ON2IT AND AMS-IX PRESENT: THREAT TALKS

Threat Talk 1:
Can't deny DDoS in 2024?
Distributed-denial-of-service attacks

Distributed-denial-of-service attacks, more commonly referred to as DDOS attacks, are malicious attempts to disrupt traffic of a specific server, service or network by overwhelming said target or its surroundings with an abundance of internet traffic. Think of it as an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.

DDoS attacks are becoming increasingly more frequent, and there doesn't appear to be any signs of slowing down. Want to know how often these attacks really take place? Below you'll find infographics on DDoS attacks in general, as well as three recent threats associated with DDoS attacks.

If you're looking for insights in the type of DDoS attacks that are being used, expert opinions on the best prevention and remediation and much more, tune in for this episode of Threat Talks: Can't deny DDoS in 2024.

In this episode of Threat Talks we will discuss the following threats:

1. Mirai botnet
2. HTTP/2 Rapid Reset
3. Reflection & Amplification

Fact 1

According to Kaspersky's quarterly report of late 2023, **57,116** DDoS attacks were reported.

Source: Kaspersky

Fact 2

A Ponemon Institute study revealed that during a DDoS attack, every minute of downtime costs **$22,000**.

Source: Cloudbric

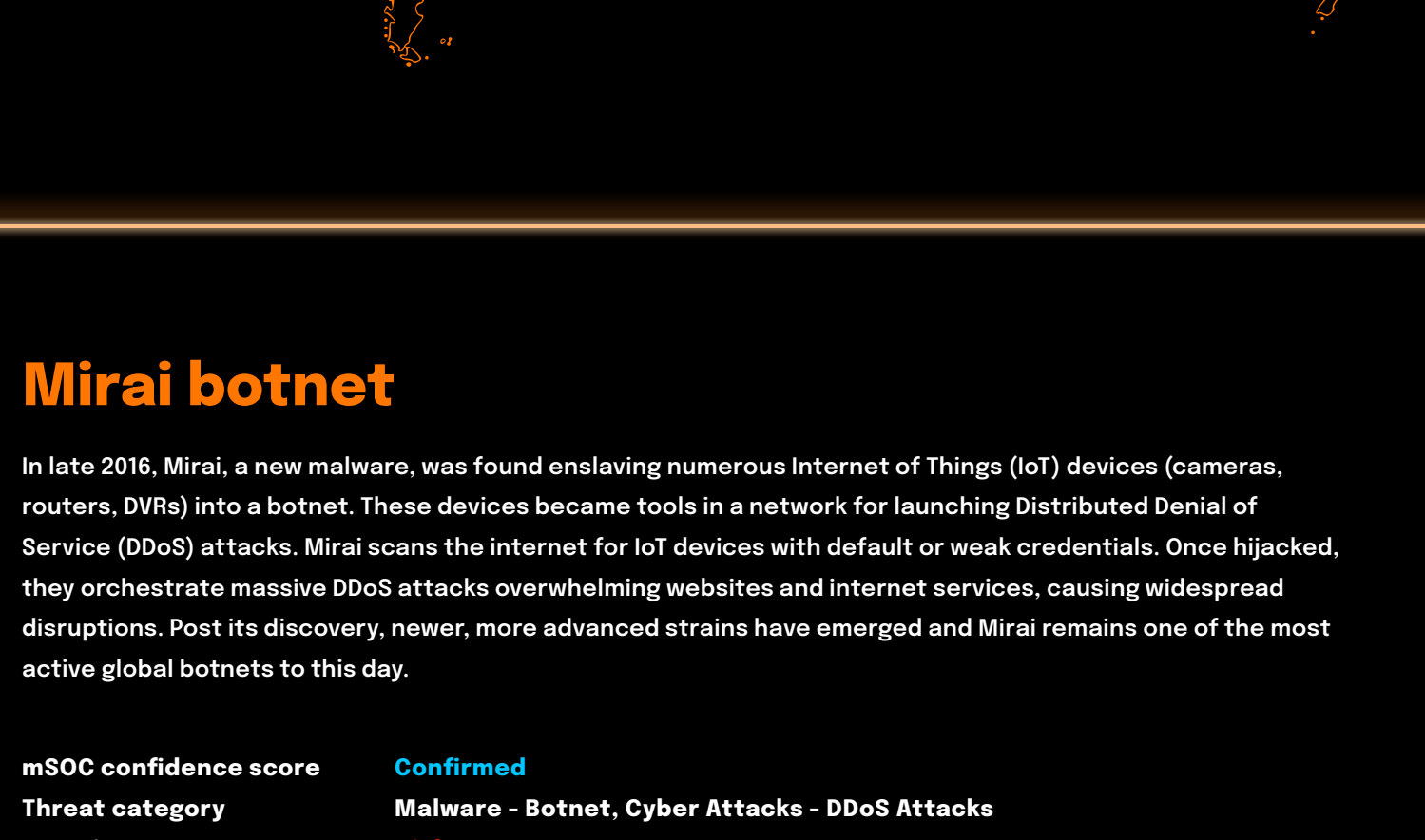
Fact 3

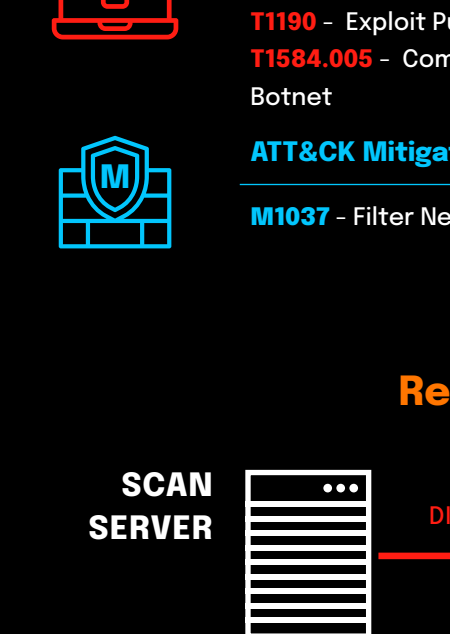
The longest DDOS attack in history occurred in 2019 and lasted **509 hours**.

Source: Kaspersky

Top Attacked Industry by Region

Source: Cloudflare





Mirai botnet

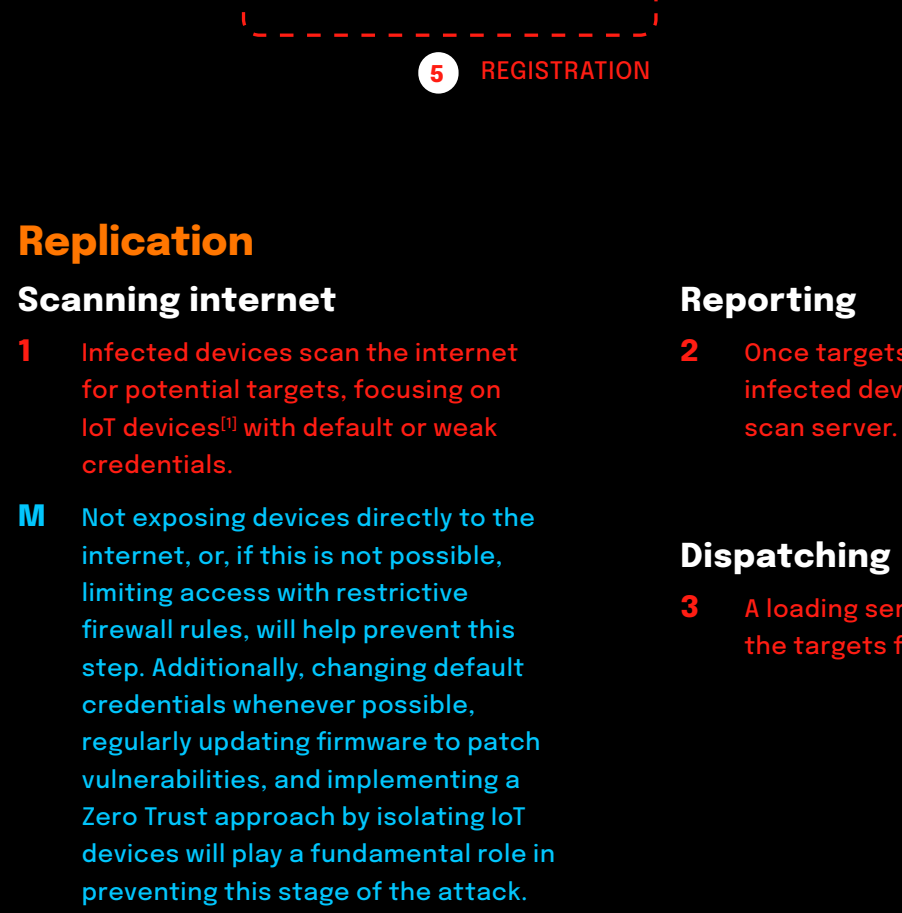
In late 2016, Mirai, a new malware, was found enslaving numerous Internet of Things (IoT) devices (cameras, routers, DVRs) into a botnet. These devices became tools in a network for launching Distributed Denial of Service (DDoS) attacks. Mirai scans the internet for IoT devices with default or weak credentials. Once hijacked, they orchestrate massive DDoS attacks overwhelming websites and internet services, causing widespread disruptions. Post its discovery, newer, more advanced strains have emerged and Mirai remains one of the most active global botnets to this day.

mSOC confidence score Confirmed
Threat category Malware - Botnet, Cyber Attacks - DDoS Attacks
Severity High

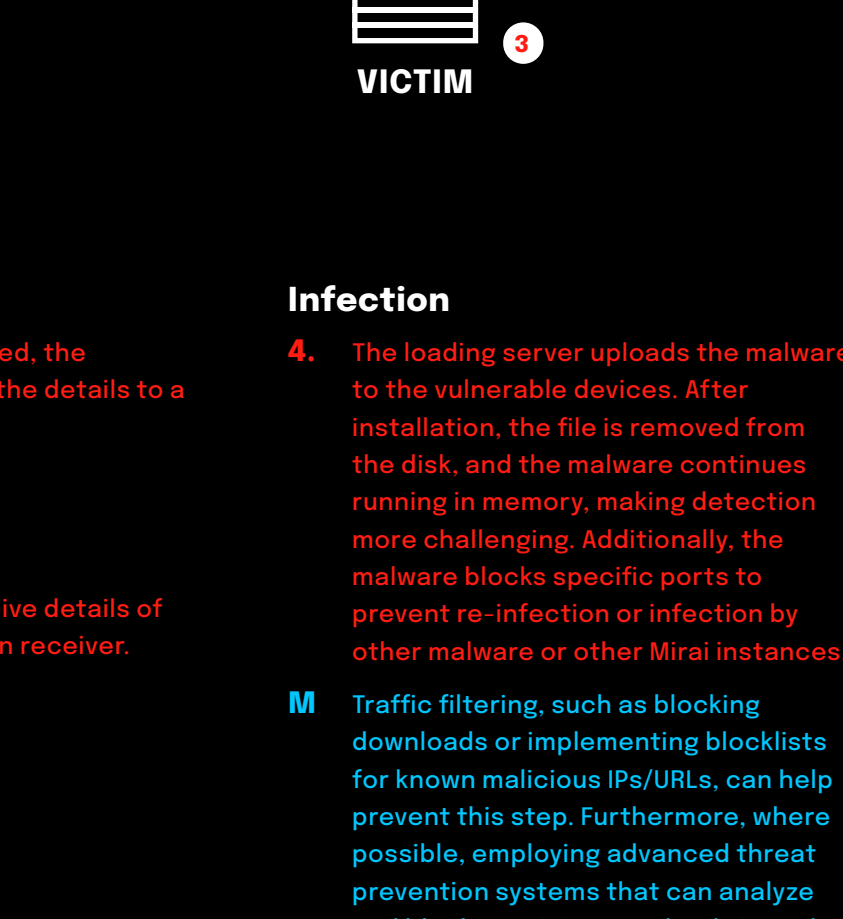
ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1190 - Exploit Public-Facing Application T1584.005 - Compromise Infrastructure: Botnet	Exploiting IoT device weak credentials	Fileless Malware	Low	Any, Individuals

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1037 - Filter Network Traffic	Public facing access	Network logs	Medium	Any, Cybercriminal, Hacktivist

Replication



Attack



Replication

Scanning internet

1 Infected devices scan the internet for potential targets, focusing on IoT devices[1] with default or weak credentials.

M Not exposing devices directly to the internet, or, if this is not possible, limiting access with restrictive firewall rules, will help prevent this step. Additionally, changing default credentials whenever possible, regularly updating firmware to patch vulnerabilities, and implementing a Zero Trust approach by isolating IoT devices will play a fundamental role in preventing this stage of the attack.

Reporting

2 Once targets are identified, the infected devices report the details to a scan server.

Dispatching

3 A loading server will receive details of the targets from the scan receiver.

Infection

4. The loading server uploads the malware to the vulnerable devices. After installation, the file is removed from the disk, and the malware continues running in memory, making detection more challenging. Additionally, the malware blocks specific ports to prevent re-infection or infection by other malware or other Mirai instances.

M Traffic filtering, such as blocking downloads or implementing blocklists for known malicious IPs/URLs, can help prevent this step. Furthermore, where possible, employing advanced threat prevention systems that can analyze and block suspicious payloads in real-time can further strengthen defenses.

Registration

5. Newly infected devices register with the command and control server, becoming part of the botnet[2]. They then start scanning the internet for new targets, as explained in step 1, leading to exponential growth of the botnet.

M Implementing dynamic blocklists for known malicious Command and Control servers or malicious IPs can help prevent this step. Additionally, monitoring outbound traffic for suspicious behavior, such as internet scanning, is essential to detect compromised devices that are actively seeking new targets, indicating that they are part of a botnet."

Attack

Command and Control

1 The attacker utilizes the command and control server to send commands to the botnet, including information about the target.

M Modern firewalls and Intrusion Prevention Systems (IPS) are able to recognize Command and Control (C2) traffic and block this, still this heavily depends on how the C2 traffic is being sent.

Attack Execution

2 Upon receiving the commands, the botnet initiates the attack by sending packets to flood the target, following the specified attack pattern.

M Traffic monitoring and health check tools will help detect attacks such as DDoS in time. Implementing GEO blocking may help reduce the size of the attack. Some firewalls have features to combat these kinds of attacks by implementing DDoS protection functionalities. Fine-tuning firewall settings and implementing load balancing can also be helpful. Services like Cloudflare offer solutions to help mitigate these attacks and can help preventing downtime.

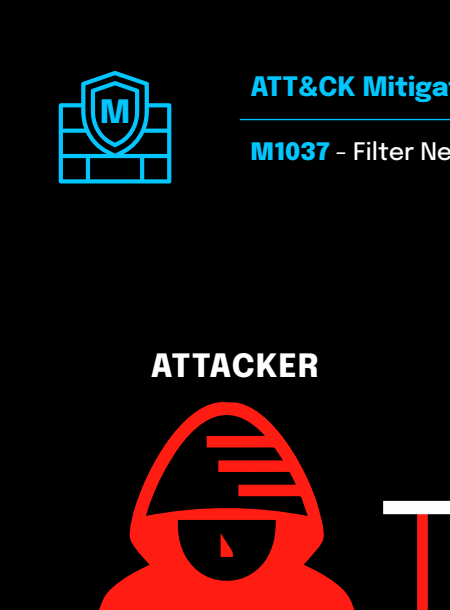
DDoS

3 A successful attack results in a denial of service, rendering the target unreachable or causing it to crash.

M Having redundant systems and backup strategies in place is essential for maintaining operations and preventing downtime.

[1] IoT, which stands for the Internet of Things, refers to everyday objects that are connected to the internet and capable of sending and receiving data. These devices can communicate autonomously with each other. Examples include common household items like smart thermostats, home security cameras, and smart lights, as well as specialized enterprise devices such as certain medical equipment and manufacturing tools.

[2] A botnet is a network of computers or other internet-connected devices that have been infected with malware, allowing a hacker to control them. These infected devices, called "bots," can be used together to perform tasks like sending spam emails, stealing data, or launching attacks on websites, often without the owners' knowledge.



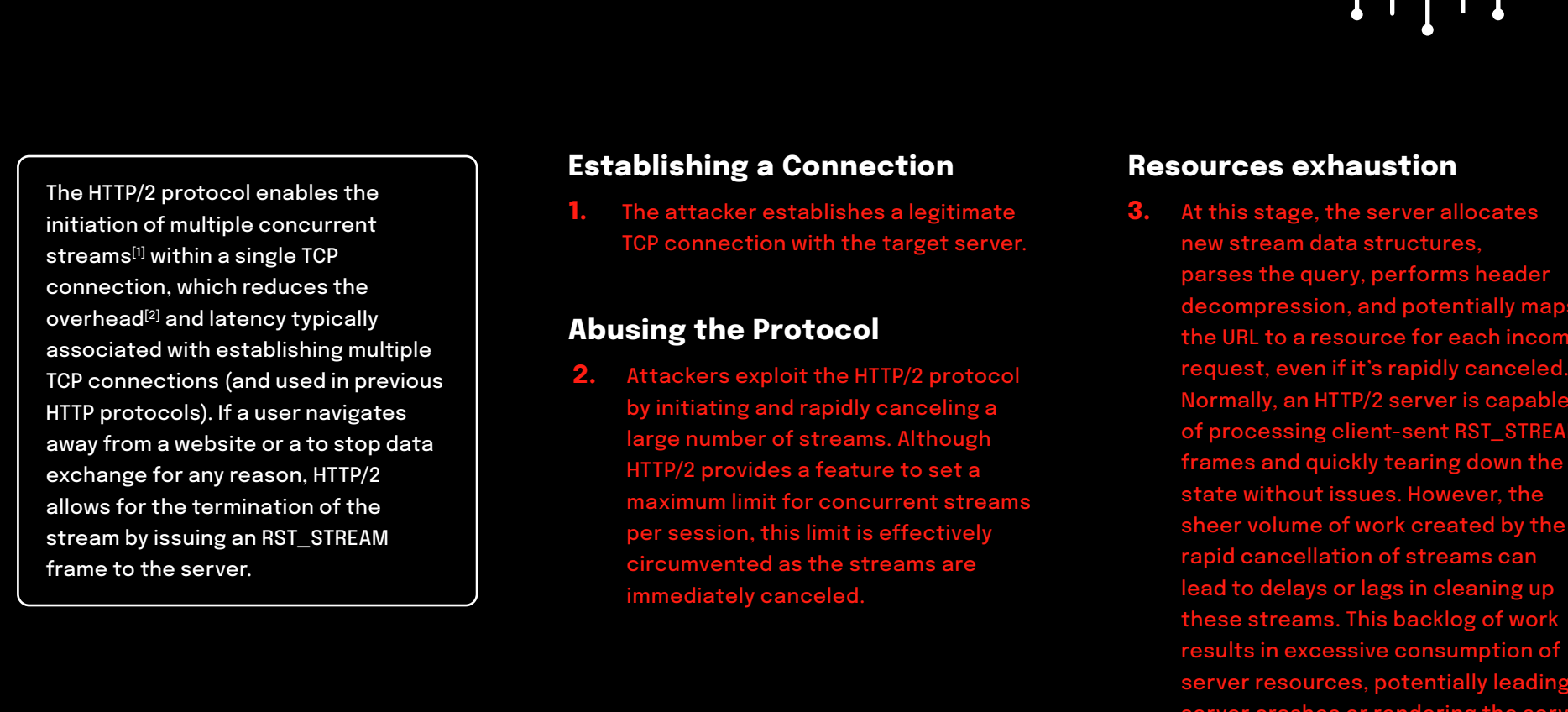
HTTP/2 rapid reset

In 2023, a new DDoS attack technique, HTTP/2 Rapid Reset, emerged, leveraging a feature of the HTTP/2 protocol (CVE 2023-44487). This method enables attackers to generate substantial traffic with relatively small botnets. It involves rapidly resetting HTTP/2 streams, causing a flood of requests that overwhelm targeted servers and websites. This attack is a significant threat to modern web servers using HTTP/2, exploiting the RST_STREAM frame of the protocol. Attackers manipulate this frame to rapidly open and close streams, overloading server resources.

mSOC confidence score Confirmed
Threat category Cyber Attacks - DDoS Attacks, Vulnerability disclosure - CVE
Severity High (CVSS score 7.5)

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1498 - Network Denial of Service	Exploiting HTTP/2 Protocol	IP spoofing, Botnet use	Medium	Any, Enterprises, Government, Military

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1037 - Filter Network Traffic	Public Facing Access	Network traffic logs, Health monitoring	High	Any, Cybercriminals, Hacktivists



The HTTP/2 protocol enables the initiation of multiple concurrent streams[1] within a single TCP connection, which reduces the overhead[2] and latency typically associated with establishing multiple TCP connections (and used in previous HTTP protocols). If a user navigates away from a website or a to stop data exchange for any reason, HTTP/2 allows for the termination of the stream by issuing an RST_STREAM frame to the server.

Establishing a Connection

1. The attacker establishes a legitimate TCP connection with the target server.

Abusing the Protocol

2. Attackers exploit the HTTP/2 protocol by initiating and rapidly canceling a large number of streams. Although HTTP/2 provides a feature to set a maximum limit for concurrent streams per session, this limit is effectively circumvented as the streams are immediately canceled.

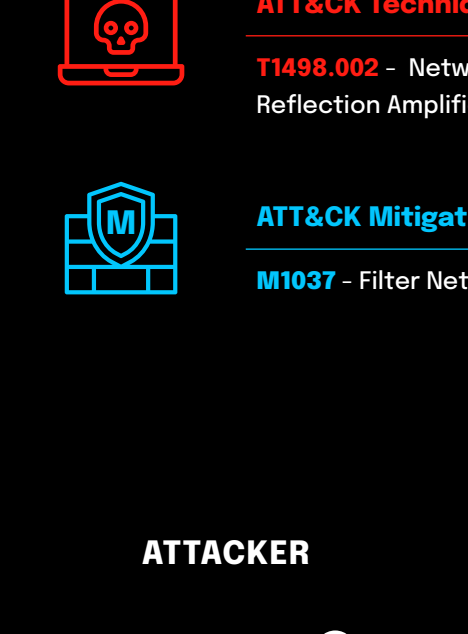
Resources exhaustion

3. At this stage, the server allocates new stream data structures, parses the query, performs header decompression, and potentially maps the URL to a resource for each incoming request, even if it's rapidly canceled. Normally, an HTTP/2 server is capable of processing client-sent RST_STREAM frames and quickly tearing down the state without issues. However, the sheer volume of work created by the rapid cancellation of streams can lead to delays or lags in cleaning up these streams. This backlog of work results in excessive consumption of server resources, potentially leading to server crashes or rendering the server unreachable.

M. Implementing health checks and server resource monitoring can alert administrators before resources are exhausted. Providers like Cloudflare offer solutions to guard against these kinds of attacks.

[1] A stream is an independent bidirectional sequence of frames exchanged between the client and the server (e.g., HTML content, CSS file, JavaScript file, etc.).

[2] Additional time and resources required to set up and maintain multiple TCP connections.



Reflection and Amplification DDoS attacks

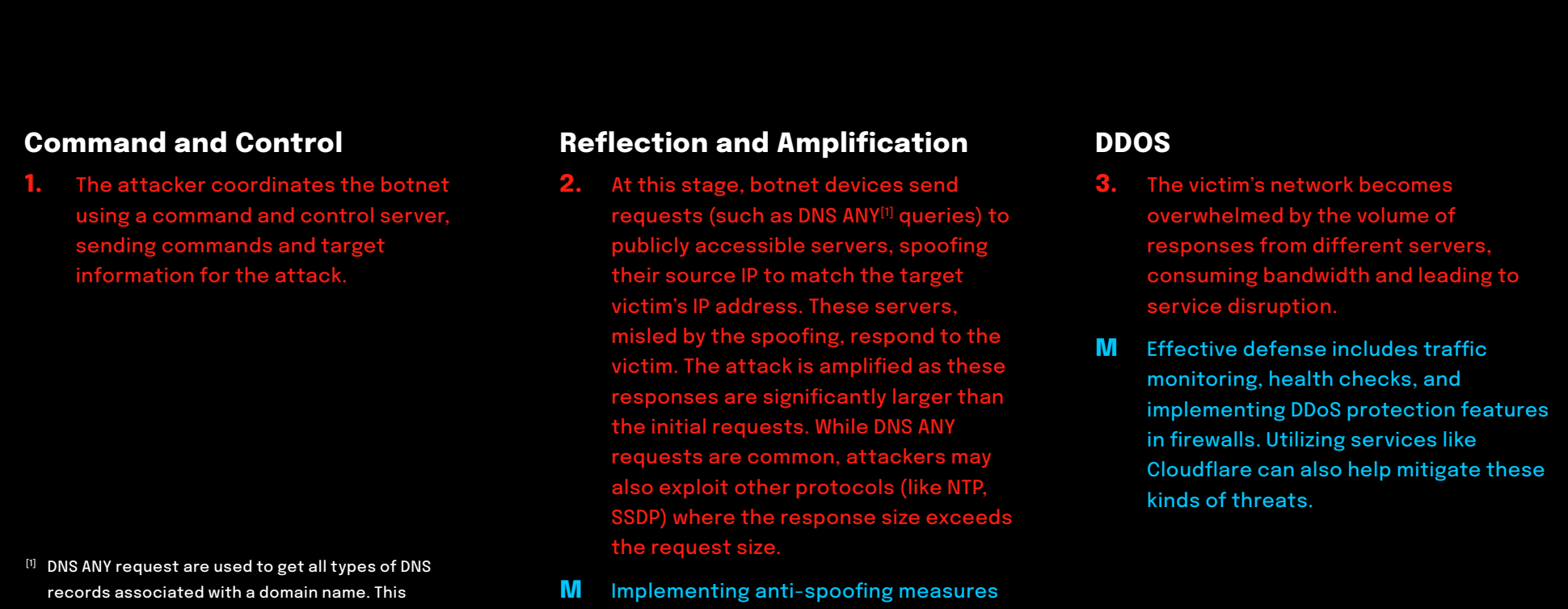
Reflection and Amplification DDoS attacks have become a prevalent threat in the cyber landscape. These attacks exploit the combination of reflection techniques and amplification tactics to generate massive traffic volumes, overwhelming target systems. In a reflection attack, attackers spoof the target's IP address and send requests to multiple servers (reflectors), which then respond to the target's IP. Amplification occurs when these responses are significantly larger than the requests, multiplying the volume of traffic directed at the victim.

These kind of attacks commonly exploit protocols such as DNS, NTP, and SSDP, which can respond with much larger payloads compared to the initial request.

mSOC confidence score Confirmed
Threat category Cyber Attacks - DDoS Attacks
Severity Critical

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1498.002 - Network Denial of Service - Reflection Amplification	Exploiting normal functionality of protocols (DNS, NTP, SSDP)	IP spoofing, Botnet use	Medium	Any, Enterprises, Government, Military

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1037 - Filter Network Traffic	Public Facing Access	Network traffic logs, Health monitoring	High	Any, Cybercriminals, Hacktivists



Command and Control

1. The attacker coordinates the botnet using a command and control server, sending commands and target information for the attack.

Reflection and Amplification

2. At this stage, botnet devices send requests (such as DNS ANY[1] queries) to publicly accessible servers, spoofing their source IP to match the target victim's IP address. These servers, misled by the spoofing, respond to the victim. The attack is amplified as these responses are significantly larger than the initial requests. While DNS ANY requests are common, attackers may also exploit other protocols (like NTP, SSDP) where the response size exceeds the request size.

M Implementing anti-spoofing measures can prevent your devices from being used in the attack if they are part of a botnet. Restricting or disabling responses to queries such as DNS ANY can reduce the risk of servers being used as amplification reflectors.

DDOS

3. The victim's network becomes overwhelmed by the volume of responses from different servers, consuming bandwidth and leading to service disruption.

M Effective defense includes traffic monitoring, health checks, and implementing DDoS protection features in firewalls. Utilizing services like Cloudflare can also help mitigate these kinds of threats.

[1] DNS ANY request are used to get all types of DNS records associated with a domain name. This includes records such as A (address), MX (mail exchange), NS (name server), SOA (start of authority), TXT (text), and more. Since the response to an ANY query can be significantly larger than the query itself, attackers send these queries to multiple DNS servers which then send all their records to the target, overwhelming it with traffic.

Taxonomy

ATT&CK Technique
Which technique of the MITRE ATT&CK framework does the threat correspond to.

ATT&CK Mitigation
Which mitigation of the MITRE ATT&CK framework can be applied.

Attack Strategy
Plan devised by the attacker to exploit specific system vulnerabilities.

Attack Vector
What is the primary method of attack.

Evasion
Tactics used by the attacker to avoid detection or bypass security.

Detection
Mechanism to identify malicious activities or system anomalies.

Complexity
How easy it is to exploit the vulnerability or carry out the attack.

Threat Level
How severe the threat is.

Target Type
The category of organization that may potentially be targeted.

Threat Actor Type
What type of threat actor may be involved.

CONTACT US

mSOC score explanation:
We assign scores to both our sources and the news items. Sources are scored on a numeric scale ranging from 0 (untrustworthy) to 5 (verified), while news items are scored with a letter, ranging from E (unreliable) to A (reliable). By considering the scores of both the source and the news item and the quality of the available information, we classify the overall reliability into three categories: Confirmed, Verified, and Credible. Interested in learning more about our reliability scoring system for sources and news items? Our Threat Intelligence team would be happy to walk you through our procedure, so please don't hesitate to reach out.

threat-talks.com

ON2IT ZERO TRUST INNOVATORS amsix