An analysis of the evolution of botnets

Cole Stephan
cstephan@iastate.edu
An analysis of the evolution of botnet malware

by

Cole Stephan

A creative component submitted to the graduate faculty
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Information Assurance

Program of Study Committee:
Doug Jacobson, Major Professor

Iowa State University
Ames, Iowa

2019

Copyright © Cole Stephan, 2019. All rights reserved.
TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION .............................................. 1

CHAPTER 2. A HISTORY OF BOTNETS ................................. 2

CHAPTER 3. OPERATION OF BOTNETS ................................. 6
  3.0.1 Botnet Infection and Formation ............................. 6
  3.1 Botnet Communication Methods .............................. 7
    3.1.1 Centralized ................................................. 7
  3.2 Advanced Detection Avoidance Methods ...................... 8

CHAPTER 4. IMPACT OF BOTNETS ................................. 9

CHAPTER 5. POTENTIAL FUTURE OF BOTNETS .................. 10

CHAPTER 6. CONCLUSION ............................................. 12

BIBLIOGRAPHY .......................................................... 13
CHAPTER 1. INTRODUCTION

Botnets are a threat to the Internet as a whole and every machine is a potential target, ranging from smart home devices such as baby monitors to national power grids. With every passing year the number of Internet connected devices grows, and so too does the number of potential targets. With the number of devices that are controlled by botnets, malicious actors can use them to contract out to other hackers or use them for their own means. This report is an analysis of the development of botnets from their inception to 2019, how they operate, the risks that they pose to individuals and nations, and how they may develop going into the future.
CHAPTER 2. A HISTORY OF BOTNETS

Note: It should be noted that due to the sheer number of botnets in existence, this history will attempt to cover only the more notable and more known botnets in detail, and less of their derivatives and various iterations except when necessary. Even so, some larger botnets that have had an impact on the internet are not covered as they do not mark a significant change in technical capabilities compared to previously discussed botnets or have made similar impacts as other mentioned botnets.

As the fundamental characteristics of a botnet are shared with other pieces of malware such as worms and trojan horses, it is worth mentioning the original famous piece of malware named the Morris Worm. Created by university student Robert Morris, and let loose on the early Internet in November, 1988, the Morris Worm was reported to have infected 6,000 UNIX machines, which accounted for roughly ten percent of the Internet at that time. Originally designed to target and exploit insecure UNIX machines to spread awareness of the dangers of lack security, it had the unintended side effect of infecting machines multiple times and slowing them down enough to be practically unusable until disinfected. The spread of the worm caused monetary losses guessed to be at least $100,000 as machines and networks were taken offline to be fixed, as well as prompting the creation of the Computer Emergency Response Team (CERT) Coordination Center, which is dedicated to research and counter cyber threats to the Internet.

It wasn't until a decade later that the first pieces of malware that used IRC channel
communication for commands began to become widespread. Sub7 is a famous example of a trojan virus that used IRC to communicate to the attacker. Spread through infected software, Sub7 would install a backdoor into the target computer once run that opened an IRC channel to the attacker to notify them of the target infection. From there, the hacker could access files, steal credentials, add additional malicious code, or whatever else the attacker wished to do with the privilege they gained on the machine.

Pretty Park is another example of malware from that time that used IRC for commands. As a worm, the virus would self-propagate via email by attaching a malicious .exe file to the body of the mail it sent. Once a user would execute the file, it would install itself on the host system, hide itself by modifying registry files and hiding its process from the task list, install a backdoor, and run two internet applications. The first application would be to attempt to connect to an IRC channel that would allow the malicious actor to monitor infected devices. The second application scanned email address books on the victim, and sent further infected emails to anyone on the list to propagate itself further. These two examples of early malware would be precursors to more advanced botnet technology.

One of the first botnets that became publicly noticed was a botnet used to send phishing emails to users of Earthlink, an Internet service provider that also offers services such as email and web hosting. The author of the virus stole an estimated $3 million from stolen credit cards and other financial information, and managed to send 1.25 billion phishing emails within a year, which accounted for over 25% of the total emails worldwide sent by 2001. The financial impact to the company was estimated to be around $4.1 million. This showed the potential gains for hackers that successfully exploited botnets, as well as the damage they could do to companies and individuals.

By the mid 2000s botnets began to grow more advanced in multiple aspects, such as
developing peer to peer (P2P) communication abilities and advanced stealth techniques, as well as widening their scope of attack. The Zeus botnet is a prime example of these advancements. First detected in July 2007 and spreading quickly from there, the Zeus botnet was mainly used to steal credentials and financial information, but also has the capability to run arbitrary code on infected machines as well as being used to install ransomware. Further developments of the virus, such as Gameover Zeus, a version that uses encrypted P2P for communication between nodes and command and control servers, have further developed its capabilities. To date, Zeus and its derivatives have caused estimated losses in the hundreds of millions for businesses across the world.

The mid 2000s also saw a rise in a number of botnets dedicated to botnets spread through email spam. The Grum, Storm, and Cutwail botnets alone made up a majority of spam emails sent from 2007-2010. Researchers also saw new techniques being used in botnets like Storm, such as the central CC server being replaced by a P2P model, and remote control servers being hidden by ever changing IP addresses, making tracking and dismantling the botnet much more difficult. As botnets began to grow in size, they also began to see use in Distributed denial-of-service attacks (DDOS), meant to limit or stop access to web services by overwhelming the target with requests, rendering them incapable of actual communication.

With the rise of online advertising in the past decade, with 2019 looking to have spending on digital advertising surpassing that of traditional methods[9], hackers began to use botnets to commit ad fraud. Ad fraud is when either human or non-human actors click on or otherwise interact with advertisements in order to gain malicious actors money from advertisers without actually intending to purchase or genuinely interact with the advertised business or product. Advanced botnets such as Methbot have developed techniques to mimic human interaction with advertisements to avoid detection from ad providers, and
are estimated to cause losses to advertisers at a minimum of $3 million dollars a day just from Methbot alone[11]. With the continual rise of online advertising revenue, it is likely that botnets will continue to take advantage of this trend. Other botnets have begun using victims resources in order to mine cryptocurrency. The Smominru botnet is estimated to make thousands of dollars a week from using bots they have accumulated to mine various cryptocurrencies.

With the rise of the Internet of Things (IoT) in recent years, the number of devices connected to the Internet has skyrocketed, with an estimated addition of 1.1 billion new devices in 2018 alone[10]. Many of these devices are inherently insecure, with default credentials or unpatchable vulnerabilities, making them easy targets for botnets. The Mirai botnet that was behind the massive attack on Dyn in 2016 was a botnet built with IoT devices, and is estimated to have had 600,000 bots at its peak, and was able to DDOS Dyn with a peak rate of 1.2 Tbps.
CHAPTER 3. OPERATION OF BOTNETS

3.0.1 Botnet Infection and Formation

Botnets are formed by the same methods used by other pieces of malware, such as malicious email files, malicious websites and downloads, social engineering, or any other traditional method of infection. After initial infection, the operation of the new bot differs between different pieces of malware. Most bots will attempt to hide themselves on their new host machine through different methods. Depending on the infection, the bot may be able to install a rootkit (or was installed by a rootkit), granting further access and granting a greater ability to hide. Or a bot may hide by naming its files and processes similar or the same as system processes. Once hidden, a bot may then download additional files or start or kill processes to further the infection or protect itself, as well as setup communication to the CC server. From there, the bot will wait for commands while attempting to spread itself further to other devices on its network. This process then repeats with every new victim that is infected. Internet of Things devices are particularly vulnerable to this as many have default credentials to login to administrator accounts on devices and are unpatchable.

An advanced botnet such as Mirai serves as a good example to show how a botnet operates during initial infection. Understanding the Mirai Botnet by Antonakakis et al.[2] gives a good explanation of this process. After finding a potential victim, Mirai attempts to brute force a Telnet connection. If it is successful, the victim IP and credentials are sent to a report server. Next a loader analyzes the victim system to determine what kind of system it is infecting and then proceeds to download malware specific to that environment. To hide itself, the infection will delete the downloaded software after it begins to run, and makes
detecting its processes more difficult by naming them pseudorandomly. It will also kill any other processes bound to ports 22 or 23, which may include previous malware. Finally, the bot will wait for commands from the CC server, as well as scanning the network for further victims.

3.1 Botnet Communication Methods

3.1.1 Centralized

Botnets often use a centralized command and control server(s) to send commands to the network. This setup is popular because it is relatively simple to setup and manage, and common protocols such as IRC or HTTP can be used to issue commands. This helps guarantee command delivery and limits communication complexity. However, having a single or few central command servers create issues for attackers. First, large amounts of traffic are directed to the CC servers and make it much easier to detect and take down, which can allow law enforcement to quickly take down the botnet once they find the server. As well as making the CC server more easily detectable, it allows victims to more easily discover that theyre infected when they see that their machine is sending traffic to a known CC server.

3.1.1.1 Peer to Peer

More sophisticated botnets may use Peer to Peer (p2p) communication to send commands. This method protects the botnet from the vulnerabilities of a centralized command setup, as removing a single node in the network wont take down the entire network. However, this adds complexity to the botnet, which is a double edged sword for attackers, as increased complexity makes creating the malware harder and more prone to message send failures, but increasing the difficulty for law enforcement and researchers to take down and track the network.
3.2 Advanced Detection Avoidance Methods

More sophisticated malware may use a variety of advanced methods to obfuscate their processes and traffic and make it hard to find the bots as well as the CC servers. As previously mentioned, the Mirai botnet and others may obfuscate their running process names to hide from host system detection, or they may be used in conjunction with rootkits to get further system access to hide. P2P traffic can make it harder to track down a network of bots, however the hosts stay consistent. More advanced botnets may use methods such as domain fluxing or IP fluxing[3]. These methods involve a constantly changing IP address or domain name of the CC server, making blacklisting and tracking the servers very difficult. Domain names that are used may even be randomly generated in order to avoid lists of domains that may be discovered over time[4].
CHAPTER 4. IMPACT OF BOTNETS

The spread of botnets and their use has had an effect across many industries around the world. Botnets are commonly known to be used for massive DDOS attacks on different targets ranging from individual websites to key internet infrastructure. These attacks can take targets offline for hours, if not for days depending on the targets ability to stop the attacks and the attackers goals. One of the largest DDOS attacks in recent years was the attack on Dyn in 2016[5], in which the Mirai botnet attacked the DNS provider, disrupting traffic to a large portion of the internet, including large websites like Github, Paypal, Amazon, and others. Disruptions for large businesses such as these can cause millions of dollars of lost revenue in a short amount of time.

The major target of botnets, well beyond DDOS attacks, is financial services and online stores, according to Kasperskys 2018 report on botnet activity[4]. Botnets such as ZeuS target the finances of victims, stealing login credentials or other information that will allow them to steal from their targets, or the bots install ransomware to hold system hostage until the victim pays the attacker to unlock their systems. In 2013, it was estimated that Cryptolocker ransoms earned malicious actors over over $27 million[6], showing the potential amount of money that can be earned from operating a botnet.
CHAPTER 5. POTENTIAL FUTURE OF BOTNETS

With the massive growth of IoT devices, it is likely that botnets that target such devices will grow larger and larger attacks to become more commonplace. A similar growth in SCADA devices, which are used in industrial settings for cyber-physical control and will pave the way for smarter industry and smart cities, may also present a similar target to botnets. As SCADA devices control real world machines, hackers will be able to physically alter their behavior. Such an attack has already happened in 2010 with Stuxnet, a worm designed to damage uranium enrichment equipment. Similar attacks may become more commonplace as industrial control networks become more infiltrated and attackers (likely nation-state actors) find use in attacking in such a way.

Botnets are also appearing to use new techniques to better adapt to attempted take-downs, attacker privacy, and automation. Automation of certain functions, like programming bots to act as a swarm, giving the bot a rudimentary intelligence and allowing it to react to different situations, such as tampering and delivering different payloads without direct intervention from humans. Blockchain technology is also being researched as a possible avenue to replace traditional CC servers. Blockchain offers anonymity to the controller, and removes the risk of tampering by non-botnet owners and CC server take-downs.

Online advertising spending also continues to grow every year, and it is likely that botnets will continue to generate fraudulent activity to gain large amounts of money from ad platforms. Cryptocurrency also continues to grow in value, so it is likely that more
botnets will be used to mine them in order to gain attackers money.
CHAPTER 6. CONCLUSION

Botnets have been around in some form or another for at least two decades now, and look to only continue to grow, not only in size but also complexity. Starting from simple IRC channels and email, to developing automation and using the latest computer techniques, botnets have adapted and grown in many ways since their inception. Major botnets and their hundreds of variations look as if they will continue to plague the Internet for the foreseeable future, despite the efforts of researchers and law enforcement. The arms race between better security systems and better botnets will see more advanced malware making its way on the Internet, becoming harder to track and takedown.
BIBLIOGRAPHY


