TIR-20250611 Understanding and Mitigating Modern DDoS Attacks

6/11/2025

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

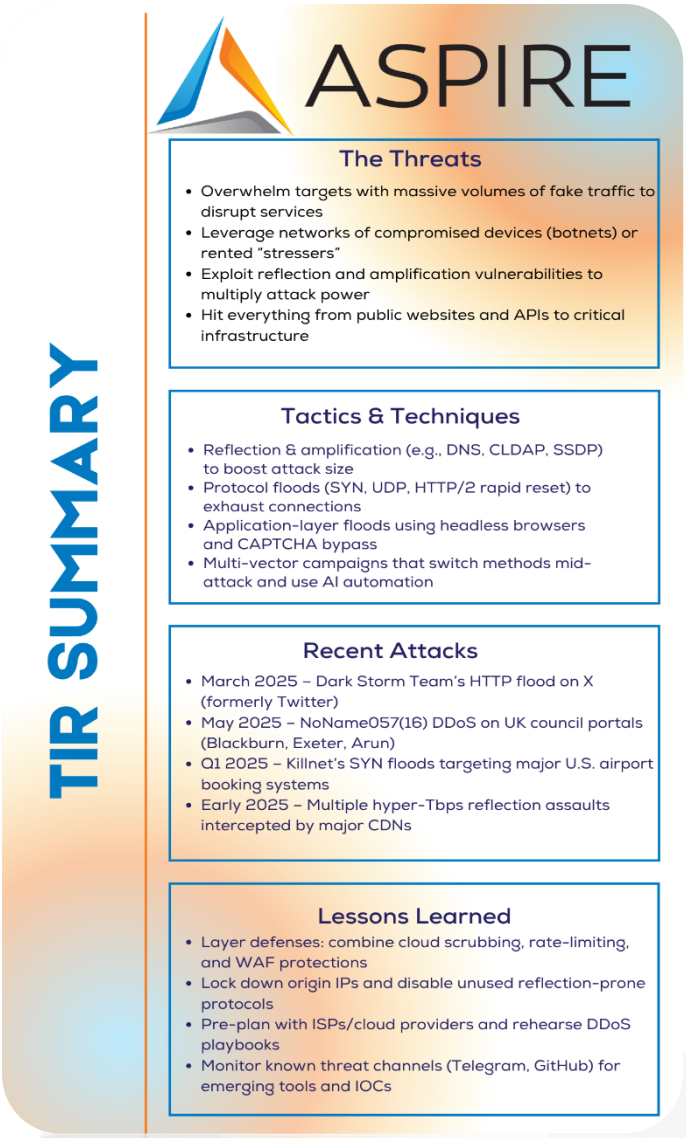
Executive Summary

In the first quarter of 2025, organizations experienced a high volume of Distributed Denial of Service (DDoS) attacks. Cloudflare blocked 20.5 million attacks, a staggering 358% year-over-year increase and a 198% spike from the previous quarter. Nearly 700 attacks exceeded 1 Tbps or 1 Bpps, averaging eight hyper-volumetric assaults daily. DDoS attacks are no longer just about flooding bandwidth; they're now calculated disruptions meant to exploit weaknesses at every layer of an organization's infrastructure.

The surge in DDoS activity is being driven by a mix of real-world problems. There are too many unsecured IoT devices, widespread use

of proxy-based botnets, easy access to DDoS-for-hire services, and a spike in politically motivated attacks. Prominent attack groups such as Killnet, NoName057(16), and Dark Storm Team have executed campaigns against airports, government services, and even major social platforms. Ransomware operations are also increasingly pairing DDoS threats with data theft and extortion to pressure victims into paying a ransom.

Traditional perimeter defenses, while still necessary, are no longer sufficient. Today's organizations need a layered DDoS mitigation strategy that includes behavior-based detection, cloud-based scrubbing, and threat intelligence feeds.



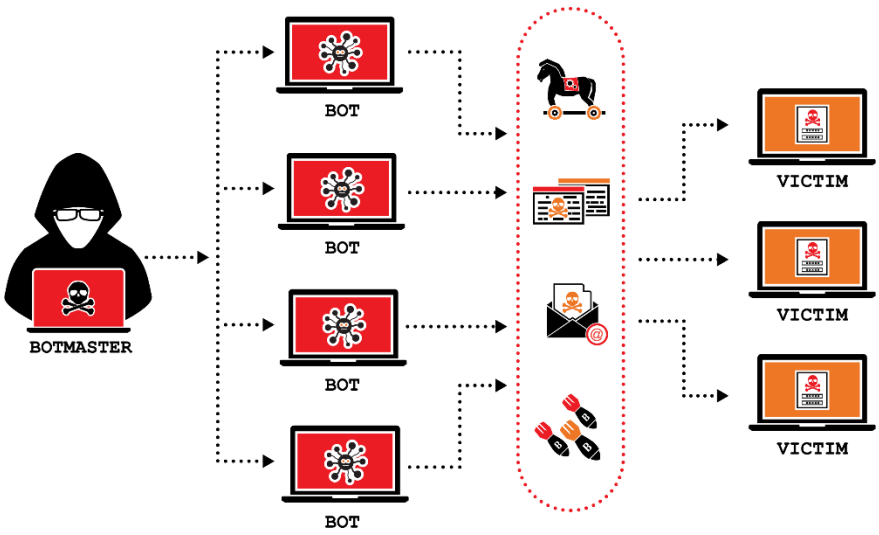
WHAT IS A DDOS ATTACK?

Before we get into DDoS attack trends, let's break down what a DDoS attack actually is. A distributed denial-of-service (DDoS) attack is a tactic used by threat actors to overload a website, app, or online service with massive amounts of traffic, with the goal of making it slow, unreliable, or completely unavailable. The traffic may look legitimate, but it's not; it's bulk fake requests, often sent through a botnet.

A botnet is a network of compromised devices that have been taken over by malware. These can include everyday items like home routers, webcams, smart TVs, and other internet-connected devices.

What makes DDoS attacks particularly hard to stop is that the traffic comes from thousands, or even millions, of different sources. That's the "distributed" part. It's not just one attacker sending requests; it's an army of devices sending a flood all at once. Because it mimics normal user behavior, filtering out the bad traffic without blocking real users becomes a challenge. These attacks don't require advanced hacking skills and can be rented as a service, making them a common tool for disruption or extortion.

Image 1: How a DDoS Attack Unfolds



Source: hashedout

Why Organizations Should Care

DDoS attacks hit where it hurts, which is availability. Even if no data is stolen, the business impact can be costly. Customers expect services to be fast and reliable; if they can't access your platform when they need to, they'll leave. The damage can erode trust and brand credibility over time.

What makes DDoS especially disruptive is the way it's used. It's not always a standalone event. In some cases, it's a smokescreen for more serious intrusions happening behind the scenes. In others, it's part of a broader extortion play where attackers threaten to keep you offline unless you pay. These tactics are being used right now against organizations across nearly every sector.

And because launching a DDoS attack doesn't require deep technical skill or high-end resources, it's become a go-to move for threat actors of all kinds. If your business depends on uptime, customer access, or digital operations, ignoring DDoS risk isn't an option.

THE 2025 DDOS LANDSCAPE

In 2025, DDoS attacks became bigger, faster, and more accessible than in previous years, with the tools behind them continuing to evolve. Mirai variants now leverage millions of poorly secured devices - those with weak passwords, outdated firmware, or no security controls. These compromised devices are quietly pulled into botnets that can launch attacks at global scale with little warning.

Cloudflare reported that CLDAP amplification attacks increased by 3,488% quarter over quarter in early 2025, while abuse of ESP protocol jumped 2,301% in the same time period. Attackers are mixing multiple techniques in a single campaign, using reflection and amplification tactics in combination with brute-force floods like SYN or UDP storms. These blended attacks overwhelm even well-prepared networks within seconds and leave little room for delay in response.

On the geopolitical front, DDoS attacks have become a routine tactic in conflicts and protests. Groups like Killnet and NoName057(16), both associated with Russian-aligned hacktivism, have repeatedly targeted government entities, airports, public infrastructure, and financial services across Europe and North America. Their campaigns are often

public, highly coordinated, and designed to create maximum disruption with minimal effort.

Making things worse, the barrier to entry has dropped even further. Telegram-based DDoS-for-hire services are thriving. For as little as $20, anyone can launch a one-hour attack using a clean dashboard, customizable tools, and rotating proxy infrastructure. These pay-to-play platforms don't require technical skill and they come fully packaged and ready to use.

Evolved Attack Techniques

Modern DDoS attacks don't rely on one method, but they use many, often in combination. Protocol manipulation is one of the biggest changes researchers have seen. HTTP/2 and HTTP/3 are being exploited through techniques like rapid reset, where connections are rapidly initiated and canceled before the server can respond, overwhelming it with unfinished tasks. This tactic sidesteps many rate-limiting protections that assume a full request cycle. Attacks using this method were reported by Google, AWS, and Cloudflare in late 2023 and into 2024, and the technique continues to be refined by threat actors.

Amplification attacks haven't gone away, they've just evolved. DNS, NTP, and SSDP reflection are still used, but CLDAP and ESP are being added to the mix. These protocols are often overlooked in standard monitoring setups, giving attackers new blind spots to exploit. Attackers are also hitting multiple services and ports at once, making it harder for defenders to identify a single source or tactic. These multi-protocol floods are not only more effective but also more unpredictable.

Application-layer attacks have also become harder to spot and stop. Instead of relying on brute force, attackers now deploy bots with realistic behavior, such as browsing sites, navigating menus, and mimicking human input patterns. They use headless browsers and automated CAPTCHA-solving to blend in with normal traffic. Combined with AI-based orchestration, attackers can run real-time feedback loops to adjust attacks on the fly, shifting tactics based on a target's response or filtering thresholds.

KILLNET AND INDUSTRY SPECIFIC IMPACT

On March 10, 2025, X (formerly Twitter) went down globally. The outage lasted less than two hours, but the impact was massive. Dark Storm Team quickly claimed responsibility, stating the attack was a response to ongoing geopolitical conflict. Security researchers observed evidence of a coordinated HTTP flood, likely amplified via residential proxies and executed through Telegram-controlled botnets. The attackers exploited a misconfiguration that allowed traffic to bypass X's front-end Cloudflare protection.

In May 2025, the group NoName057(16) launched a campaign targeting UK local councils. Websites in Blackburn, Exeter, and Arun were all hit with floods that temporarily knocked them offline. This operation coincided with the group's renewed activity against EU infrastructure, and analysts linked the campaign to a GitHub-hosted DDoS toolkit named DDOSIA. The group incentivizes contributors through a Telegram channel and a cryptocurrency reward system.

Earlier in the year, Killnet continued targeting U.S. airport websites, a campaign that began in late 2024. The attacks disrupted online booking and check-in systems at multiple hubs and were paired with propaganda messages accusing the U.S. of supporting adversaries abroad.

Industry-Specific Impact

In the **public sector**, government websites and civic services are targeted for symbolic and strategic reasons. During geopolitical tensions or public demonstrations, attackers may knock voter portals or city service websites offline, and not just to cause downtime, but to undermine public trust. The UK council incidents in May 2025 showed us how even small-scale disruptions can create public confusion and erode confidence in government systems.

In the **financial sector**, the stakes are even higher. Downtime translates directly to monetary loss, and that's exactly what extortion-focused attackers count on. Banks and fintech platforms rely on uptime for everything from transactions to trading. A brief disruption during peak hours can ripple across markets and damage investor confidence. Additionally, DDoS is increasingly being paired with ransom notes, 'Pay us, or we'll take your site down again.' And for institutions running services, that threat has weight.

Retail and **gaming** platforms face a different kind of pressure. L7 floods that target login pages, checkout flows, or multiplayer servers are often designed to interrupt high-traffic events, like product launches or gaming tournaments. The result? Revenue loss and

frustrated users who may never return. These attacks are often low-volume but precisely timed, bypassing traditional defenses that are built to stop larger-scale floods.

Healthcare remains a soft target. Many organizations in this sector still rely on legacy infrastructure that isn't equipped to handle complex DDoS attacks. A successful flood can take down patient portals, delay telehealth sessions, or disrupt internal communications. These are issues that impact both care delivery and operational continuity. With lives potentially on the line, attackers know that even a few minutes of disruption can cause outsized panic or push institutions to pay quickly just to restore order.

Conclusion

DDoS attacks aren't going away, but they are adapting. What we're seeing now is just the beginning of a shift in how these attacks are used. Instead of relying on brute force alone, attackers are getting smarter. They're using shorter, more targeted floods to cause just enough disruption to get noticed or to buy time for something else. You'll see a big wave of bogus requests, and before you know it their automated tools are already scanning for gaps and tweaking their attack.

As we move through 2025, we can expect faster attacks that are harder to trace and often tied to something bigger. This could be a political message, an extortion demand, or a cover for a breach happening in the background. Smaller organizations and supply chain partners may also become more frequent targets because they're easier to knock offline and harder to defend.

Aspire's Recommendations

- **Use multi-layered defense** - Combine cloud scrubbing services, rate-limiting, and app-layer protections. Relying on one method won't cut it anymore.

- **Protect origin infrastructure** - Prevent attackers from bypassing your defenses by locking down origin IPs and enforcing DNS restrictions.

- **Shut down unused protocols** - Disable CLDAP, ESP, and other reflection-prone protocols unless they're critical to operations.

- **Deploy behavior-based detection** - Use tools that can flag unusual browsing patterns, fake browser behavior, and scripted interaction, especially on login and checkout pages.

- **Geo-fence high-risk traffic** - Block or rate-limit traffic from regions frequently used in botnet based attacks, particularly if they're not part of your customer base.

- **Harden third-party dependencies** - Identify weak links, like unsecured APIs or CDN misconfigs, and patch them before they're used as entry points.

- **Work with your service provider** - Make sure your ISP or cloud provider knows your normal traffic baselines and can spot deviations fast.

- **Plan and rehearse** - Test your DDoS playbook through simulated incidents and include all relevant teams, not just security.

- **Track known attack infrastructure** - Monitor GitHub, Telegram, and threat feeds for indicators tied to Killnet tools like DDOSIA or botnet IPs and build automated blocking where possible.

MITRE MAP

Killnet

Initial Access	T1583.005 - Acquire Infrastructure: Botnet T1583.006 - Acquire Infrastructure: Web Services
Command and Control	T1102 - Web Service
Impact	T1499 - Endpoint Denial of Service T1499.001 - Endpoint Denial of Service: OS Exhaustion Flood T1499.004 - Endpoint Denial of Service: Application or System Exploitation T1585.001 - Establish Accounts: Social Media Accounts T1588.002 - Obtain Capabilities: Tool

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
    - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
    - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
    - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
    - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**
    - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
    - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

SUPPORTING DOCUMENTATION

Targeted by 20.5 million DDoS attacks, up 358% year-over-year: Cloudflare's 2025 Q1 DDoS Threat Report

What is a Distributed Denial-of-Service (DDos) attack? | IBM

Germany Most Targeted Country in Q1 2025 DDoS Attacks

Cloudflare mitigates record number of DDoS attacks in 2025

Cloudflare's Q1 DDoS report finds 20.5 million attacks - SAMENA Daily News

Killnet | Flashpoint

2024 State of The Threat – A Year in Review

DDoS attacks jump 358% compared to last year - Help Net Security

Russia says DDoS attack disrupts Telegram, WhatsApp | Reuters

202304051200_KillNet Analyst Note_TLPWHITE

NoName057(16) - The Pro-Russian Hacktivist Group Targeting NATO | SentinelOne

Pro-Russian Hacker Group: Noname057(16) | Radware

DDoS now a strategic threat | Cybernews

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.