MAZEBOLT

Top 10 DDoS Attacks to Prepare for in 2024

Executive Summary

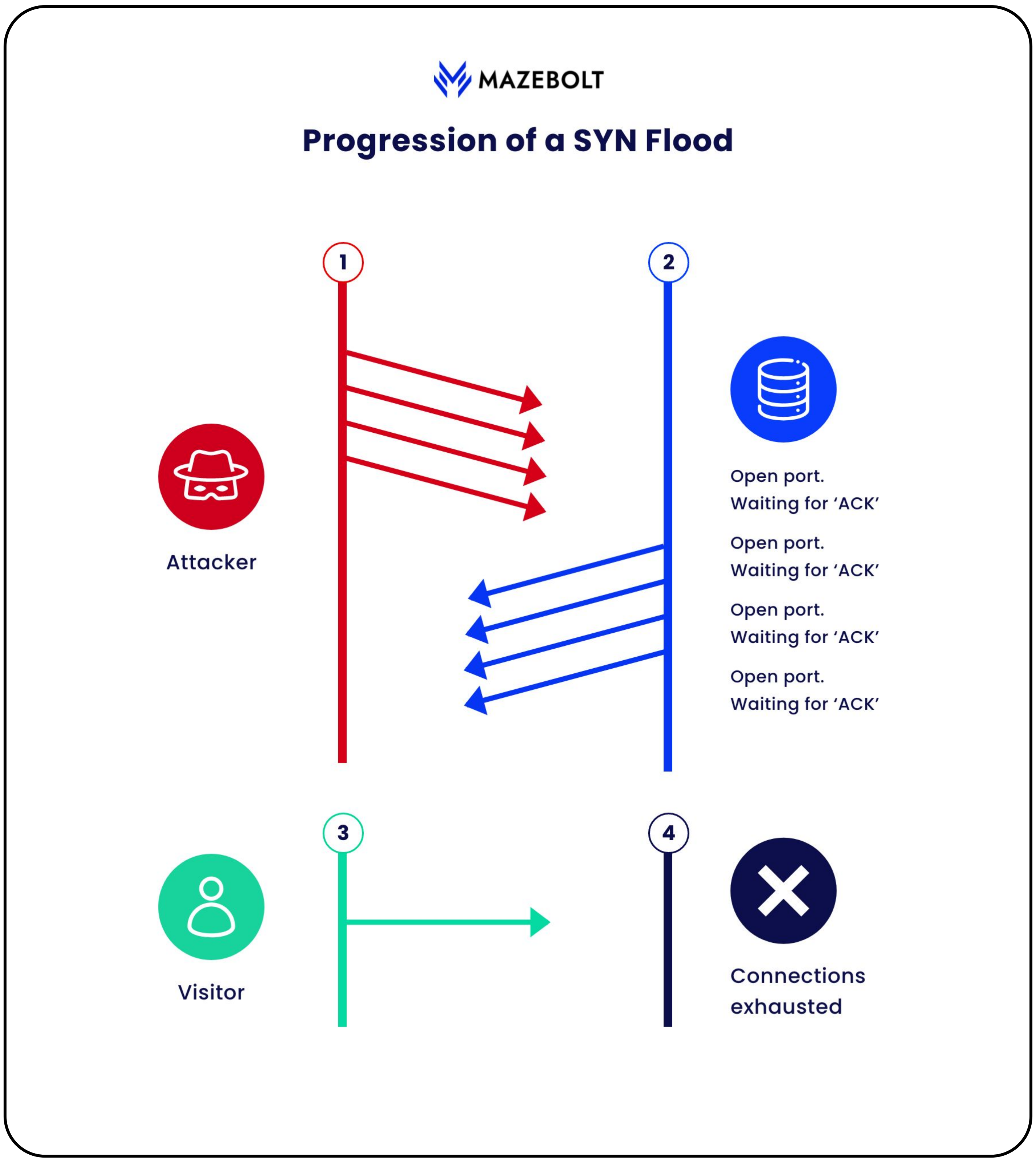
DDoS attacks are a type of cyber attack that are designed to overwhelm a targeted network with traffic, disrupting or shutting down service to legitimate traffic. DDoS attacks can be particularly damaging, as they affect not only the target organization but also its customers, partners, and other stakeholders. Recent years have shown that DDoS attacks are becoming more complex and hazardous, and because DDoS attacks can originate from thousands of sources, they can be difficult to stop. A successful DDoS attack could last hours or even days, and in some cases weeks.

Due to the rising "popularity" of DDoS attacks with various global threat actors, DDoS attacks have evolved to ransom attacks, especially against financial institutions and organizations. Perpetrators see the opportunity and launch ransom DDoS attacks that can shut down organizations for substantial periods of time, and in the past few years, DDoS attacks were used as a cover to divert and distract security teams while other forms of attack were launched to gain access to sensitive data. To defend against DDoS attacks, it is important to understand the various tactics and techniques that attackers may use. In the coming pages, we will explore the 10 most common DDoS attack vectors.

It is important to note that some of these attack vectors are considered "obsolete", as they have not been in use in recent years. But if there's one thing we've learned in recent years is that one should never underestimate DDoS threat actors. Just like reviving "obsolete" botnets in 2022, DDoS perpetrators can and might bring back an old attack vector, create a new variant, or simply use an attack vector that mitigation providers dismissed. Whatever the case might be, it is important to get familiar with the most common DDoS attack vectors out there.

1. SYN flood

Exploits a weakness in the TCP connection sequence (also known as the "three-way handshake") to consume server resources and prevent legitimate traffic from being accepted. Threat actors use this method to disrupt services by sending a large number of SYN (Short for synchronize) packets to a targeted server, and in many cases, they use fake IP addresses. The server, receives multiple, apparently legitimate requests to establish communication and it responds to each attempt with a SYN-ACK packet from each open port. Before the connection can time out, more SYN packets arrive, which leaves an increasingly large number of connections half-open, creating a flooded environment which consumes bandwidth and server resources that ultimately disrupts service.

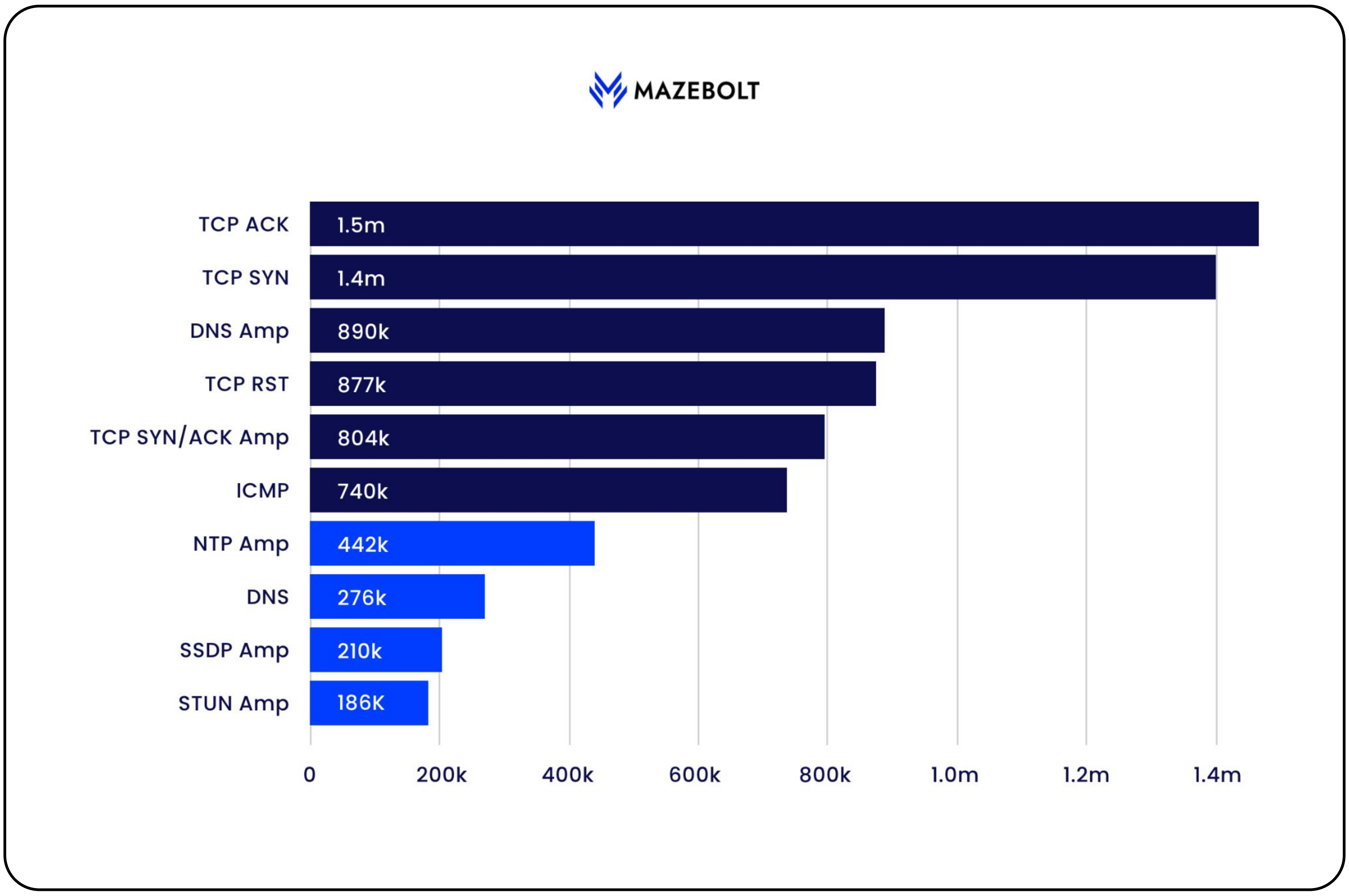


2. UDP flood

Involves sending a large number of random UDP (User Datagram Protocol) packets to a targeted server or network, to overwhelm it with traffic. Perpetrators use UDP floods to send thousands of packets to a targeted server, which checks for applications associated with these datagrams. The target finds no such applications and sends back a “Destination Unreachable” packet. As more and more UDP packets are received and answered, the system becomes overwhelmed and unresponsive to customers, thus falling victim to a disruptive and overwhelming attack.

3. TCP flood

This attack vector is similar to a SYN flood, but it involves sending a large number of TCP connection requests to a targeted server or network in order to consume server resources and prevent legitimate traffic from being accepted. According to recent reports, continuing a trend that started in early 2021, TCP flood attacks remain the most used DDoS attack vector, comprising approximately 46% of all DDoS attacks in the first half of 2022. One of the largest DDoS attacks that took place in 2022 was a multi-vector attack that was launched by a Mirai botnet variant against Minecraft, the popular game. This attack included both UDP and TCP floods, and was mitigated by the mitigation vendor, who admitted this specific attack was one of the hardest they’ve had to mitigate in recent years.

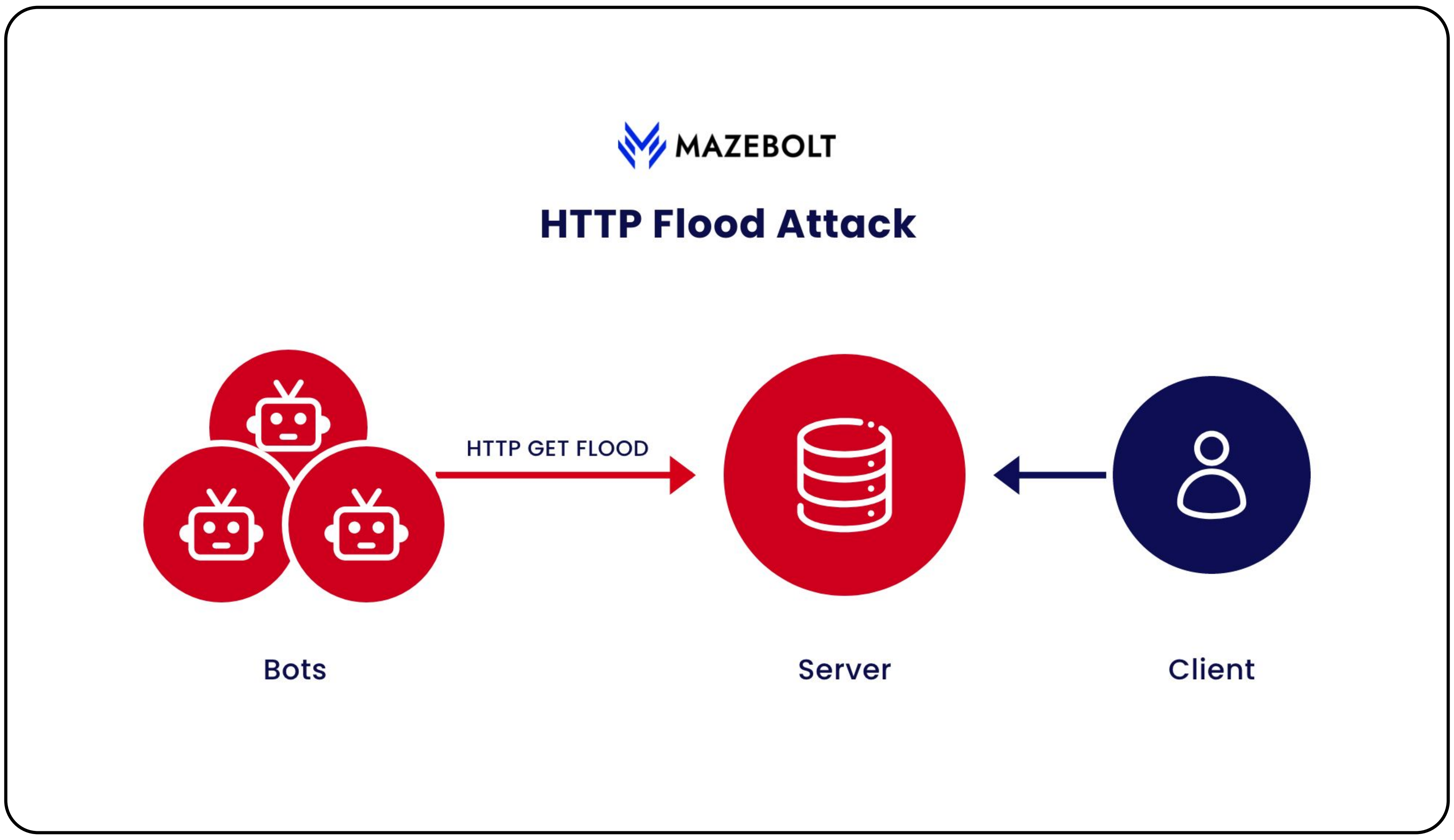


4. DNS amplification

Sends many DNS lookup requests to servers that are configured to amplify responses, with the intention of overwhelming the target system with traffic. Using this vector, the perpetrator will send a DNS query with a forged IP address to an open DNS resolver, prompting it to reply to that address with a DNS response. But as numerous fake queries are sent, and with several DNS resolvers replying simultaneously, the target network will be overwhelmed by the amount of DNS responses. To amplify the DNS attack, the perpetrator will relay DNS requests through one or more botnets, thus increasing the amount of traffic on the target's servers, making it harder to trace the origin of said traffic.

5. HTTP flood

Is performed by sending thousands, and sometimes even millions of HTTP requests to a targeted web server to overwhelm it with traffic. The goal is, of course, to disrupt and deny service for online applications and sites relying on online services for their operations. HTTP flood attacks are volumetric attacks, often using a botnet made up of a group of Internet-connected computers, each of which has been maliciously taken over, usually with the assistance of malware like Trojan Horses. HTTP floods require less bandwidth than other attack vectors to bring down the target. Thus, they demand a more in-depth understanding of the target, and each attack must be tailored to be effective. This is because HTTP flood attacks are a layer 7 DDoS attack, and mitigating application layer attacks is complex, as the malicious traffic is difficult to distinguish from normal traffic. These reasons make HTTP flood attacks much harder to detect and block.



6. NTP amplification

This attack vector involves sending many requests to Network Time Protocol (NTP) servers. NTP is one of the oldest network protocols and is mainly used by Internet-connected machines to synchronize their clocks. In addition, older versions of NTP support a monitoring service that enables administrators to query a given NTP server for a traffic count. The command sends the requester a list of the last 600 hosts that have connected to the queried server. The perpetrator then sends the request to an NTP server, using a fake IP, and the target responds, but this response is considerably larger than the request, amplifying the amount of traffic directed at the target server and eventually leading to a denial of service for legitimate requests.

7. SSDP amplification

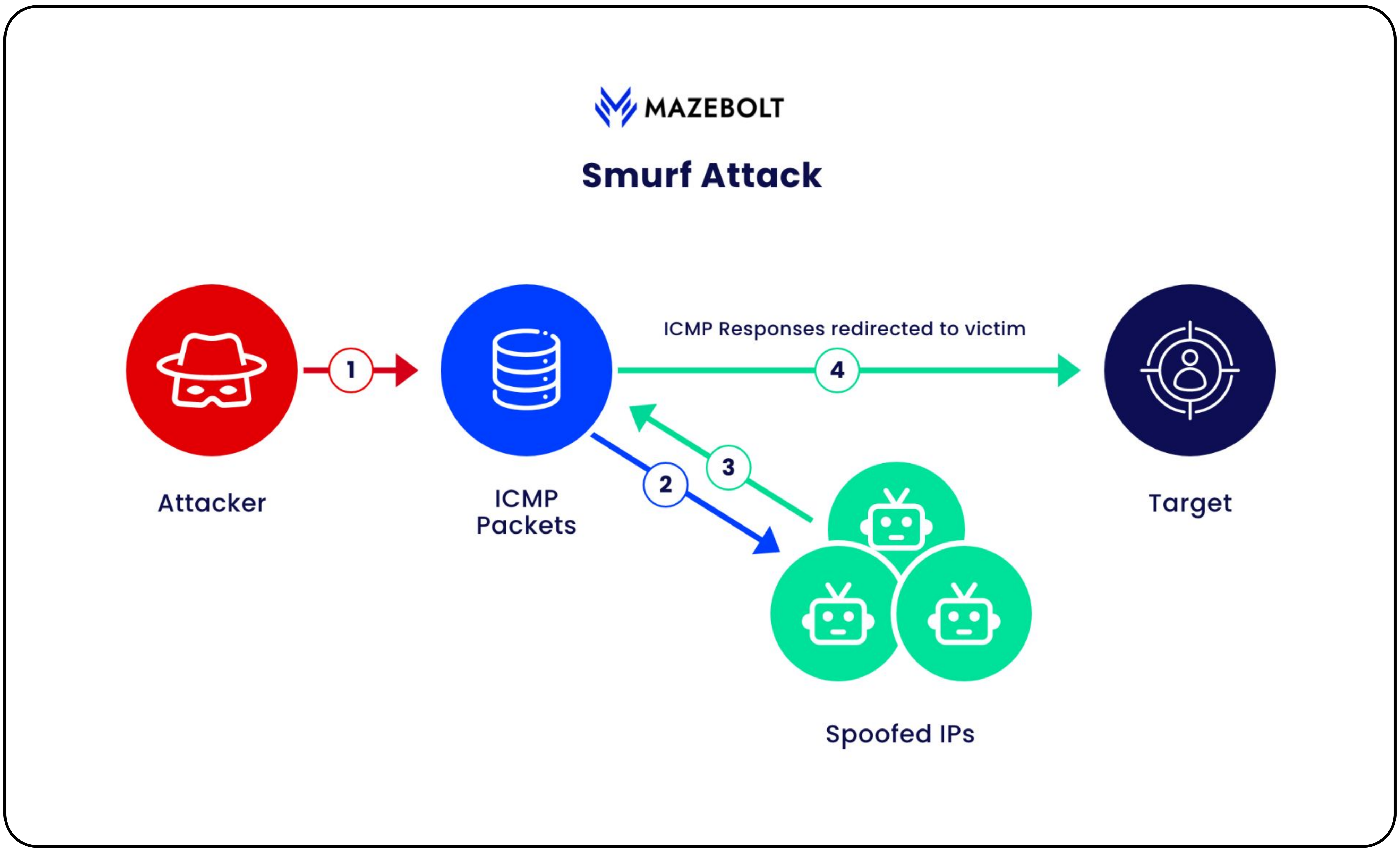
The Simple Service Discovery Protocol (SSDP) is a reflection-based attack vector that exploits Universal Plug and Play (UPnP) networking protocols to send an amplified amount of traffic to a target, overwhelming its network and taking its web activity offline. The SSDP protocol is used to allow UPnP devices to broadcast their existence to other devices on the network. An SSDP attack exploits that request for services by asking devices to respond to the targeted victim, in large volumes, thus creating an overwhelmed network that cannot function properly and must go down.

8. Chargen amplification

The Character Generator Protocol (Chargen), is a very old protocol that is still in use today with most Internet-enabled devices such as printers and copiers. The Chargen protocol can be exploited to execute amplified attacks that are implemented by sending small packets carrying a spoofed IP of the target to devices running Chargen. These spoofed queries to such devices are then used to send UDP floods as responses from these devices to the target. When the target tries to make sense of these queries, it fails to do so, and eventually, the server will exhaust its resources and go offline or reboot. Besides the harm that may be caused to the victim of a Chargen amplification attack, the Chargen servers involved in the attack may also be affected and crash due to the large number of inquiries received from a botnet consisting of thousands of machines.

9. Smurf attack

This type of attack uses a large number of ICMP (Internet Control Message Protocol) echo request packets to a network's broadcast address, with the goal of overwhelming the target system with traffic. Most devices on the target network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. The unusual name comes from the idea of very small, but numerous attackers overwhelming a much larger opponent, like in popular the animation show The Smurfs. It is true that nowadays, administrators can make a network reasonably immune to Smurf attacks, but as DDoS attacks become more sophisticated in recent years, one must not rule out this veteran attack vector.



10. Fragglе attack

A Fraggle Attack is another veteran DDoS attack vector that involves sending a large amount of spoofed UDP traffic to a router’s broadcast address within a network. It is very similar to the Smurf attack, which uses spoofed ICMP traffic rather than UDP traffic to achieve the same goal. As with the Smurf attack, this attack vector is rarely used nowadays, as routers no longer forward packets directed at their broadcast addresses. But as we’ve learned in recent years, threat actors do not hesitate to use old but proven methods to carry out their malicious disruptive DDoS attacks.

Now that we know the vectors – what do we do?

Although these attack vectors are known, and some of them even considered obsolete, one must remember that as networks become more complex, DDoS attacks vectors evolve to become more sophisticated. Many DDoS attacks combine several attack vectors and sometimes are even used as a distraction for other cyber-criminal activities. Ongoing testing for DDoS vulnerabilities across your entire live environment is essential for ensuring the resilience and availability of a network or website. Many organizations are concerned about the expected downtime, due to red team testing, but exposing DDoS mitigation gaps does not mean red team testing alone.

In order to expose the existing gaps in the mitigation layers and invest the proper efforts in remediation, an organization must take the proactive approach: continuous and non-disruptive testing for DDoS vulnerabilities across the entire attack surface. This will expose said gaps, which will be followed by remediating the vulnerabilities and unknown attack vectors, without compromising business operations. This can be achieved with a few necessary actions that are crucial, as coming years promise yet another escalation in the DDoS battlefront. The vulnerabilities are present, and attack vectors are evolving, as do botnets and their variants. A proactive approach to DDoS attack surface management can make the difference between downtime following a DDoS attack, to no downtime at all.

About MazeBolt

MazeBolt pioneers a new standard in testing DDoS vulnerabilities that provides enterprises with full visibility into their dynamic DDoS attack surface. Its vulnerability solution, RADAR™ testing, continuously observes tens of thousands of potential DDoS attack entry points, identifying how attackers succeed in bypassing existing mitigation systems. RADAR's autonomous risk detection allows cybersecurity teams to go beyond traditional DDoS testing by continuously detecting, analyzing and prioritizing remediation across the network with zero operational downtime. Global enterprises, including financial services, insurance, and governments rely on MazeBolt for full visibility into their DDoS security posture.

LEARN MORE

MAZEBOLT