

Distributed Denial of Service (DDoS) Attacks

Introduction:

In the digital age, the internet has become an integral part of our lives, powering everything from basic communication to critical infrastructure systems. However, as dependence on the internet has grown, so too have the threats that target its infrastructure. One of the most notorious and disruptive threats is the Distributed Denial of Service (DDoS) attack. A DDoS attack seeks to make an online service unavailable by overwhelming it with traffic from multiple sources, effectively paralyzing the target system. This report delves into the types of DDoS attacks, how they function, what motivates attackers, historical examples, their impacts, and the strategies used to mitigate such threats.

Types of DDoS Attacks: DDoS attacks can take several forms, each leveraging different aspects of network or system vulnerabilities. Some of the most common types include:

DDoS attacks can take several forms, each leveraging different aspects of network or system vulnerabilities. Some of the most common types include:

1. **Volumetric Attacks**

These attacks aim to saturate the bandwidth of the targeted site. Examples include UDP floods and ICMP floods. Attackers send high volumes of traffic to a target to overwhelm its capacity.

2. **Protocol Attacks**

These exploit weaknesses in network protocols to exhaust server resources. Examples include SYN floods, Ping of Death, and fragmented packet attacks.

3. **Application Layer Attacks**

These target the application layer (Layer 7 of the OSI model), attempting to crash web servers by sending seemingly legitimate requests. HTTP floods and Slowloris attacks fall into this category.

4. **Amplification Attacks**

Attackers exploit vulnerabilities in publicly accessible servers (e.g., DNS, NTP) to amplify the traffic directed at the target, often reaching magnitudes far greater than the initial input.

How DDoS Attacks Work: A DDoS attack typically uses a **botnet**, which is a network of compromised computers (bots) under the control of an attacker. The process follows these stages:

1. **Infection and Control:** Malware is spread to vulnerable systems, allowing the attacker to control them remotely.
2. **Command and Control (C&C):** The attacker issues commands to the botnet via C&C servers.
3. **Attack Execution:** Bots simultaneously send requests or data packets to the target system or network, overwhelming it.

Unlike Denial of Service (DoS) attacks, which originate from a single source, DDoS attacks leverage multiple sources, making detection and mitigation significantly more difficult.

Motivations Behind DDoS Attacks:

1. **Financial Gain:** Attackers may extort money from victims by threatening to launch a DDoS attack unless a ransom is paid.
2. **Hacktivism:** Groups use DDoS attacks as a form of protest against organizations or governments.
3. **Competition:** Rival businesses may launch attacks to take down competitors' websites during critical sales periods.
4. **Testing and Demonstration:** Some attacks are carried out by individuals experimenting or showcasing their capabilities.

Notable DDoS Attacks in History: Several high-profile DDoS attacks have left lasting impressions in the cybersecurity community:

1. **Dyn DNS Attack (2016):** A massive DDoS attack on Dyn, a major DNS provider, brought down major websites like Twitter, Reddit, and Netflix. It was executed using the Mirai botnet, which hijacked IoT devices.
2. **GitHub Attack (2018):** GitHub was targeted with a record-breaking attack peaking at 1.35 Tbps. The attackers used a Memcached amplification technique.
3. **Estonia Cyberattacks (2007):** In one of the earliest examples of cyberwarfare, Estonia experienced large-scale DDoS attacks targeting government, media, and banking websites.

Impact of DDoS Attacks:

1. **Financial Losses:** Companies lose revenue due to website downtime and disrupted services.
2. **Reputational Damage:** Users may lose trust in organizations unable to maintain online stability.
3. **Operational Disruption:** Essential services may be interrupted, including banking, healthcare, and government functions.
4. **Security Breaches:** DDoS attacks can act as smokescreens, diverting attention while other cybercrimes are committed.

Prevention and Mitigation Strategies:

1. **Traffic Filtering:** Use of firewalls and intrusion prevention systems to detect and block suspicious traffic.
2. **Rate Limiting:** Restricting the number of requests a server will accept from a single IP address.
3. **Content Delivery Networks (CDNs):** Distribute web traffic across multiple servers globally, reducing the impact of an attack.
4. **Cloud-Based DDoS Protection:** Services like Cloudflare, AWS Shield, and Akamai offer scalable protection.
5. **Anomaly Detection:** Monitoring network traffic for unusual patterns helps identify and respond to attacks early.

Conclusion:

DDoS attacks remain a critical threat to the integrity and availability of online services. Their increasing complexity and accessibility make them a favored weapon among cybercriminals. While no system is entirely immune, a proactive and layered security strategy can significantly reduce the risks. As technology continues to evolve, so too must our defenses against these malicious disruptions.

References:

1. Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2), 39-53.
2. Cloudflare. (n.d.). What is a DDoS attack? Retrieved from <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>
3. Krebs, B. (2016). KrebsOnSecurity Hit With Record DDoS. Retrieved from <https://krebsonsecurity.com>
4. Arbor Networks. (2018). Worldwide Infrastructure Security Report.
5. Symantec. (2019). Internet Security Threat Report.

Live DDoS Example:

```
Activities Terminal Apr 2 11:24 student@ioe-it-lab-2-123: ~/Desktop/CS_TE41/A2

-----
D D O S   A T T A C K
-----

The IP address of the Host to Attack is : 192.168.5.135
The PORT address of the Host to Attack is : 1024

-----
[ ] 0%
[====] 25%
[=====] 50%
[=====] 75%
-----
```

Capturing from Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Source	Destination	Protocol	Length	Info
97581	192.168.5.123	192.168.5.135	UDP	602	60435 → 55883 Len=5000
97582	192.168.5.123	192.168.5.135	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=b7c9) [Reassembled in #97585]
97583	192.168.5.123	192.168.5.135	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=b7c9) [Reassembled in #97585]
97584	192.168.5.123	192.168.5.135	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=2960, ID=b7c9) [Reassembled in #97585]
97585	192.168.5.123	192.168.5.135	UDP	602	60435 → 55884 Len=5000
97586	192.168.5.123	192.168.5.135	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=b7ca) [Reassembled in #97589]
97587	192.168.5.123	192.168.5.135	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=b7ca) [Reassembled in #97589]
97588	192.168.5.123	192.168.5.135	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=2960, ID=b7ca) [Reassembled in #97589]
97589	192.168.5.123	192.168.5.135	UDP	602	60435 → 55885 Len=5000
97590	192.168.5.123	192.168.5.135	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=b7cb) [Reassembled in #97593]
97591	192.168.5.123	192.168.5.135	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=b7cb) [Reassembled in #97593]
97592	192.168.5.123	192.168.5.135	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=2960, ID=b7cb) [Reassembled in #97593]
97593	192.168.5.123	192.168.5.135	UDP	602	60435 → 55886 Len=5000
97594	192.168.5.123	192.168.5.135	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=b7cc) [Reassembled in #97597]
97595	192.168.5.123	192.168.5.135	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=b7cc) [Reassembled in #97597]
97596	192.168.5.123	192.168.5.135	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=2960, ID=b7cc) [Reassembled in #97597]
97597	192.168.5.123	192.168.5.135	UDP	602	60435 → 55887 Len=5000
97598	192.168.5.123	192.168.5.135	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=b7cd) [Reassembled in #97601]
97599	192.168.5.123	192.168.5.135	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=b7cd) [Reassembled in #97601]
97600	192.168.5.123	192.168.5.135	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=2960, ID=b7cd) [Reassembled in #97601]
97601	192.168.5.123	192.168.5.135	UDP	602	60435 → 55888 Len=5000
97602	192.168.5.123	192.168.5.135	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=b7ce) [Reassembled in #97605]

> Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF{...} Ethernet II, Src: MonHaiPrecis_c7:fb:25 (f4:6b:8c:c7:fb:25), Dst: MonHaiPrecis_c5:fa:17 (f4:6b:8c:c5:fa:17) Internet Protocol Version 4, Src: 192.168.5.123, Dst: 192.168.5.135 Data (1480 bytes)

0000 f4 6b 8c c5 fa 17 f4 6b 8c c7 fb 25 08 00 45 00 ...k...k...E: 0010 05 dc 58 e6 20 00 40 11 6f d8 c0 a8 05 7b c0 a8 ...X...@...{... 0020 05 87 ec 13 7c f9 13 90 d4 ba 54 51 7c 66 88 8b ...[...TQ|F... 0030 1d 36 b6 95 80 41 f1 5a 09 92 15 b8 a1 de 10 e4 ...6...A-Z...v... 0040 1c a6 7c cc 58 c2 9a e0 5c 8e 7c 12 e2 96 88 76 ...|X... \...v... 0050 cc b7 cd 84 fb 87 cc 11 eb 4c e6 25 74 4a c5 f4 ...-...L%tj... 0060 34 1e 8e f3 04 6e 6a 0e 62 e1 1d b7 12 50 b0 f0 4...n]-b...P... 0070 64 3b d9 1f 89 5e d6 a8 76 30 99 25 f2 f9 40 b8 d...v0%...@... 0080 a7 32 8a ba 1d e2 ab d3 8c 9f 5e fa 78 bf 34 32 2...x...k...42 0090 29 31 45 4d 08 75 aa 8d 4c 60 88 fa 6d b2 7a b6)1EM-u...L'-m=z... 00a0 70 f5 22 fb 6f ca bf 1c 45 54 4d eb 98 6c 5b c9 p...o...ETH:1[

Info can only be sorted with 10000 or fewer visible rows; increase cache size in Layout preferences

Packets: 97944 Profile: Default

27°C Partly sunny

Search

ENG US 00:20 02-04-2025