HACKTIVISM AND DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS - POLITICALLY CHARGED CYBERCRIME

Kyle Sershon CRJS310_28844

Executive Summary

- Hacktivism is on the rise due to rising political tensions over the past decade.
- Unlike hacking done for monetary gain, hacktivists are motivated by social and political ideology.
- Hacktivist attacks may have different motivations, but still lead to large monetary losses.
- DDoS attacks against business and government infrastructure can incur high costs and create prolonged downtime of websites.

Introduction

Many types of cybercrime occur in society, and motives can vary for each crime. A hacker can be motivated by financial gain, revenge, curiosity, or boredom; this list is not all-inclusive. Hacktivism focuses on a specific type of cybercrime in which an attacker commits a crime based on political ideology. It is important not to blur the line between cyber warfare or cyber terrorism, which includes state-sponsored actors, and hacktivism. Many politically charged hacktivists unite to disrupt and damage companies, the government, and society. What makes Hacktivism different from financially motivated crimes or crimes of revenge is that the offender commits the crime, appealing to what they deem morally right. For instance, someone who associates with the far left may specifically target the republican administration to sabotage their agendas. Attacks are not limited to government agencies. Non-profits, publicly traded companies, and individuals can be hacktivism targets. Society and politics have never been more polarized in recent modern history. Hacktivism is not just about specific policies in the government; the choices companies and organizations make can also make them susceptible targets. Politics within a company, such as removing DEI policies or mass profits gained at its customers' or employees' expense, or catering to unfavored factions and groups in society, can easily become candidates for one of these groups. In 2022, the hacktivist group Anonymous

attacked Epik, a domain hosting company based in Seattle, Washington, which hosted multiple far-right websites. Anonymous stole data in a breach, which was later leaked to the world. The data stolen included Passwords, Names, and other PII of its customers, which allowed other hacktivists to dox individuals associated with the company and sites they hosted. Epik hosted websites that related to QAnon conspiracies and briefly hosted the Neo-Nazi "Daily Stormer" and other far-right ideological websites. This is only one of many attacks done by hacktivists, but it demonstrates that everyone can ultimately be the target of a costly attack.

Distributed Denial of Service (DDOS)

Remember that the motive of a hacktivist is not typically personal gain, but to disrupt and cause as much chaos as possible against their targets. That is why some of the most frequently performed hacktivist attacks include DDoS. A Distributed Denial of Service (DDoS) attack is performed by multiple compromised systems to flood a specific target with traffic with the goal of disrupting its service. An example in the figure below shows traffic related to a political party that was the target of a massive DDoS attack on October 29th , 2024, that lasted nearly 4 hours and left the government campaign site unavailable. This attack was just a few days before the national election in the United States. During the attack, the website was flooded with multiple requests to load its webpage. It peaked at about 206,000 requests per second, totaling nearly 2 billion requests in 4 hours. To show

just how significant this attack was, Analytics.usa.gov shows that currently, NIST.gov has had 7.4 million sessions for 40 days.

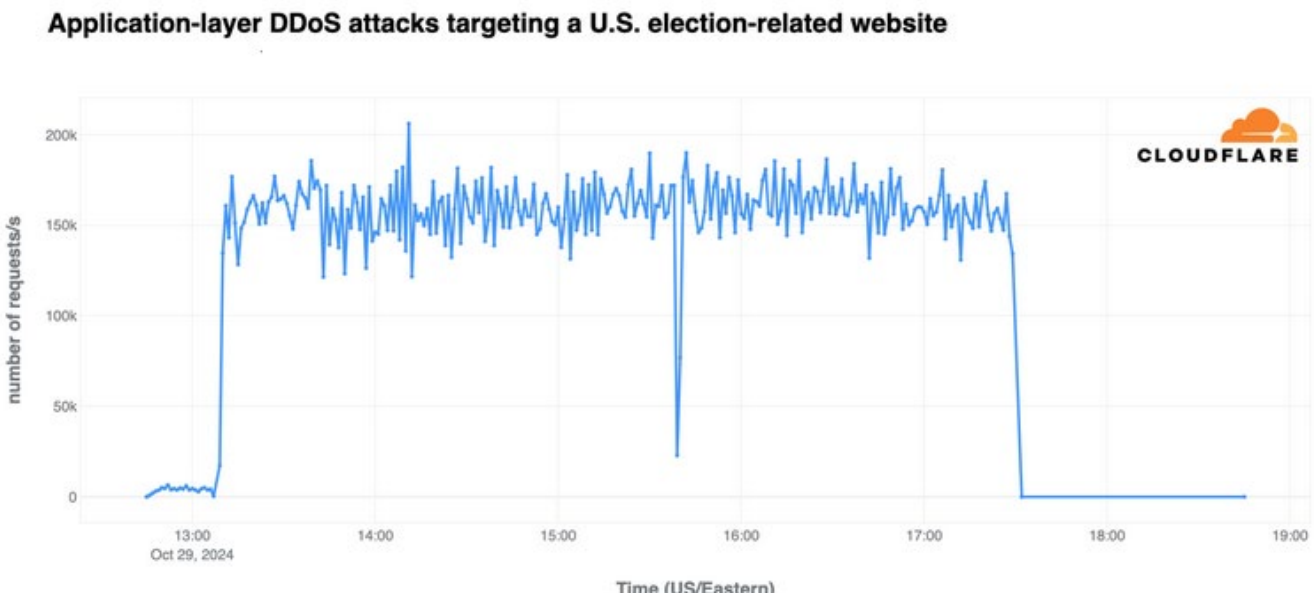

Figure 1 : blog.cloudflare.com (Woolbright & Tomé, 2024)

This type of attack cripples' webservers and leave the site unreachable by legitimate users. Like other general cyberattacks, DDoS attacks have increased over the past year. In the 1st half of 2024, Cloudflare is estimated to mitigate nearly 8.5 million DDoS attacks. These attacks are also costly, with an average cost of roughly $6,000 per minute, depending on the scale of the attack. In today's world, Internet of Things (IoT) devices and the evolution of AI have been used to amplify attacks.

DDoS architecture consists of some key elements. The attacker, the Botnet, and the Target. The attacker will be the person or device carrying out the assault, and the target is the recipient of the attack. "A botnet is essentially a network of compromised internet-connected devices, controlled by the attacker. These devices, often unknown to their legitimate users, become tools in generating massive volumes of attack traffic. The

distributed nature of botnets makes it challenging to trace and neutralize them, as they can comprise devices from all around the globe." (Vinay Tila Patil) The image depicts a top level view of DDoS attack architecture.

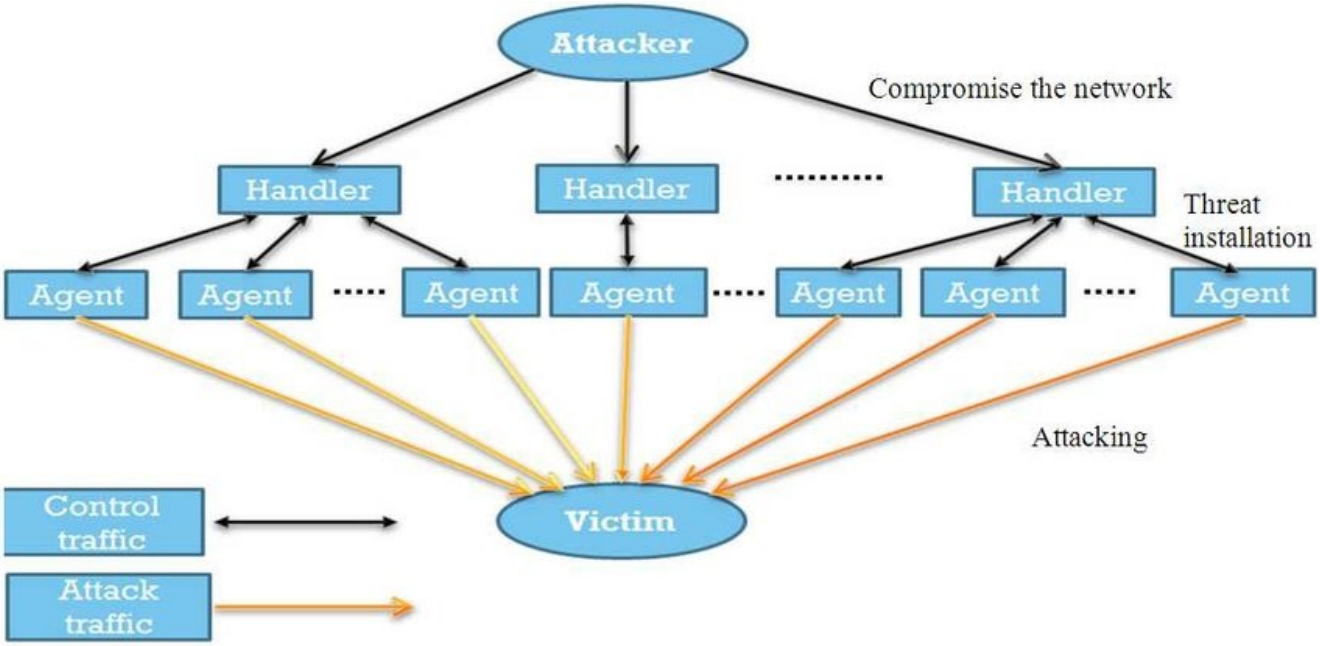

Figure 2 : Architecture of Distributed Denial of Service (DDoS) attack (Bhaya & Manna, 2014)

The volume of DDoS attacks is constantly growing and remains one of the largest threats in cybersecurity. The Information Commissioner's Office in the UK reported, "DDoS attacks accounted for 25% of all hacking incidents reported to the FCA". Hacktivists can use DDoS attacks to disrupt government websites, interrupt IoT devices like polling stations during elections, and interrupt access to government resources such as voter registration pages. It is essential to understand that public-facing sites should be heavily armored against these attacks. Disruptions to services can reduce legitimate web traffic, which disrupts organizational procedures and customer interaction with sites.

What can be done?

It is no mystery that tensions in the current political landscape, not just in the United States but worldwide, are at an all-time high. Misinformation and Disinformation have spread like wildfire, and with most people getting their news from social media, which tends to place people in echo chambers among their political affiliation, there has been a rise in hacktivist-related attacks. DDoS attacks are widespread because they are somewhat easy to perform and can even be purchased as a service from specific malicious actors. Although addressing the current political tension is a multi-tiered problem with no finite resolution, we cannot dismiss that this polarity has driven many people to lash out at opposing factions. It is also essential to note that hacktivism is different from cyberterrorism. Cyber terrorism involves state-sponsored actors, while hacktivists typically act without state sponsorship and for their agenda. The motive for these crimes, perhaps, makes it extremely dangerous. As mentioned, these attacks are carried out based on ideology, and the attacker feels they are appealing to what is good for society in a somewhat vigilante manner.

As with most cyberattacks, increasing awareness is key to help mitigate DDoS attacks against infrastructure. After understanding the threat, a multilayered approach can be taken. Hiring cloud service companies to help manage your network is critical to increasing security. Many companies specializing in cloud security utilize powerful tools like AI and machine learning, which use artificial intelligence to detect when systems are under

unusual traffic and can alert administrators or help mitigate the attack while assisting in disaster recovery. AI and Machine learning can also be used to detect and stop attacks. In an article about DDoS attack detection, the Journal of Electric Systems states, "Technological advancements like AI and machine learning offer dual-edged swords, aiding both attackers and defenders." Encourage administrators to implement strong rules on WAFs (Web Application firewalls) and enable Rate limiting.

Another important aspect is to make sure the attacks are reported to officials. The IC3, a section of the FBI, allows reporting cybercrimes, including DDoS attacks. Reporting these attacks allows the FBI to investigate and identify the source of the attack, which could lead to prosecution. Hacktivism appeals to many people; it can sometimes be viewed positively, depending on who attacks it and why. Even though groups like Anonymous and others have been glorified in the media, DDoS attacks are cyber trespass and are considered cybercrime, regardless of motive.

Lastly, education, as always, is key. Employees and the public should be educated on all types of malicious attacks on the web. Teaching good cyber hygiene and how to identify when something is wrong is essential. Generally, "If you see something, say something." People need to ensure they are keeping devices up to date with the latest security patches, and practice setting up strong passwords for home networks, so devices do not get hijacked and become part of DDoS botnets. We should also inform people not to glorify or encourage these types of attacks, even if you disagree with their targets. A combined effort from government, business, and society is crucial in increasing security posture against this type of cybercrime.

Glossary

- **DDoS**- the intentional paralyzing of a computer network by flooding it with data sent simultaneously from many individual computers.
- **Hacktivist** - a person who gains unauthorized access to computer files or networks in order to further social or political ends.
- **Hacktivism** – the act of performing cybertrespass to further political or social ideology.
- **Machine Learning** - a field of artificial intelligence that focuses on enabling computers to learn from data without explicit programming
- **AI – Artificial Intelligence** – the theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.
- **Misinformation -** refers to false or inaccurate information, whether intentionally or unintentionally spread.
- **Disinformation** – Intentionally spreading false information
- **Botnet -** a network of private computers infected with malicious software and controlled as a group without the owners' knowledge
- **PII –** (Personal Identification Information) – Any information that can be used to identify a specific person, including names, addresses, phone numbers, email addresses, social security numbers, etc.

- Doxing - the action or process of searching for and publishing private or identifying information about a particular individual on the internet, typically with malicious intent.

References

Bhaya, W. S., & Manna, M. E. (2014). Review clustering mechanisms of distributed denial of service attacks. *Journal of Computer Science*, *10*(10), 2037–2046. https://doi.org/10.3844/jcssp. Figure 2 .

Simpson, J. A. (2002). *Oxford English Dictionary*. Oxford University Press.

Vinay Tila Patil. (2024). DDoS Attack Detection: Strategies, Techniques, and Future Directions. *Journal of Electrical Systems*, *20*(9s), 2030–2046. https://doi.org/10.52783/jes.4808

Woolbright, J., & Tomé, J. (2024, November 6). *Exploring Internet traffic shifts and cyber attacks during the 2024 US election*. The Cloudflare Blog. https://blog.cloudflare.com/exploring-internet-traffic-shifts-and-cyber-attacks-during-the-2024-us-election/. Figure 1.