



```
01101010010011011101010100110100100010101001110101011001010011010
1001101110100110000 10111001010110100110
000101010011101 0101100101001101
010011011101 001100001011
101011010 0110100 1000101010
101010 11 00101001101 010 0 001101
0101 0100 11010010001 01010 011101
011 0010100 1101010 0100110 1110
011 000010111 001010110 100
10010001010100111010101100101001101010010011011101001100001011100
01101001101001000101010011101010110010100110101001001101110101010
01001000101010011101010110010100110101001001101110100110000101110
10110100110100100010101001110101011001010011010100100110111010011
01011100101011010011010010001010100111010101100101001101010010011
```

Inside a Hacker's Mind

This whitepaper provides a comprehensive picture on DDoS hackers, their psyche, and motivations and offers suggestions on how to ensure DDoS protection



Table of Contents

Introduction	3
The Evolving Hacker Community	4
What motivates Hackers	4
Modus Operandi of DDoS Hackers	5
Best Practices to Mitigate DDoS Attacks:	8
Summary: Beating Hackers at their Own Game	8
References	9

Table of Figures

<i>Figure 1 – Anonymous Hackers Mask</i> _____	3
<i>Figure 2 - A Tweet by the Anonymous Group</i> _____	4
<i>Figure 3 - Another Tweet by Anonymous</i> _____	5

Index of Tables

<i>Table 1 - Cost of DDoS Services on the Dark Net</i> _____	6
--	----------



Introduction

It was in 1974 that the first DDoS attack was launched when David Dennis—a 13-year-old learned about a new command that could be run on CERL’s PLATO terminals. Called “external” or “ext,” the command could cause the terminal to lock up—requiring a shutdown and power-on to regain functionality. He tested his knowledge which forced several users to power off simultaneously. In the 45 years since its inception, this form of attack has gained the status of the most persistent and damaging of all cyber-attacks.

The next milestone in DDoS attacks occurred in August 1999, when a hacker used a tool called `Trinoo` or `Trin00`, to disable the University of Minnesota’s computer network for more than two days. Trinoo is one of the first publicly available DDoS programs and a ground-setter for other widely available DDoS tools that would emerge in the future. Using a compromised host, the attacker executes automated processes to make a list of vulnerable machines. Using this list, scripts are run to compromise those machines and convert them into Trinoo Masters or Daemons. A single Master can control several Daemons which are the compromised hosts that launch the UDP floods against the victim machine. As a final step, the DDoS attack is launched, when the attacker issues a command on the Master hosts and the Masters instruct the Daemons to start an attack against specified IP addresses.

The next significant DDoS attack milestone, also in the year 2000 occurred when Michael Calce, a 15-year-old boy who used the online name “Mafiaboy,” launched one of the first recorded DDoS attacks. Calce hacked into the computer networks of several universities. He used their servers to operate a DDoS attack that crashed several major websites, including CNN, E-Trade, eBay, and Yahoo.

Figure 1 – Anonymous Hackers Mask

By the first half of 2014, there were more than 100 events over 100GB/sec. By June of the same year, this number doubled. By this time various enterprises, mostly financial institutions, and government agencies had all experienced DDoS attacks. The attacks were increasing in complexity and size. The estimated cumulative cost was pegged at \$1.2billion.



Other DDoS Attacks over the years

- 2002 – The Domain Name System root servers were attacked, in an attempt to disrupt the entire internet
- 2007 – Politically motivated attacks by Russian nationalists against Estonia, completely disrupting its governmental operations, as the country was an early adopter of electronic government
- 2008 – The first broad-scale appearance of “Anonymous” against the Church of Scientology
- Q3 2012- to Q1 2013- Bank of America, Capital One, Chase, Citibank, PNC Bank, and Wells Fargo were attacked in retaliation for sanctions on Iran.

[Excerpts from the blog 'Yes, they are Out to Get You - And it's Going to Cost You'.](#)

The Evolving Hacker Community

The hacker community developed in tandem with technology during the 1950s and 1960s. The systems back then were slow and the technicians and programmers who maintained these cumbersome systems were considered highly intelligent specialists. Their ability to 'work-around' and 'cut across' obstacles led to them being called "Hacks". This respect led to a breed of youngsters, in most cases teenagers and men in their twenties, who began to explore these systems and engage in mischievous or outright malicious acts against other systems. Thus, up to the year 2000, there are instances of youngsters who launched DDoS attacks for juvenile reasons, and without any monetary motives attached to them.

By early 2000 the hacker community was shaped like a pyramid. The first tier consisted of highly skilled elite hackers who could create original attack tools. The second tier, a larger group had good technical skills, and used tools to suit their own needs. The third tier of hackers - script kiddies or noobs as they were known, had some computer knowledge and could use basic hacking tools.

Figure 2 - A Tweet by the Anonymous Group



By the end of 2010, the demography of DDoS attackers was shifting towards young men in their thirties who had definite motives for launching DDoS attacks. Like for example, James Robinson, who attacked the Akron Phoenix because he had grudges against the city's police force. Another example is Austin Thompson, who was the father of attacks on gaming companies. His motive was to maliciously spoil Christmas vacations. Black Hat hackers were stereotyped rebels.

By 2020, DDoS hackers became parts of hacker communities, catering to consumers who were ready to pay to participate. These hackers would commoditize DDoS attacks and would look for opportunities to cause major disruptions because of strong political, competition, or pure monetary motives. These highly skilled and focused groups of DDoS attackers are careful to mask their identities but still revel in the attention from the media. 'Anonymous' is one such group that took credit for the massive attack in June 2020 on T-Mobile, AT&T, Verizon, Sprint, and even YouTube, Fortnite, and Twitch.



What motivates Hackers

Black hat hackers have malicious motives behind their attacks. However, there are exceptions. According to Cyber Security Intelligence, a DDoS attack on TalkTalk in 2019 was launched by a bunch of teenagers purely with the motive of entertaining themselves. The recipients did not see anything funny and Cyber Security Intelligence reports: "in one day its share price fell by 12% and, in total, an estimated £360 million was wiped off its stock value. The direct one-off cost of dealing with the attack was reportedly more than £30 million."

Paras Jha, a 22-year-old computer student from Fanwood, N.J. developed Mirai with two other co-conspirators both around 22 years of age. He is supposed to have revelled in the uproar caused by his first attack. The motive was to delay classmen registration for an advanced computer science class he wanted to take.

Figure 3 - Another Tweet by Anonymous

Moving on to other not-so-funny motives, the group calling itself Anonymous mentioned earlier, launched DDoS attacks that crippled the websites of the Turkish government and financial enterprises for political reasons.



Another group called New World Hackers launched an attack on U.S. presidential candidate Donald Trump's website again motivated by political reasons.



But the one reason that never goes away is monetary motivation. Hackers motivated by greed launch attacks to steal confidential data. They often use DDoS attacks as smokescreens to distract IT even as they breach an enterprise's database. An example is the Linode attack where Linode asked its customers to reset their passwords.

[Linode's final words after the DDoS attack](#),
 "Sincere apologies are in order. As a company that hosts critical infrastructure for our customers, we are trusted with the responsibility of keeping that infrastructure online. We hope the transparency and forward-thinking in this post can regain some of that trust. We would also like to thank you for your kind words of understanding and support. Many of us had our holidays ruined by these relentless attacks, and it's a difficult thing to try and explain to our loved ones."

Cyber extortion or demanding ransom in the form of Bitcoins is now gathering momentum. The hackers demand ransom threatening data exposure or long periods of downtime. Research by MarketWatch says that nearly 24.6% of companies in the research confirm their willingness to pay hackers their ransom.

Modus Operandi of DDoS Hackers

Assembling the botnets necessary to conduct DDoS attacks can be time-consuming and difficult. However, hackers have it even easier now as DDoS attacks can be purchased in the Dark Web. Cyber criminals have developed a business model that works this way: More sophisticated cyber criminals create botnets and sell or lease them to less sophisticated cybercriminals on the dark web – that part of the Internet where criminals can buy and sell goods such as botnets and stolen credit card numbers anonymously.

The dark web is usually accessed through the Tor browser, which provides an anonymous way to search the Internet. Botnets are leased on the dark web for as little as a couple of hundred dollars. Various dark web sites sell a wide range of illegal goods, services, and stolen data. In some ways, these dark web sites operate like conventional online retailers. They may provide customer guarantees, discounts, and user ratings. It is believed that the price for one day of DDoS service ranges as follows:

Table 1 - Cost of DDoS Services on the Dark Net

Offering	Price
1-hour DDoS Service	US\$10
1-day DDoS Service	US\$30-70
1-week DDoS Service	US\$150
1-month DDoS Service	US\$1200



As with most cyberattacks, DDoS attacks are a 'when', not an 'if'. More importantly, DDoS attacks generally target all three levels of your IT infrastructure:

Layer 3 (Volumetric IP level) attacks are used to saturate bandwidth lines as well as overload L3 processing devices such as routers, filling up buffers, slowing web or service performance, and ultimately preventing website access or the ability to access services. The network layer (Layer 3) transfers packets (data sequences) from one network to another. It can be compared to a freeway where there is a sudden influx of traffic causing regular travelers to be denied a travel route to their destination.

Types of Layer 3 Attacks

- ICMP Ping (Type 8) Flood
- IP Fragmented Flood
- Malformed IP Flood

Layer 4 (Transport Protocol level) attacks that take place in the transport layer of the OSI model, rely on extremely high volumes (floods) of data to slow down web server performance, consume bandwidth and eventually degrade access for legitimate users. The Transport layer (Layer 4) controls the functionality and processes for transferring data sequences from the starting point to various destinations, without compromising the quality of transfers. It is responsible for ensuring the reliability of a given link through flow control. To summarize, Layer 4 refers to the fourth layer of the Open Systems Interconnection (OSI) Model, known as the transport layer.

Layer 4 attacks exploit weaknesses in normal protocols to exhaust the capabilities of the network leading to a denial of service. As network services work on a first come first served basis, the request is received, the computer processes the request and then goes to the next request and so forth. In a DDoS attack, the queue becomes overwhelming and there are not enough resources to handle the requests. An example of a protocol attack is a SYN flood. The SYN is the initial request by a client to open a connection, to which the server replies with a SYN-ACK. Finally, the client acknowledges and responds with an ACK which is like a 'thank you' message finalizing the TCP connection. However, during a DDoS attack, spoofed (fake source IP address) SYN requests are sent. Since the return address for these packets is fake, the SYN-ACK is delivered to the wrong address, and the ACK is never received for these requests, creating a break in the process forcing the server to expand resources waiting for the final ACK.

Types of Layer 4 Attacks



- SYN Flood
- UDP Fragmentation or UDP Garbage Flood
- ACK Flood
- Empty Connection Flood
- FIN Flood
- FIN+ACK Flag Flood
- URG Flag Flood
- ALL TCP Flags Flood
- PSH+ACK Flag Flood
- RST Flood

Layer 7 (Lower volume, higher connections, low and slow, application attacks) exploits weaknesses in the application layer, overwhelming the database or server powering the application directly. Layer 7 attacks are usually more complex and therefore harder to mitigate. Often they are of lower volume but not always.

The Application Layer (Layer 7) is the closest to the end-user and existing applications. Layer 7 mitigation defends applications and protects them from attacks using web application firewalls. Sometimes malicious requests sneak in and penetrate defenses causing massive damage which is hard to diagnose and even more difficult to mitigate. DDoS attacks on the 7th layer of the OSI model are usually used to reach the resource limits of the targeted service/application and result in a resource saturation. This eventually results in the unavailability of that resource/application to legitimate users.

Types of Layer 7 Attacks

- Brobot Flood
- SlowLoris
- DNS Request Flood
- HTTP Flood with Browser Enumeration
- HTTP GET Flood
- HTTPS Flood
- Dynamic HTTP Flood
- SSL Negotiation Flood

Best Practices to Mitigate DDoS Attacks:

- It is important to configure the DDoS mitigation solution for each service within an organization.
- Use Signature-based protections (which holds a bunch of DDoS attack identifiers, i.e. when its engine detects one, it drops it - just like the antivirus app on a PC).
- Use SYN protections with several types of challenges (RST challenge / TCP cookie-based challenge etc) on TCP based services (such as a JS challenge for HTTP).
- Use OOS protections to avoid false positives to the network services' availability.
- Use cps/requests rate limit protections on services - depending on the expected connections/requests on the relevant service



- Blacklist all recognized 'Bad IPs' - and ask the ISP to block them on their perimeter
- Increase the authentication level of your services to protect against bad bots and malicious attackers.

Summary: Beating Hackers at their Own Game

Even with the most sophisticated DDoS mitigation and testing solutions deployed, most companies are left with a staggering 48% DDoS vulnerability level. Mitigation solutions do not constantly re-configure and fine-tune their DDoS mitigation policies. Leaving their ongoing visibility limited and forcing them to troubleshoot issues at the very worst possible time, that is, when systems are brought down by a successful DDoS attack. These solutions are all reactive, reacting to an attack, and not closing DDoS vulnerabilities before an attack happens.

DDoS Red Team Testing simulates a small variety of real DDoS attack vectors in a controlled manner to validate the human response (Red Team) and procedural handling to a successful DDoS attack. Red team testing does not identify a company's vulnerability level to DDoS attacks and is usually performed on average twice a year. Red team testing is a static test done on dynamic systems. Any information gained from this testing is valid for that point in time only.

However, RADAR™, MazeBolt's new patented technology solution, simulates DDoS attacks continuously and non-disruptively. Delivering advanced intelligence, through straightforward reports on how to remediate the DDoS vulnerabilities found.

Closing the DDoS gap by assisting your mitigation solution to fix ongoing security gaps before they are exploited. Using RADAR™ you never have to rely on risky zero-day reactive mitigation capabilities.

RADAR™ assists organizations in achieving, maintaining, and verifying the continuous closing of their DDoS vulnerability gaps. Reducing and maintaining the vulnerability level from an average of 48% to under 2% ongoing.

About MazeBolt

[MazeBolt](#) is an innovation leader in cybersecurity and part of the DDoS mitigation space. Offering full DDoS risk detection and elimination and working with any mitigation system to provide end to end full coverage. Supporting organizations in avoiding downtime and closing DDoS vulnerabilities before an attack happens.'

References

<https://www.digitalattackmap.com/understanding-ddos/>



<https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf>

<https://eugene.kaspersky.com/2016/12/06/a-brief-history-of-ddos-attacks/>

<https://www.cisomag.com/ddos-attacks-rose-180-in-2019-compared-to-2018/>

<https://krebsonsecurity.com/2018/10/mirai-co-author-gets-6-months-confinement-8-6m-in-fines-for-rutgers-attacks/>

<https://portswigger.net/daily-swig/20-years-of-ddos-attacks-what-has-changed>

<https://techbeacon.com/security/anonymous-tweets-ddos-everyone-freaks-out>

<https://en.wikipedia.org/wiki/Trinoo#:~:text=Using%20Trinoo,-Step%201&text=The%20attacker%2C%20using%20a%20compromised,find%20other%20hosts%20to%20compromise.>

