**Sri Lanka Institute of Information Technology**

**B.Sc. (Hons) Information Technology- Cyber security**



Y2 S1

Introduction to Cyber Security – IE2022

**Distributed Denial-of-Service (DDoS) attacks**

J A C P Jayasooriya

IT23554504

**Contents**

**1. Abstract**

* Overview of DDoS threats
* Objectives and scope of the report

**2. Introduction**

* Importance of cybersecurity in the digital age
* Definition and mechanics of DDoS attacks
* Historical context and growing sophistication
* Purpose of the report

**3. Evolution of DDoS Attacks**

* 3.1 Origins of DoS and Birth of DDoS (1990s)
  + Early attacks (e.g., Panix SYN flood)
* 3.2 Rise of Botnets (2000s)
  + High-profile attacks (e.g., Mafiaboy, MyDoom botnet)
* 3.3 Hacktivism and Cybercrime (2010–2015)
  + Operation Payback, DDoS-for-hire services
* 3.4 IoT Botnets and Terabit Attacks (2016–2019)
  + Mirai botnet, Dyn DNS attack
* 3.5 Multi-Vector and Ransom DDoS (2020–Present)
  + Ransom DDoS (RDoS), cloud-targeting attacks

**4. Future Developments in DDoS Attacks**

* 4.1 AI-Powered Adaptive Attacks
* 4.2 Expansion via IoT/Edge Devices
* 4.3 Serverless/Cloud-Native DDoS
* 4.4 Hybrid and Ransom Campaigns
* 4.5 Quantum Computing’s Impact

**5. Countermeasures and Defense Strategies**

* 5.1 Traditional Mitigation Techniques
  + Rate limiting, traffic scrubbing
* 5.2 Advanced Defense Mechanisms
  + AI/ML detection, Zero Trust Architecture
* 5.3 Collaborative and Policy Responses
  + ISP partnerships, international cooperation

**6. Conclusion**

* Summary of key findings
* Call to action for resilience and innovation

**7. References**

* Cited academic papers, reports, and articles

**Abstract**

In the current era of technology, Distributed Denial of Service (DDoS) attacks have emerged as one of the most pervasive and intrusive cyber security threats. This report explores the past, impact, and future direction of DDoS attacks, a technique where numerous compromised systems flood a victim with an onslaught of traffic, rendering services unavailable. More and more organizations are dependent on Internet infrastructure to conduct business, and attackers take advantage of system vulnerabilities to cause damage, reputations to be hurt, and hold ransom money for it. The report begins by charting the genesis of the idea of denial-of-service, followed by how the DDoS attack has developed from simple volumetric floods to sophisticated multi-vector botnet, IoT, and application-layer exploit campaigns.

The report highlights notable real-world attacks, including highly publicized attacks against government services, banks, and technology firms, to describe the scale and potential of such cyber-attacks. In addition, the paper also addresses current mitigation techniques, such as rate limiting, traffic filtering, along with utilization of high-end DDoS protection services.

In this instance, the study predicts the emergence of new forms of DDoS attacks, including AI-based and botnet-powered attacks, which need to be protected in advance and globally coordinated. The report aims to raise awareness about DDoS threats, inspire better readiness among IT professionals, and make contributions to the broader debate about how to secure online spaces.

**Introduction**

With the worldwide interconnectedness of today's digital communications era, the reliability and availability of internet services are key to the operations of business, governments, and individuals. Among the most dangerous disruptions to these services' stability and accessibility is the Distributed Denial of Service (DDoS) attack. Over the last two decades, DDoS attacks have been gaining momentum, becoming a major cyberthreat with the potential for destruction.

They are very famous for their ability to disrupt regular business, create financial losses, damage reputations, and exploit weaknesses in public and private sector networks and as with the development and growth of the Internet, so too has the severity, magnitude, and sophistication of the DDoS attacks required with a higher level of consciousness and more robust defense systems.

A Distributed Denial of Service, or DDoS, is a coordinated effort to make a particular server, service, or network unavailable through loading it with an excessive volume of internet traffic. A DoS is an attack source, and a DDoS is where a group of systems—a giant botnet—is assembled to swamp the victim with traffic in quantities larger than it can handle.

This kind of attack is difficult to deflect since it is distributed, and its installation goes unnoticed until damage has already been done. DDoS attacks are aimed at a vast range of targets like corporations, government agencies, banks, online shopping sites, and even general users. The attacks may either last a couple of days or a couple of minutes, and their effect ranges from short-term inconvenience to long-term financial loss and data loss.

DDoS attacks have been present for quite a while, but their growing prevalence over the past few years, along with their sophistication, have caused them to be an important cybersecurity issue. Large DDoS attacks have taken down some of the globe's biggest organizations and services, including GitHub, Dyn DNS, Amazon Web Services, and even government networks. Attackers employ DDoS attacks as a facade or a diversion, distracting the security teams and allowing them to carry out more complex attacks such as data breaches or ransomware. The simplicity with which DDoS-for-hire services, or "booter" or "stresser" services, have gained accessibility has also enabled even beginner attackers to launch enormous attacks at affordable prices. Therefore, DDoS developed from a tool used as a joke or a protesting tool to cyberwar and cybercrime tool, which may be misused.

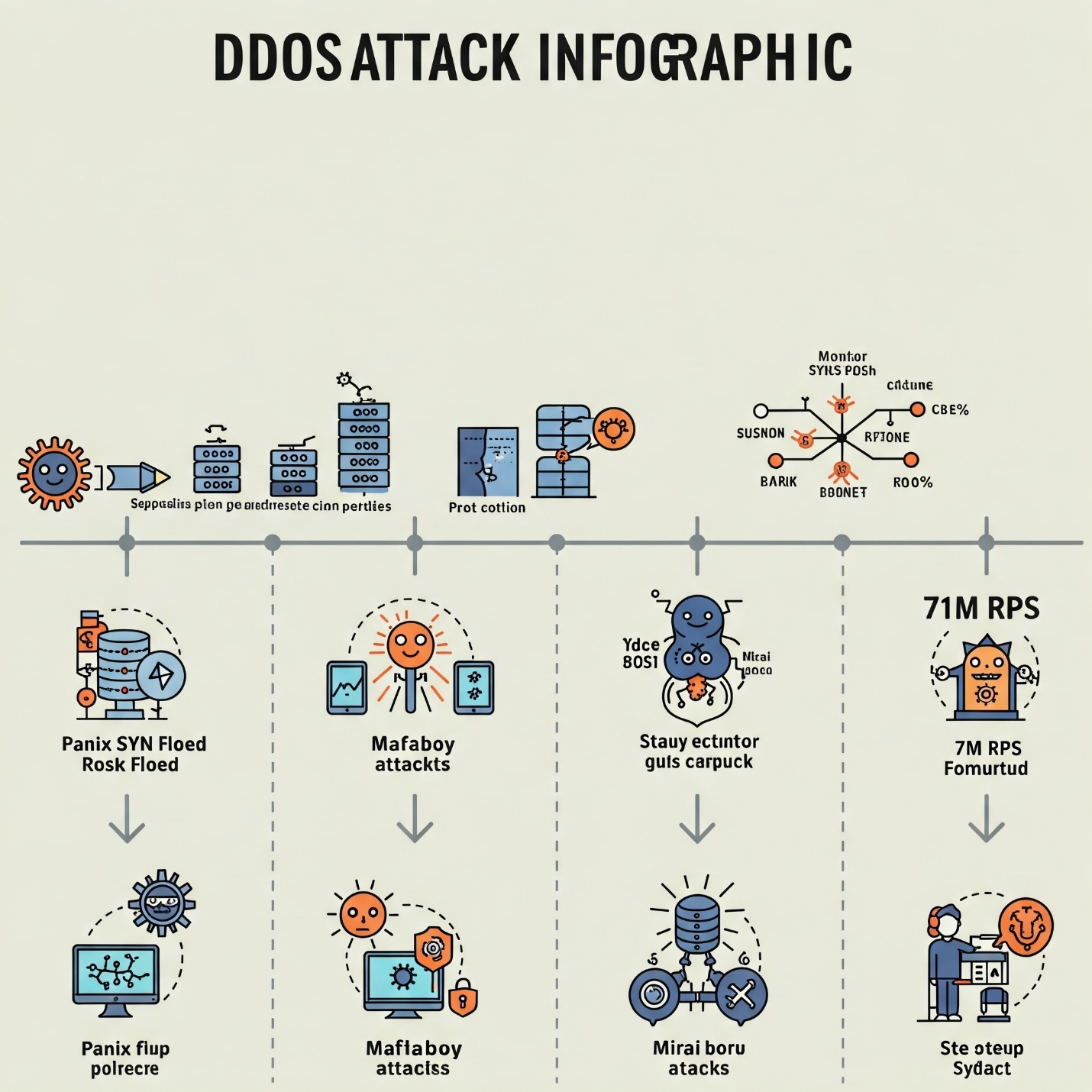
There is a requirement that cyber security specialists, network managers, and businesses utilizing the internet infrastructure are aware of the mechanism and effect of DDoS attacks. With the diversity of attack vectors—volumetric attacks created in kind, protocol attacks, and application-layer attacks—DDoS protection needs to be layered and anticipatory, DDoS attacks also create challenges that fall outside technical mitigation, such as attribution, legal, and policy-level responses. It is a very pertinent topic in the current digitalization age, when everything is internet-based with regard to communication and services.

This report also attempts to create an awareness among the students, researchers, and practitioners on the urgent need to mitigate the DDoS threats both from technological as well as policy interventions. Taking references from the latest research studies, industry standards, and countermeasures, this report attempts to offer analytical analysis on how the organizations can enhance their readiness and response to the DDoS attacks. Material to be covered will not only instruct on the technical aspects of DDoS attacks but also put their broader implications in perspective in terms of privacy, security, and worldwide resilience in cybersecurity.

In essence, Extended Threat Service Denial (DDoS) attacks are an ongoing and dynamic threat to the field of cyber security. Since the criminals are finding it difficult to discover and acquire new tactics, so does their competitor need to update tools and methods. This report will be a reference to authority for whoever would like to research or work on the topic of research in cyber security. It provides the opportunity to study DDoS attacks from a really wide view of history, technology, practicality, and strategy.

**Evolution of the Topic: Distributed Denial-of-Service (DDoS) Attacks**

DDoS attacks of the last two decades have increased exponentially. They were simple and one-way intrusions at the start of their time and developed into bigger, more complex operations and now they are the possibility of opening up global infrastructure to risk. That is an observation on trends in cybernetics; more people connected to everything, advancements happening everywhere in terms of machinery, more internet-based value and risk. This chapter summarizes the most significant milestones in the history of DDoS attacks, history of attackers' objectives and actions, history of attack methods and tools, and history of countermeasures.



**1. Origins of DoS and the Birth of DDoS (1990s)**

Denial-of-Service was initially put into practice during the early 1990s when internet usage began to increase among schools and businesses. Early DoS attacks were very simple: they flooded a victim network or server with spurious traffic, exhausting its resources and blocking legitimate users from it.

One of the earliest major attacks was in 1996 on Panix, a very old Internet Service Provider (ISP) in New York. The attack was composed of SYN floods—a technique utilizing the TCP handshake protocol as a weapon—to exhaust server resources. While initial DoS attacks were noteworthy, they came from individual machines and thus comparatively easy to trace and block.

The initial DDoS attack—hundreds of hijacked computers all at once flood-targeting one person—emerged sometime around 1999. it was a quantum leap in harmful potential, in capability, for attackers to reap the benefits of botnets' potential: a host of zombie computers hijacked (or commandeered) but controlled remotely

by an attacker to conduct a traffic attack.

**2. The Rise of Botnets and Major Attacks (2000s)**

The early 2000s were marked by the formalization and weaponization of DDoS attacks. They were years of some of the highest profile cases to bring broad public attention to the threat.

In 2000, a 15-year-old hacker known as "Mafiaboy" organized a series of DDoS attacks using a botnet he constructed himself to bring online sites such as Yahoo!, eBay, CNN, Amazon, and Dell offline. Those attacks brought the targets down for hours and cost tens of millions of dollars in business, bringing the attention of the FBI and precipitating government-level cybersecurity efforts.

Botnets such as MyDoom (2004), Bagle, and Zotob emerged during that time. While they initially became notorious due to spams and malware spreads, they also supported notorious DDoS attacks. The hackers were transitioning from personal notoriety to commodification, and they realized that DDoS also belonged in an option to extort or disrupt businesses.

Development of user-friendly tools for performing DDoS attacks like LOIC (Low Orbit Ion Cannon) and HOIC (High Orbit Ion Cannon) became extremely simple toward the end of the 2000s and made the DDoS aspect much easier for script kiddies with minimal technical expertise and hacktivist groups like Anonymous, who could carry out mass-based attacks without elaborate technical expertise.

**3. Hacktivism, Cybercrime, and Political DDoS (2010–2015)**

2010-2015 was the period of diversification of intentions and methods in DDoS attacks. Hacktivism increased, and particularly by such organizations as Anonymous and LulzSec, who used DDoS for political or social cause promotion.

A few instances that are worth mention are:

Operation Payback (2010):

One of the schemes of DDoS attacks against anti-piracy organizations and such organizations as Visa, MasterCard, and PayPal for how they treated WikiLeaks.

DDoS-for-Hire Services

The development of websites like Booter and Stresser phases made it possible for any user who had a credit card to lease DDoS attacks for money. They were commodified in the ordinary web, and consequently, it became fashionable for cybercrime.

State-Sponsored DDoS:

Geopolitical tensions had provoked claimed nation-state DDoS attacks, such as against Estonian infrastructure in 2007 (to a large extent blamed on Russian interface) and Georgian sites during the 2008 conflict.

Technically, the era experienced increased volumes and levels of sophistication in attacks. The DNS amplification attack matured as a powerful technique, using misconfigured DNS servers to redirect and amplify attack traffic to gigabit-sized data transfer rates. Tools also started launching application layers (Layer 7) attacks, and moderation tools used traditionally found it challenging to mark the attack as malicious.

**4. IoT Botnets and the Era of Terabit DDoS (2016–2019)**

The DDoS threat landscape entirely shifted in 2016 with the emergence of the Mirai botnet. Mirai infected insecure Internet of Things (IoT) devices—such as IP cameras, routers, and digital video recorders—and created a massive botnet capable of launching attacks exceeding 1 terabit per second (Tbps).

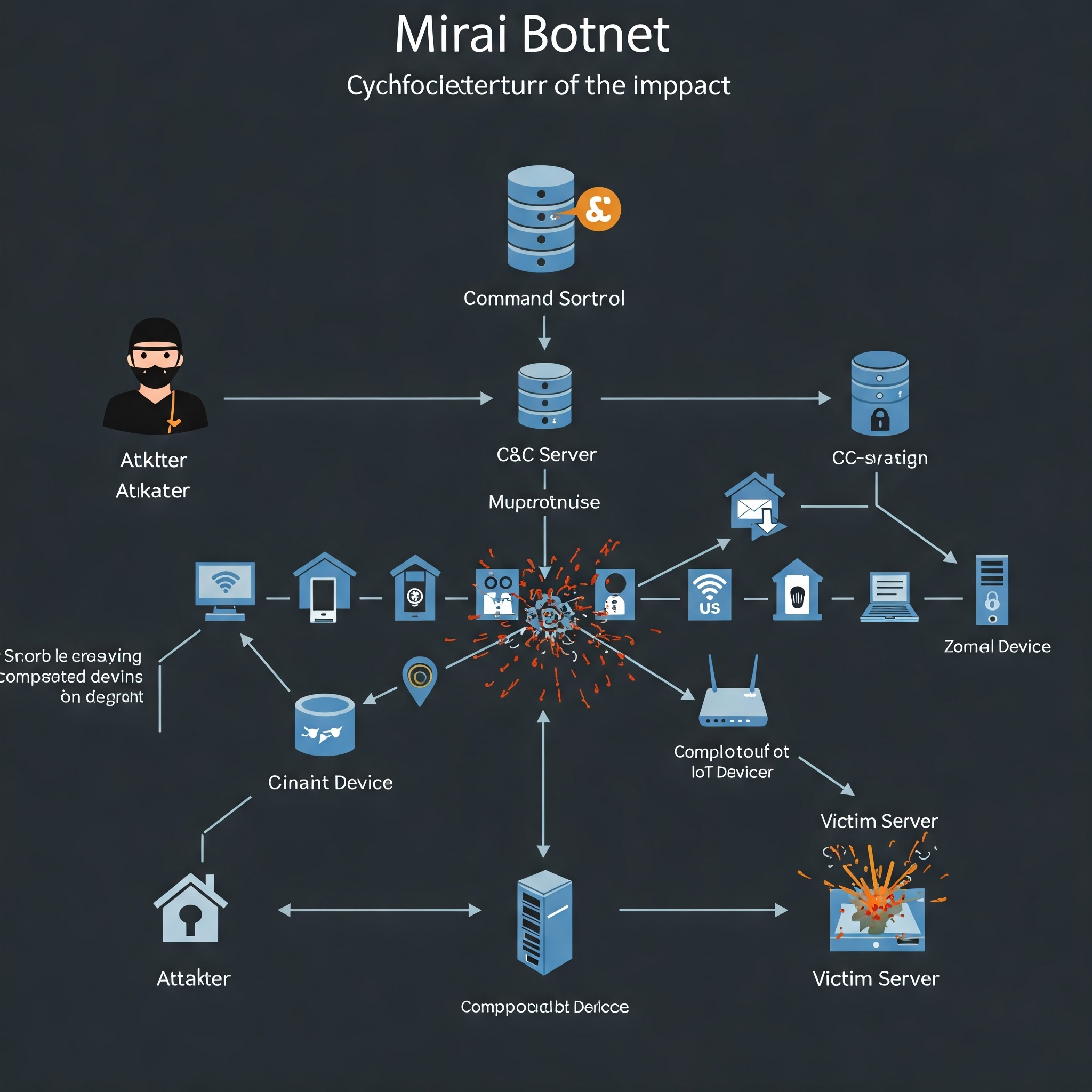
Key events:

Dyn Attack (October 2016): Botnet Mirai launched an attack on DNS provider Dyn and impacted widespread outages of major websites like Twitter, Reddit, Netflix, and Spotify.

Brian Krebs and OVH (2016): Security journalist Brian Krebs's news site was attacked with a 620 Gbps DDoS, and French web hosting company OVH was hit with a Mirai-powered attack of 1.1 Tbps.

IoT Insecurity: The mass proliferation of poorly secured IoT devices created an enormous attack surface. Devices were often shipped with default credentials and no auto-update mechanisms, making them easy prey for malware like Mirai and its variants.

This period also saw growing reliance on cloud-hosted DDoS defense solutions (e.g., Cloudflare, Akamai, AWS Shield) and an added focus on proactive protection efforts such as rate limiting, anomaly detection, and machine-learning traffic analysis.



**5. Multi-Vector and Ransom DDoS Attacks (2020–Present)**

a. Ransom DDoS (RDoS)

Threats of DDoS in place of a ransom payment, both in cryptocurrency and currency, are now being issued by cybercriminals in extortion emails. Sometimes, they launch a small-scale attack as a demonstration of capability. Groups like Fancy Lazarus and Armada Collective have used this tactic against financial institutions and enterprises.

b. Record-Breaking Attacks

Cloudflare reported mitigating a 71 million requests-per-second HTTP DDoS in 2023—setting a new record. Microsoft Azure repelled a 3.47 Tbps assault in 2022.These attacks demonstrate the manner in which DDoS has grown by orders of magnitude because of botnets, reflection strikes, and new amplification vectors

c. Reflection and Amplification Innovations

New protocols are still being utilized for amplification, including CLDAP, Memcached, NTP, and DNS. Memcached servers were utilized in 2018 to enjoy amplification rates of more than 50,000x, and it resulted in the largest known DDoS attacks so far.

d. Cloud and CDN Targeting

As organizations migrate to cloud and use Content Delivery Networks (CDNs), attackers have adapted by targeting these services directly or trying to bypass their protection layers.

e. DDoS as a Distraction

In high-end cyber-espionage campaigns, DDoS attacks are used as smokescreens to distract while other malicious activities—such as data exfiltration or ransomware delivery—are conducted quietly

**6. Countermeasures and the Security Arms Race**

As DDoS attacks grew in intensity, so too did the development of defense strategies. The evolution of mitigation reflects a continuous arms race between attackers and defenders:

Basic Filtering: First, the mitigations targeted were IP blacklisting, traffic rate limiting, and traffic throttling.

Traffic Scrubbing: Traffic flows through scrubbing centers that filter out malicious packets before reaching the destination

AI/ML-Powered Detection: The most recent solutions use machine learning methods to identify anomalous traffic and forecast attacks before the damage is done.

Anycast Networks: The content is replicated with multiple servers for it to better intercept the DDoS traffic.

Zero Trust Architectures: Not an explicit DDoS mitigator but adopting the concept of zero trusts helps contain the blast radius of successful attacks.

Cybersecurity companies now offer DDoS protection as a managed service, and ISPs typically work together with customers to disperse volumetric attacks. Governments also release advice and collaborate in public-private partnerships to protect major infrastructure from DDoS.

**Future Developments in the Area of DDoS Attacks**

As digital infrastructure continues to grow in complexity and value, Distributed Denial-of-Service (DDoS) attacks are expected to evolve in both scale and sophistication. The advent of cloud computing, edge networks, 5G, and AI is creating new opportunities for attackers as well as defenders. Even as cyber security technologies predict enhanced countermeasures, the future of DDoS attacks also predicts more innovative, long-lasting, and automatic ways to attack. This chapter explores the future trend in the area of DDoS—attack and protection using examples from life to project current trends.

**1. Rise of AI-Powered and Adaptive DDoS Attacks**

One of the most pressing future concerns is the emergence of AI-driven DDoS attacks. Traditional attacks tend to employ brute-force flooding or basic reflection strategies, while those in the future might employ machine learning to update attack patterns accordingly to the defending measures of the target in real-time.

A point of instance, an AI-powered botnet would be able to scan the network responses, identify whether throttled or filtered, and use alternative ports, protocols, or payloads that will bypass those specific defenses. These "intelligent" attacks can mimic legitimate traffic more effectively, thereby making it much harder to identify them.

Moreover, adaptive DDoS attacks may exploit traffic patterns or user behavior, timing themselves to strike during periods of peak activity or holidays, increasing damage while reducing the chances of immediate human intervention.

Example: In the future, an AI botnet can assault an e-commerce website's traffic just before a high-traffic online sale day like Black Friday, inflicting maximum damage and incurring maximum financial loss.

**2. Expansion Through IoT and Edge Devices**

The proliferation of Internet of Things (IoT) devices continues to present a massive vulnerability in cybersecurity. Over 25 billion IoT devices are predicted to be connected globally by the year 2030. A large number of these devices carry poor security configurations, and in most cases, users do not even update their firmware.

Future DDoS attacks are only going to use even larger and more diverse botnets by exploiting vulnerable smart home devices, industrial control systems, and even smart cars.

As computing shifts toward edge networks—decentralized processing close to users—there is an increased risk of attacks targeting edge devices to disrupt services like autonomous vehicle systems or healthcare IoT applications.

Example: A DDoS attack that compromises thousands of smart thermostats, printers, and wearable devices could be coordinated to simultaneously flood a city’s traffic control infrastructure, causing widespread delays or accidents**.**

**3. Serverless and Cloud-Native DDoS**

As businesses transition toward serverless platforms and cloud-native systems, an attacker can begin misusing Function-as-a-Service (FaaS) platforms to initiate the latest types of application-layer DDoS assaults.

Dynamic, automatable serverless deployment is able to cascade expensive backend work—either wastage of resources or peaking billing, or effectively being Denial-of-Wallet (DoW) attacks.

Cloud-native DDoS attacks may be less concerned with getting services offline but more inclined to send their operational cost skyrocketing. Attackers can create artificial API calls or run complex workflows within CRM or ERP systems.

Example: an attacker potentially automatically generates API calls that produce resource-intensive queries in a serverless analytics implementation, charging a company thousands of dollars in processing fees while cutting.

**4. DDoS as a Component of Hybrid and Ransom Campaigns**

Future cyberattacks are likely to include DDoS as a component of multi-stage campaigns. Rather than stand-alone attacks, DDoS may serve as a diversion, ransom demand, or be part of a larger compromise (i.e., ransomware or data exfiltration).

Ransom DDoS (RDoS) attacks are expected to grow in sophistication. Threat actors are taking advantage of blockchain anonymity solutions and AI-created ransom demands, time-based ultimatums, and catastrophic proof-of-concept attacks.

Additionally, nation-state actors may use DDoS in hybrid warfare strategies—targeting infrastructure like telecoms, hospitals, or election systems as part of coordinated cyber warfare efforts.

Example: A nation-state-sponsored group could use a DDoS attack on a news site during an election to suppress the distribution of real-time results, while simultaneously launching misinformation campaigns across social media.

**5. Quantum Computing’s Long-Term Impact**

Though still in its early stages, quantum computing poses a theoretical long-term risk and opportunity. On one hand, quantum technology could help analyze and filter large-scale DDoS traffic faster than current systems. On the other hand, cybercriminals can use quantum-powered equipment to evade cryptographic protections and control secure communication in botnets more effectively. Example: A quantum-accelerated DDoS defense system could instantly sort legitimate and malicious packets even during high-volume attacks, enabling real-time, precise mitigation.

**6. Advancements in DDoS Defense**

The future is not only characterized by more dangerous dangers but also by more cleverer and better counter-dangers.

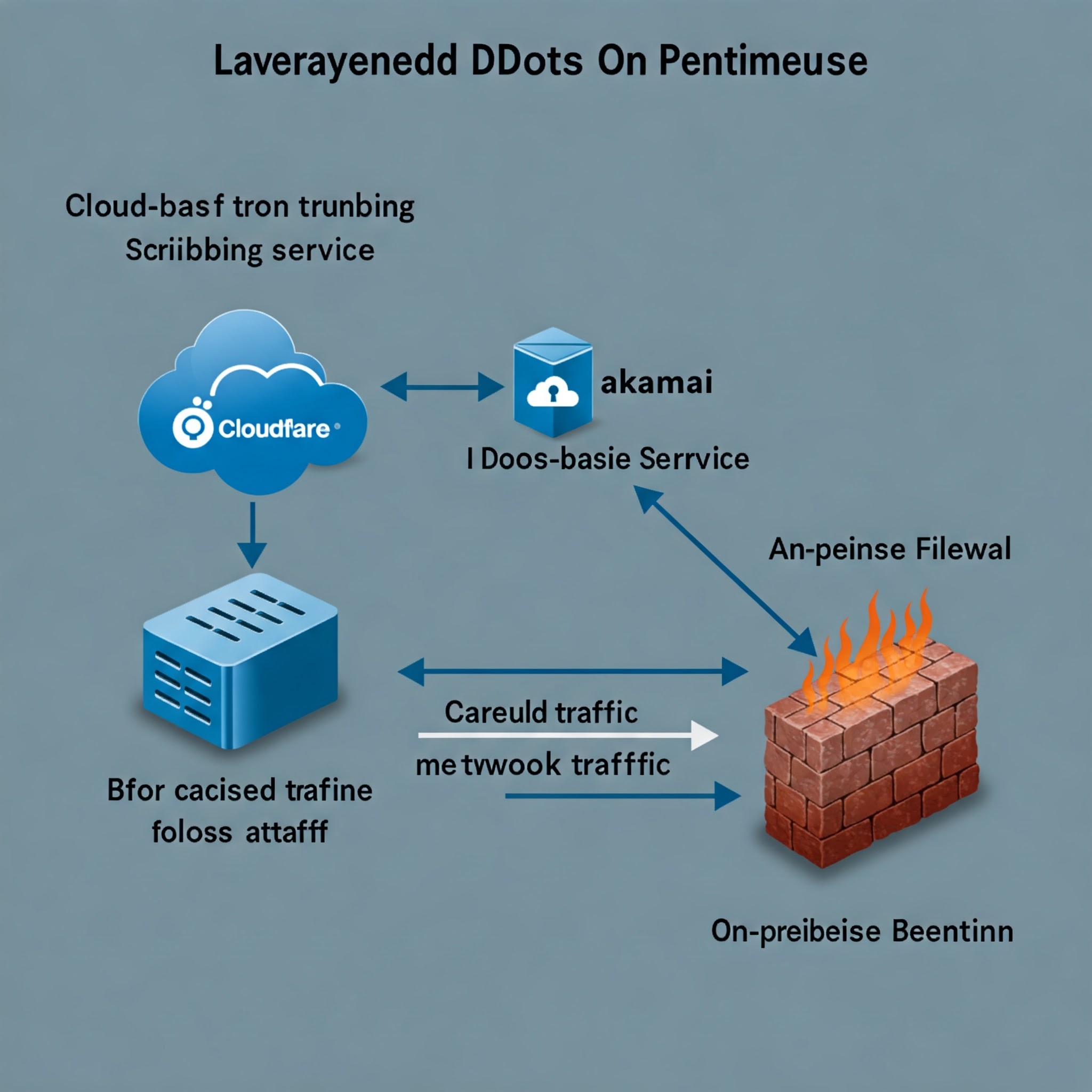
Behavioral AI Defense: Machine learning-driven algorithms accustomed to normal user and app behavior can label and block out-of-behavior traffic better.

Zero Trust Networking: This architecture limits the trust assigned to any user or system, helping to isolate and contain DDoS impacts before they spread.

Decentralized Infrastructure: Blockchain-based DNS systems or distributed CDNs can prevent attackers from bringing down single points of failure.

Proactive Mitigation with Predictive Analytics: Future defense platforms may use historical threat intelligence and real-time analytics to predict DDoS attacks before they occur.

Example: An advanced cloud firewall could potentially be able to identify an unusually rapid flood of untypical TCP SYN requests within a certain region and automatically redirect traffic to a scrub center before.



**Conclusion**

Distributed Denial-of-Service (DDoS) attacks are arguably the most persistent, crippling, and dynamic of the information era's cyber menaces. As discussed throughout this task, the character, mechanics, and impacts of DDoS attacks have dramatically changed over the past few decades—transiting from fairly simple flooding attacks to advanced, multi-vector attacks leveraging cloud infrastructure, IoT devices, and artificial intelligence. Recognizing this progression, and the projected path of such attacks, is vital to individuals, businesses, and governments looking to remain cybersecurity resilient in an ever-more connected world.

One of the core findings of this study is that the fundamental objective of DDoS attacks has remained consistent: to make a service, website, or infrastructure unavailable to its intended users. However, the methods used by attackers have become far more sophisticated. Traditional volumetric attacks like UDP and SYN floods have been accompanied by more surreptitious application-layer attacks, reflection/amplification attacks, and low-rate attacks camouflaged as normal traffic. These tactics make detection and mitigation increasingly difficult, as attackers blend into normal user behavior or exploit system vulnerabilities in new and unpredictable ways.

Equally important is the role of botnets, which continue to expand in power and reach. With the introduction of Internet of Things (IoT) devices, there are numerous more vulnerable endpoints available for attackers to exploit. IoT devices like cameras, routers, thermostats, and wearables that are not defaulted to being secured are left open and are the first targets for botnet recruitment. The infamous Mirai botnet was the quintessential example, showing how consumer-grade devices can be weaponized on a large scale to mount enormous attacks on key infrastructure.

Going forward, growing automation and artificial intelligence (AI) adoption will serve both to further DDoS defense efforts as well as frustrate them. Bad actors already use AI-boosted tools to real-time tweak attack settings, bypass security filters, and use behavioral analytics to their advantage. Defenders are employing AI-driven anomaly detectors to identify problematic traffic, predict threats, and respond faster than ever before this AI offense and defense arms race will be at the forefront of the future of DDoS warfare.

Additionally, the new technologies such as edge computing, serverless architecture, and 5G have introduced new attack surfaces .Even as these technologies enable faster, more powerful attacks, they also introduce new vulnerabilities.

Decentralization of processing data within the edge infrastructure, for instance, means that the attacker does not necessarily need to attack centralized servers anymore—now attacking the endpoints themselves. Similarly, serverless functions, which automatically scale on demand, can be manipulated to cause billing overloads (Denial-of-Wallet attacks), exhausting both computational and financial resources.

The impact of DDoS attacks also extends beyond the technical disruption. From money loss and loss of image to service delay and even potential risk to human safety (for instance, healthcare or transport) the impact may be extensive. Over the past two years, the extortionate (as in ransom DDoS or RDoS) and political saboteur weaponization of DDoS attacks has pushed them to national security concerns of utmost importance

In order to combat these evolving threats, there needs to be a multi-layered, hybrid approach. This includes investment in hardened infrastructure (like cloud-based scrubbing centers and content delivery networks), deployment of best security practices (like Zero Trust Architecture), and constant user education about the necessity to lock down their devices. International organizations, ISPs, industry groups, and governments need to all work together on threat information sharing, standardization, and stronger regulation of cybersecurity.

Conclusion, DDoS attacks are no longer just a nuisance—but a significant, evolving cyber threat that necessitates forward-thinking, strategic responses. As attackers become more resourceful and technologies more interconnected, the challenge will not merely be to stop attacks, but to predict, absorb, and adapt to them with resilience. It is by being watchful, creative, and cooperative alone that we are able to defend the digital worlds on which everyday life more and more depends.

**Reference**

[1] S. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.  
doi: 10.1109/SURV.2013.031913.00127

[2] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," *ACM Computing Surveys (CSUR)*, vol. 39, no. 1, pp. 3–es, 2007.  
doi: 10.1145/1216370.1216373

[3] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," in *Proc. 2015 International Conference on Computing, Networking and Communications (ICNC)*, Garden Grove, CA, USA, 2015, pp. 77–81.  
doi: 10.1109/ICCNC.2015.7069319

[4] M. Prince, "The DDoS that almost broke the Internet," *Cloudflare Blog*, Mar. 2020. [Online]. Available: https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/

[5] A. K. Sood and R. J. Enbody, "Targeted cyberattacks: A superset of advanced persistent threats," *IEEE Security & Privacy*, vol. 11, no. 1, pp. 54–61, 2013.  
doi: 10.1109/MSP.2012.90

[6] N. Moustafa et al., "New generations of DDoS attacks: Taxonomy, challenges and future directions," *Computer Networks*, vol. 199, 2021, Art. no. 108376.  
doi: 10.1016/j.comnet.2021.108376

[7] R. Bolla, R. Bruschi, F. Davoli, and F. Cucchietti, "Energy efficiency in the future Internet: A survey of existing approaches and trends in energy-aware fixed network infrastructures," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 2, pp. 223–244, 2011.  
doi: 10.1109/SURV.2011.041310.00087

[8] A. Sharf, "Mirai botnet code sparks fears of more massive IoT attacks," *Wired Magazine*, Oct. 2016. [Online]. Available: https://www.wired.com/2016/10/mirai-botnet-massive-iot-attacks/

[9] T. Holz, "Botnets: Detection, measurement, disinfection & defense," *European Network and Information Security Agency (ENISA)*, 2011. [Online]. Available: <https://www.enisa.europa.eu/publications/botnets-detection-measurement-disinfection-and-defence>