Deanna Bessy
Comp 116
Final Project

Botnets

Mentor: Ming Chow

Table of Contents

1 Abstract

This paper will explore the concept of botnets and their ramifications for computer security historically and today. It will examine how botnets work, case-studies on notable botnets, and the prevention and dismantling of botnets. The intention of this paper is to provide a survey of a topic that is both interesting and highly pertinent to the security of anyone who uses internet-connected devices today. Amongst the myriad sources of information and ever-growing data on this topic, this paper will attempt to extract points and examples that both engage the reader and arm them with the knowledge necessary to understand the issue at hand and to play an active role in their own security as it pertains to botnets.

2 To the Community

I first heard the word “botnet” in late 2015, when listening to a podcast simply for the purpose of keeping me awake during the drive home. Sheepishly I’ll admit that the cool name was responsible for my initial interest, and that if I had not stumbled across this podcast, it would have been at least another year before I encountered and understood this topic. In hindsight, both of these facts strike a little bit of fear in my heart— I, a Computer Science major since 2013, had operated blissfully unaware of these nasty things called “botnets” lurking about the internet for years. Which brings me to the main premise and motivation of writing this paper: knowledge is power, and ignorance is unaffordably dangerous. I harbor the fear that, as a society, a vast majority of us use technology without a basic understanding of how it works, and therefore are susceptible to the major risks associated with it.

Although this fear extends far beyond the concept of botnets, knowledge of botnets was what opened my eyes to the deeply-rooted problems with computer security today, and the idea that if we don’t learn protect ourselves, no one else will do it for us. It is my hope that this paper will spark interest and concern in readers, spreading an appetite for information amongst those who the future of computer security relies on.

2 Introduction

2.1 What's a Botnet?

The word "botnet" is, in and of itself, an ominous one. A portmanteau of the words "robot" and "network," it implies a collection of nonhuman robots under the complete control of one source, unquestioningly carrying out the potentially unsavory bidding of their controller.[1] This intuition is not far from the truth of the matter— a botnet is a collection of computers, capable of communication amongst one another and with other computers, with a common controlling source that dictates the actions of said computers. Botnets are comprised of computers whose users are usually unaware of their participation in a botnet, as membership to a botnet is triggered by software spread to computers potentially without the owner's knowledge.[2] Botnets are widely variable in their size and purpose, and their power is derived from their distributed nature and huge computing power originating from the sheer number of distinct machines participating.[2]

2.2 Botnet Applications

Historically, botnets have been used to send email spam, carry out distributed denial of service attacks, and steal personal information such as bank accounts, credit card numbers, and passwords.[3] Researchers have even harnessed the power of botnets to collect data on how people use the internet and to defend Internet of Things devices by changing weak passwords.[4, 5] The applications of botnets are wide and constantly being expanded, which is one of the reasons they still pose a significant threat to computer security over fifteen years after the first botnet was used with malicious intent.[6]

2.3 Creation and Usage

It is important to note that there are big differences between *creating* and *using* a botnet. Creation of a botnet itself, while less than savory, is significantly less harmful than the attacks perpetrated using botnets.

2.3.1 Creation: Client Server Model

Botnet creation commonly involves establishing an infrastructure of computers/devices, called bots, that communicate with and execute commands given by a central source, which may be one or more computers.[7] This means writing or, more commonly, modifying already existent bot software that has the ability to receive, respond to, and carry out commands coming the server in command.[8] Bot software must also be able to propagate once deployed to an initial host, using one or more of many different methods to spread to other hosts in order to create more bots.[7] Different, but related, software must also be developed to control the network of bots from the centralized source.[8]

This kind of botnet, as outlined, has a central source of control, often referred to as the C&C server, for “Command and Control.” This design is an example of the client-server model: many clients (the bots) operate based off information that can be provided only by the C&C server.[7] This is considered to be a major weakness for this botnet model— if the C&C server is discovered and disabled, the entire botnet is rendered useless due to a lack of commands to carry out.[7]

2.3.2 Creation: P2P and Decentralized C&C

As an alternative to a botnet design that follows the client-server model, many botnets use peer-to-peer networking, or P2P for short.[9] In P2P networking, rather than a server being the only source of information for clients, each client acts as both a client using information and a server capable of sending information to other peers in the network.[10] In the case of botnets, this means that, once a command is introduced to one bot, the command can be sent bot-to-bot until propagated through the entire system. As a result of this, botnets that use P2P have no central C&C server, and direct access to a subset of bots or even a single can be used to control the entire botnet, albeit less quickly than with the Client-Server model.[11] This makes dismantling a P2P botnet much more complex than tracking down and destroying one centralized source of control.[11]

In addition to P2P networking, other strategies can be used to decentralize control of a botnet and make it harder to dismantle.[1] One example is botnets that use the client-server model, with the added twist that servers are simply spread out geographically rather than being in one location.[1] Having servers spread across vast distances increases the difficulty of having enough cooperation to shut down all C&C servers at once.[1] Shutting down only some of the C&C servers, while potentially crippling the botnet, is only a temporary fix until other servers can be put online.

2.3.3 When a Computer isn’t a Computer

When talking about the bots that make up a botnet, the term “computer” has been thrown around, which simplifies an important detail about botnets. *Technically*, this is an accurate term for what a bot is, yet the definition of what constitutes a computer is much broader than(but still include) laptops, desktop computers, and servers. Phones, tablets, gaming systems, and almost any other internet-connected device has the potential to be used as a bot. In today’s Internet of Things world, this could include cameras, TVs, smart watches, Blu-Ray players, or even smart thermostats.[12] The possibilities are endless and ever-growing.

2.3.4 Usage

Botnet use involves putting the focusing the aforementioned infrastructure on some sort of goal to be accomplished. Botnets may be designed with a specific type of goal in mind, but ultimately what the botnet accomplishes depends on what commands are sent to the bots. For example, a botnet could be designed with the general intent of executing DDoS attacks, but could then be used to perpetrate separate DDoS events

against different targets, as specified by the herder.[13] The same concept applies to botnets designed for other purposes.[13]

This separation of botnet creation from botnet use creates some interesting secondary properties of botnets in practice. The person or group that created a botnet may not be the one actually using the botnet, and control of a botnet may change hands one or several times during its lifetime.[13] In fact, botnets can easily be rented and put to use for whatever purpose the buyer sees fit.[12] This means that controlling a botnet does not necessarily require technical know-how, but instead is open to anyone with money and a target in mind.[12,14] Botnets are not just a complicated tool that we only have to worry about being used by experts with extensive technical knowledge. They are an accessible, real threat that could be used by any entity that wishes harm on someone else.

2.3.5 Addendum

The above discussion of the creation and use of botnets is a very generalized and simplified overview of the topics at hand. Countless different variations of botnets exist, taking advantage of a huge number of creative solutions and workarounds on many different levels to increase their difficulty to dismantle and their effectiveness at carrying out crime. Listing *all* of the possible modifications made to the structure of botnets would be impossible, not to mention distracting from the goal of attaining an overview of the general concept in order to understand the scale of the security threat at hand. Sections 3 and 4, which examine notable botnet instances more in depth, do contain more detail on how and why certain botnets have deviated from the most general implementation discussed above.

3 Botnets in Practice

3.1 Pretty Park and Sub7

The Pretty Park and Sub7 botnets are notable mostly because they are the two earliest botnets known to exist, paving the road for all future botnets.[6] The two have several commonalities: both are named after the malware that infected hosts to turn them into bots, are examples of botnets with a central C&C server, and came into existence in 1999.[6] Pretty Park was a worm that spread through email attachments and was capable of stealing information from the host computer, such as instant messaging login names, passwords, and telephone numbers.[15] Interestingly, if Pretty Park encountered errors while attempting to install, it would display the "3D Pipes" screensaver on the host.[15] Sub7 was a trojan that, in addition to stealing information through the use of key logging on infected computers, could collect audio and video if the host had a microphone and/or video recording hardware, and bizarrely would also repeatedly open and close the computer's disk drive.[16,17] Although Sub7 in its original form has been eradicated, computers today are still sometimes infected by its distant descendants.[18]

3.2 Carna

A departure from the typical blatantly-criminal botnets most widely seen, the Carna botnet was established and used to perform what's now known as the "Internet Census of 2012." [19] Although it's still unknown who designed and deployed the Carna botnet, the creator released a report detailing the purpose of the botnet and how it worked. [20] The Carna botnet worked by gaining access to internet routers whose admin accounts were either unsecured or secured with one of a short list of default passwords. [21] It then used the routers to scan for other online IPv4 addresses that could be spread to and/or be recorded as in use or online at a certain time. [20] The botnet did not us a central C&C server, and data was periodically downloaded and saved to a server that was secured against most access from the internet. [20]

The result of the Carna botnet was new data on the general state of the internet at the time and general security trends of massive amounts of routers. The census revealed that hundreds of thousands of routers lacked even the most basic security, in the form of a password other than the factory default.[19] The census also showed that, out of all 3.4 billion possible IPv4 addresses, only 1.3 billion showed any signs of usage. [20] From the collected data, geographical and time-based maps of internet usage were also compiled. [20]

Although evidence points to the benign nature of the Carna botnet, its creation and usage was still illegal. Using passwords to actually gain access to a device without the owner's knowledge is illegal, even though the author may have abided by their claim of performing their project in the "least invasive way possible and with the maximum respect to the privacy of the regular device users." [20] This botnet brings up the question of whether botnets are inherently bad, or if the possibility of use for good makes them

potentially neutral or even good. I will not suggest an absolute answer to this tricky question, but instead provide an observation: during research for this paper, I put significant energy into hunting down evidence of true botnets being used for good purposes and found almost none. I saw both *suggestions* of good uses for botnets and the mislabeling of distributed computing clusters as botnets in order to provide false evidence of botnets being put to use for good.[21] Besides Carna, I could not find believable evidence of botnets actually being used to produce completely non-malicious results, despite finding incredible volumes of evidence for botnets being used with malicious intent.

3.3 Mirai

Rising to notoriety in late 2016, the Mirai botnet is known for carrying out a number of DDoS attacks much larger than any others previously recorded.[22,24] As a result of one of these DDoS attacks targeting the DNS provider Dyn, access to online services such as GitHub, Reddit, and Spotify (just to name a few) was cut off for the better part of a day in several parts of the US.[23] One of Mirai's most notable features it the type of bot that it uses: the malware that creates Mirai bots specifically targets Internet of Things devices. Not only that, but it spreads aggressively, using port scanning to discover telnet and SSH services whose passwords and usernames can be brute forced, and exploiting security weaknesses such as hard-coded passwords on other devices.[24] In addition, the Mirai botnet uses what's been called "Fragmented C&C," making impossible to take down the botnet by removing a single command server.[25] Essentially this means that what's called *the* Mirai botnet is actually several botnets, each being a subset of IoT devices with a distinct C&C server.[25] These Mirai fragments can be used alone to perpetrate smaller scale attacks, or together for combined power in larger attacks.[26]

The worst part, perhaps, of the Mirai Botnet's success at hijacking IoT devices and launching destructive DDoS attacks was the fact that the risk of such an event occurring was known, and malware source code for the botnet had been published weeks before the Dyn attack.[23, 27] This shows that, although the threat was at least somewhat known and possible preventative measures had been suggested (amongst them recalling vulnerable IoT devices and diversifying DNS providers), the threat of Mirai was willfully ignored, underestimated, or some combination of the two.[28, 23] This failure to adequately prepare for the possibility of such a large-scale attack and the revelation that poor security in IoT devices has significant, tangible consequences have raised concerns that continued massive DDoS attacks lurk in the future and that we are not sufficiently attempting to prevent them.

4 Action Items

4.1 To Organizations

This pertains mostly to organizations that have significant online presences, therefore being susceptible to both infection by botnet malware and to being a target for a botnet attack. In my opinion, the first item of action for organizations is to acknowledge the severity of the threat that botnets pose and to take it seriously. Simply going through the motions to placate angry customers or to preserve profit with a bandaid isn't good enough; some sort of institutional knowledge and systematic implementation of security across multiple levels in necessary. Otherwise, organizations risk falling behind the innovation of those attempting to use botnets to harm them.

First and foremost, organizations, no matter their size, must require basic security from their employees and the internet-connected devices that they interact with: strong passwords, robust spam filtering for work email, scanning of files downloaded to work computers, and basic security training for employees should all be non-optional.
Of course, people are lazy and unpredictable, meaning that these defenses will only prevent basic, simplistic attacks that aim to use a company's devices in a botnet.

Beyond that, organizations need to have strategies in place to catch attempts at turning their devices into bots, to make sure their product, if it includes software, has security measures included, and to make sure that they can respond to and function when the target of a botnet attack. These strategies are multi-tiered and could fill many more pages on their own. The Mirai botnet in particular points to several things that companies need to begin action on, and other botnet attacks on companies provide other lessons to learn from. These considerations include, but aren't limited to: implementing more robust DDoS detection and defense, having backups ready for important resources such as DNS, and deploying patches and recalls incredibly quickly after security shortcomings are uncovered.

4.2 To Individuals

The most important lesson to glean from this paper on botnets is that it's extremely important for individuals to make sure that *all* of their devices are properly secured. No device is too small to justify a lack of caution when it comes to security measures. This includes having strong passwords and encryption on sensitive information stored digitally. Common sense when connected to the internet about what sources seem reputable to download or execute programs from and observations about anything that seems out of the ordinary can go a long way. While a single individual most likely won't take down a botnet on their own, the more devices that are properly secured and unavailable for use in botnets, the less powerful botnets have the potential to be.
As individuals, it's unlikely that we can stop the onslaught of attackers with botnets at their disposal, the rise of internet-connected devices that provide more and more botnet

fodder, or the companies' policies that drive production of insecure devices. We do, however, have vast amounts of control over our own belongings and our personal habits when it comes to security. Individuals have at their disposal more information than ever before, and should take full advantage of this fact to stay up-to-date on security trends that affect them, enabling them protect themselves on some level.

5 Conclusion

In conclusion: the topic of botnets is a vast one, with many applications and ramifications that are always changing. It is, however, fascinating for these very same reasons. The concept of botnets, and their use for committing crimes, is not going away any time soon. The possibilities for usage, profit, and research on them is far from exhausted. I lean towards believing that botnets are here to stay, as the task of completely eradicating them seems complex far beyond feasibility. Thus, we must learn to live with them, gaining as much knowledge and power against them as possible in the hope of maintaining some sense of order, safety, and security among the growing ranks of internet connected devices.

6 References

1. Anonymous. "Internet Census 2012." Internet Census 2012. 2012. Web. 14 Dec. 2016.
2. "Booters, Stressers and DDoSers." Incapsula.com. Imperva Capsula. Web. 13 Dec. 2016.
3. "Botnet Command and Control Techniques." Botnet Command and Control Techniques. ScienceDirect, 2007. Web. 14 Dec. 2016.
4. "Botnets." F-Secure Labs. Web. 14 Dec. 2016.
5. Bradley, Tony. "Sub7 / Backdoor-G RAT." Lifewire. 7 Feb. 2016. Web. 14 Dec. 2016.
6. Bradley, Tony. "Sub7 Trojan / Backdoor." Lifewire. Web. 20 Oct. 2016.
7. Clinton August 22, 2013, Nate. "Can Illegal Networks of Zombie Computers Be a Force For... Good?" Cooper. 22 Aug. 2013. Web. 14 Dec. 2016.
8. Cobb, Stephen. "Botnet Malware: What It Is and How to Fight It." WeLiveSecurity. 24 Oct. 2014. Web. 13 Dec. 2016.
9. Dobbins, Roland. "Mirai IoT Botnet Description and DDoS Attack Mitigation." Arbor Threat Intelligence. 28 Oct. 2016. Web. 12 Dec. 2016.
10. Ducklin, Paul. "Researcher Uses Botnet to Map Internet." Naked Security. Sophos Ltd., 20 Mar. 2013. Web. 14 Dec. 2016.
11. Ferguson, Rik. The Botnet Chronicals. White Paper. Trendmicro, Nov. 2010. Web. 12 Dec. 2016.
12. Fox-Brewster, Thomas. "Hackers Sell $7,500 IoT Cannon To Bring Down The Web Again." Forbes. Forbes Magazine, 23 Oct. 2016. Web. 13 Dec. 2016.
13. Gallagher, Sean. "How One Rent-a-botnet Army of Cameras, DVRs Caused Internet Chaos." Ars Technica. 25 Oct. 2016. Web. 12 Dec. 2016.
14. Holbrook, Kevin P. "Mirai and the Botnet – Is There Really Anything to Fear?" Momenta Partners. 8 Nov. 2016. Web. 12 Dec. 2016.
15. Kassner, Michael. "10 Answers to Your Questions about Botnets." TechRepublic. 22 Dec. 2008. Web. 13 Dec. 2016.
16. Krebs, Brian. "Krebs on Security." Krebs on Security RSS. 1 Oct. 2016. Web. 13 Dec. 2016.

17. Krebs, Brian. "KrebsOnSecurity Hit With Record DDoS." Krebs on Security. 21 Sept. 2016. Web. 13 Dec. 2016.
18. Mullis, Simon. "Cybercriminal Intent: How to Build Your Own Botnet in Less Than 15 Minutes « Executive Perspective." FireEye. 02 Aug. 2013. Web. 13 Dec. 2016.
19. Newman, Lily H. "What We Know About Friday's Massive East Coast Internet Outage." Wired. 21 Oct. 2016. Web. 14 Dec. 2016.
20. Nixon, Allison, John Costello, and Zach Wikholm. "An After-Action Analysis of the Mirai Botnet Attacks on Dyn." Flashpoint. 29 Nov. 2016. Web. 14 Dec. 2016.
21. Padgett, Kelsey, Dina Temple-Raston, and Andy Mills. "Darkode." Audio blog post. Radiolab. 21 Sept. 2015. Web. 12 Dec. 2016.
22. Posey, Brien. "Understanding the Differences between Client/server and Peer-to-peer Networks." TechRepublic. 08 June 2007. Web. 13 Dec. 2016.
23. "PrettyPark Threat Description." F-Secure Labs. Web. 14 Dec. 2016.
24. Rashid, Fahmida Y. "Malware Increasingly Using P2P for C&C Functions." SecurityWeek. 6 June 2013. Web. 14 Dec. 2016.
25. Stöcker, Christian. "Mapping the Internet: A Hacker's Secret Internet Census." Spiegel Online. Web. 13 Dec. 2016.
26. Symantec Security Response. "Mirai: What You Need to Know about the Botnet behind Recent Major DDoS Attacks." Symantec. 27 Oct. 2016. Web. 14 Dec. 2016.
27. Vijayan, Jai. "'Do Gooder Worm' Changes Default Passwords In Vulnerable IoT Devices." DARKReading. 31 Oct. 2016. Web. 13 Dec. 2016.
28. "Virus Encyclopedia: Sub7." Panda Security. Web. 14 Dec. 2016.