaran. "A Foray into Conficker's Logic and Rendezvous Points." In Proceedings of the 2Nd USENIX Conference on Large-Scale Exploits and Emergent Threats: Botnets, Spyware, Worms, and More, 7–7. LEET'09. Berkeley, CA, USA: USENIX Association, 2009. http://dl.acm.org/citation.cfm?id=1855676.1855683.

Riccardi, Marco, Roberto Di Pietro, Marta Palanques, and Jorge Aguilí Vila. "Titans' Revenge: Detecting Zeus via Its Own Flaws." Comput. Netw. 57, no. 2 (February 2013): 422–435. https://doi.org/10.1016/j.comnet.2012.06.023.

Richard D. Boscovich. "Microsoft Works with Financial Services Industry Leaders, Law Enforcement and Others to Disrupt Massive Financial Cybercrime Ring." The Official Microsoft Blog, June 5, 2013. Accessed August 4, 2018. https://blogs.technet.microsoft.com/microsoft_blog/2013/06/05/microsoft-works-with-financial-services-industry-leaders-law-enforcement-and-others-to-disrupt-massive-financial-cybercrime-ring/.

Richard D. Boscovich. "ZeroAccess Criminals Wave White Flag: The Impact of Partnerships on Cybercrime." The Official Microsoft Blog, December 19, 2013. Accessed August 4, 2018. https://blogs.technet.microsoft.com/microsoft_blog/2013/12/19/zeroaccess-criminals-wave-white-flag-the-impact-of-partnerships-on-cybercrime/.

Richard P. Quinn. "The FBI's Role in Cyber Security." Testimony, Federal Bureau of Investigation, April 16, 2014. Accessed August 4, 2018. https://www.fbi.gov/news/testimony/the-fbis-role-in-cyber-security.

Robert Westervelt. "Botnet Masters Turn to Google, Social Networks to Avoid Detection." TechTarget, November 10 2009. Accessed August 5, 2018. https://searchsecurity.techtarget.com/news/1373974/Botnet-masters-turn-to-Google-social-networks-to-avoid-detection

Sanatinia, Amirali, and Guevara Noubir. "OnionBots: Subverting Privacy Infrastructure for Cyber Attacks." In Proceedings of the 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 69–80. DSN '15. Washington, DC, USA: IEEE Computer Society, 2015. https://doi.org/10.1109/DSN.2015.40.

Scanlon, Mark and Kechadi, Tahar. "The Case for a Collaborative Universal Peer-to-Peer Botnet Investigation Framework". Proceedings of the 9th International Conference on Cyber Warfare and Security (ICCWS 2014), Purdue University, West Lafayette, IN, USA, 24–25 March 2014; pp. 287–293.

Shaun Nichols. "Microsoft: The Kremlin's Hackers Are Already Sniffing, Probing around America's 2018 Elections." July 20, 2018. Accessed July 24, 2018. https://www.theregister.co.uk/2018/07/20/microsoft_fancy_bear_warning/.

Silva, Sérgio S. C., Rodrigo M. P. Silva, Raquel C. G. Pinto, and Ronaldo M. Salles. "Botnets: A Survey." Computer Networks, Botnet Activity: Analysis, Detection and Shutdown, 57, no. 2 (February 4, 2013): 378–403. https://doi.org/10.1016/j.comnet.2012.07.021.

Sinha, P., A. Boukhtouta, V. H. Belarde, and M. Debbabi. "Insights from the Analysis of the Mariposa Botnet." In 2010 Fifth International Conference on Risks and Security of Internet and Systems (CRiSIS), 1–9, 2010. https://doi.org/10.1109/CRISIS.2010.5764915.

Sood, A. K., and S. Zeadally. "A Taxonomy of Domain-Generation Algorithms." IEEE Security Privacy 14, no. 4 (July 2016): 46–53. https://doi.org/10.1109/MSP.2016.76.

Stone-Gross, Brett, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna. "Your Botnet Is My Botnet: Analysis of a Botnet Takeover." In Proceedings of the 16th ACM Conference on Computer and Communications Security, 635–647. CCS '09. New York, NY, USA: ACM, 2009. https://doi.org/10.1145/1653662.1653738.

Tajalizadehkhoob, Samaneh, Carlos Gañán, Arman Noroozian, and Michel van Eeten. "The Role of Hosting Providers in Fighting Command and Control Infrastructure of Financial Malware." In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 575–586. ASIA CCS '17. New York, NY, USA: ACM, 2017. https://doi.org/10.1145/3052973.3053023.

Takashi Katsuki. "Malware Targeting Windows 8 Uses Google Docs." Symantec Security Response, November 16, 2012. Accessed February 16, 2018. http://www.symantec.com/connect/blogs/malware-targeting-windows-8-uses-google-docs

The Global DNS Security, Stability, & Resiliency Symposium. "Summary, Trends, and Next Steps." April 2nd, 2009. Accessed August 4, 2018. https://spinlock.com/wp-content/uploads/2010/02/2009-DNS-SSR-Symposium-Report.pdf

Tim Cranton. "Cracking Down on Botnets." The Official Microsoft Blog (blog), February 24, 2010. Accessed August 4, 2018. https://blogs.microsoft.com/blog/2010/02/24/cracking-down-on-botnets/.

Truong, Dinh-Tu, and Guang Cheng. "Detecting Domain-Flux Botnet Based on DNS Traffic Features in Managed Network." *Security and Communication Networks* 9, no. 14 (September 25, 2016): 2338–47. https://doi.org/10.1002/sec.1495.

U.S. v Levashov, Case No. 3: 17-cv-00074. In the United States District Court For the District of Alaska. Accessed August 4, 2018. https://www.justice.gov/opa/press-release/file/956506/download

Vincent, James. "Could Your Fridge Send You Spam? Security Researchers Report 'Internet." The Independent, January 20, 2014. Accessed August 4, 2018. http://www.independent.co.uk/life-style/gadgets-and-tech/news/could-your-fridge-send-you-spam-security-researchers-report-internet-of-things-botnet-9072033.html.

Wang, D., Voelker, G., and Savage, S. "Juice: A longitudinal study of an SEO botnet." In Proceedings of NDSS'13, San Diego, CA, February 2013.

Weber, Tim. "Criminals 'May Overwhelm the Web." BBC News, January 25, 2007. Accessed August 4, 2018. http://news.bbc.co.uk/2/hi/business/6298641.stm.

William J. Lynn. “Defending a New Domain.” Foreign Affairs, September 1, 2010. Accessed August 4, 2018. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

Xiaonan Zang, Athichart Tangpong, George Kesidis and David J. Miller, CSE Dept Technical Report on “Botnet Detection through Fine Flow Classification” Report No. CSE11-001, Jan. 31, 2011. Accessed August 6, 2018. https://pdfs.semanticscholar.org/65d8/4a548730798d36b181c3cec4d892d2e6612d.pdf

Yadron, Danny. “Police Grapple With Cybercrime.” Wall Street Journal, April 20, 2014, sec. US. Accessed August 4, 2018. https://www.wsj.com/articles/police-grapple-with-cybercrime-1398037674.

Zach Lerner, “Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets”, In Harvard Journal of Law & Technology. Volume 28, No. 1 Fall 2014.

Zand, Ali, Giovanni Vigna, Xifeng Yan, and Christopher Kruegel. “Extracting Probable Command and Control Signatures for Detecting Botnets.” In Proceedings of the 29th Annual ACM Symposium on Applied Computing, 1657–1662. SAC ’14. New York, NY, USA: ACM, 2014. https://doi.org/10.1145/2554850.2554896.

Zeidanloo, H. R., and A. A. Manaf. “Botnet Command and Control Mechanisms.” In 2009 Second International Conference on Computer and Electrical Engineering, 1:564–68, 2009. https://doi.org/10.1109/ICCEE.2009.151.

Zeifman, Igal. “2015 Bot Traffic Report: Humans Take Back the Web, Bad Bots Not...” Incapsula Blog, December 9, 2015. https://www.incapsula.com/blog/bot-traffic-report-2015.html.

Zetter, Kim. “Hacker Lexicon: Botnets, the Zombie Computer Armies That Earn Hackers Millions.” WIRED, December 15, 2015. Accessed February 15, 2018. https://www.wired.com/2015/12/hacker-lexicon-botnets-the-zombie-computer-armies-that-earn-hackers-millions/.

Zetter, Kim. “Lawmaker Wants ‘Show of Force’ Against North Korea for Website Attacks.” WIRED, July 10, 2009. Accessed April 15, 2018. https://www.wired.com/2009/07/show-of-force/.