digicert®

Fighting Distributed Denial-of-Service Campaigns

WHITE PAPER

Fighting Distributed Denial-of-Service Campaigns

A Distributed Denial-of-Service (DDoS) attack overwhelms a target with a flood of traffic across the internet, rendering it inaccessible to legitimate users. These campaigns have evolved from simple pranks to sophisticated operations, with motivations ranging from online political protests to criminal extortion and state-sponsored warfare. Over the decades since the first DDoS attacks, both their frequency and scale have steadily increased.

DDoS attacks differ from other types of cyberattacks. Many threats can be prevented with proactive measures like applying security patches, updating antivirus software, or configuring firewalls. However, DDoS attacks offer no direct prevention since the attacker controls the timing, size, and duration of the attack. Even the most secure systems can be overwhelmed when flooded with enough network and application traffic, and the attack continues until the perpetrators choose to stop. This changes an organization's approach to DDoS defense away from trying to stop all the malicious traffic. Rather, the goal is to mitigate sufficient attack traffic to eliminate the impact and restore system availability.

However, DDoS attackers frequently target organizations with similar profiles (e.g., in the same country or industry) in prolonged, coordinated campaigns that can last a year or more. These campaigns and the criminals and platforms behind them can be disrupted with a strong, collaborative effort from the global community of security professionals, network operators, and law enforcement agencies to mitigate attacks, dismantle infrastructure, and bring the perpetrators to justice.

Effectively combating DDoS campaigns requires broad cooperation among various stakeholders. Mitigation providers must collaborate closely with targeted organizations to develop adaptive and resilient defense mechanisms. International law enforcement agencies play a crucial role in tracing and disrupting the sources of these attacks. Malware and vulnerability researchers are pivotal in uncovering the tactics and tools employed by attackers. By fostering a multi-tiered, collaborative approach across industries and borders, we can dismantle long-running DDoS campaigns and protect digital infrastructure on a global scale.

The Lifecycle of a DDoS Campaign

A DDoS campaign typically follows a loosely structured lifecycle, beginning with the identification of vulnerabilities that serve as the foundation for the creation of a DDoS platform. These vulnerabilities, often discovered through exploit development and later Internet-scale scanning, allow attackers to devise and deploy tools capable of orchestrating large-scale disruptions.

This platform can take several forms. It might be an amplification network that uses protocols like NTP LISTMON or authoritative DNS servers to increase attack volume through reflection and amplification. Alternatively, it can consist of compromised IoT devices running custom firmware and connected to Command and Control (C2) servers, as seen with the Mirai botnet and its variants.

The platform could also be built with compromised web servers running remote PHP webshells, such as the Brobot botnet used against the US financial services industry in 2012 and 2013. Regardless of its construction, the DDoS platform transforms devices into attack nodes. These nodes collectively form a scalable, distributed bot framework capable of overwhelming targets with network traffic that requires mitigation efforts.

Once the platform is built, attackers begin by conducting tests on a range of carefully chosen targets. These initial attacks serve as a critical testing ground, allowing adversaries to evaluate the performance of their methods in real-world scenarios. Through these trials, they gather valuable insights into how their tools and attack strategies perform against different systems and defenses. By analyzing the outcomes of these tests, attackers can refine their techniques, adapt their tools, and enhance the overall effectiveness of their attack platform, ensuring it is better suited to overcome potential obstacles in future operations.

Following this testing phase, attackers compile a list of targets, which may include government websites, critical infrastructure, high-profile organizations, recognizable brands in the target country, eCommerce companies, or any entity deemed vulnerable or valuable. The campaign escalates as attackers initiate attacks against the pre-determined targets, using their platform and DDoS payloads to maximize disruption. Throughout the offensive phase, attackers closely monitor the target's availability, conducting real-time battle damage assessments to evaluate the impact of their attack and, when necessary, adapt their approach to achieve their objectives.

As the campaign progresses and the attackers achieve successes in their attacks, it often draws the attention of law enforcement and cybersecurity stakeholders. When the scale and impact of the attacks reach a critical threshold, the campaign becomes a high priority for takedown efforts. Coordinated actions from law enforcement and other government agencies frequently lead to the identification, disruption, and dismantling of the attack infrastructure, as well as arrests and legal consequences for the perpetrators wherever possible.

As law enforcement takedowns grow increasingly effective, attackers often adapt by restructuring their operations to maintain their campaigns. This process may involve adding new nodes to their attack infrastructure, developing additional exploits targeting a broader range of devices, and even recruiting additional perpetrators or collaborating with other groups of attackers to bolster their efforts.

Following significant disruptions, including arrests and the successful dismantling of their platforms, these attackers may pivot their focus towards retaliatory campaigns against entities associated with law enforcement. Frequently, this includes targeting government websites and related digital assets, aiming to undermine public trust and demonstrate resilience.

Over time, when law enforcement efforts consistently outpace the ability of cybercriminals to reconstitute their operations, the campaign inevitably begins to lose momentum. The attackers' capacity for further attacks is disrupted, and the remaining actors, the takedown "survivors," are forced to regroup. At this stage, some may cease operations entirely, deterred by the heightened risk and effectiveness of enforcement actions. However, others may adopt a more strategic approach, going underground to recruit members and build a new platform, biding their time until conditions are favorable for initiating future attack campaigns. Then, the cycle begins again.

In some cases, other cybercriminals step into the void created by the dismantling of a botnet to establish their own operations. These opportunistic actors exploit the disruption to recruit skilled individuals, repurpose existing infrastructure, and capitalize on any residual vulnerabilities left behind. By leveraging the lessons learned from their predecessors, these new actors often adopt more sophisticated techniques, enhancing their chances of evading detection. This cyclical process highlights the adaptability and resilience of the cybercriminal ecosystem, creating ongoing challenges for law enforcement and cybersecurity professionals in combating botnet operations.

Notable DDoS Campaigns and Their Responses

History provides valuable lessons in the fight against DDoS attacks. Examining past campaigns reveals the evolution of both attack vectors and defensive strategies.

Operation Ababil (2012-2013)

In 2012 and 2013, a series of DDoS attacks known as Operation Ababil targeted the U.S. banking sector. A hacktivist group calling itself "Cyber fighters of Izz Ad-Din Al Qassam" claimed responsibility, citing political motivations. The campaign used a botnet called Brobot to launch 4 waves of attacks reaching over 60 Gbps against top US financial institutions. Brobot consisted of compromised web servers running WordPress and Joomla. A large percentage of these were in Virtual Private Server farms that had the Content Management System installed by default, and that remained unmanaged.

The Response

The financial industry responded by working heavily with DDoS mitigation services. By creating industry working groups between the government, mitigation providers, ISPs, threat researchers, and infrastructure providers, Brobot infections were identified, and hosting providers worked to remove them and prevent reinfection.

This campaign highlighted the need for dedicated, high-capacity defenses beyond standard network firewalls. It also prompted greater collaboration between financial institutions and government agencies to share threat intelligence and coordinate responses. In 2016, the U.S. Department of Justice indicted seven individuals linked to the Iranian government for their role in the attacks.

The Mirai Botnet (2016-2017)

The Mirai botnet represented a significant escalation in DDoS capabilities. It was created by exploiting unsecured IoT devices, like IP cameras and home routers. In September 2016, Mirai was used in a massive 620 Gbps attack against the website of a security journalist.

Weeks later, the botnet targeted a European hosting provider, with an attack reaching a peak of 1.1 Tbps. The most disruptive Mirai attack was against a major DNS provider. This campaign reached 1.2 Tbps and caused widespread outages for some of the biggest websites on the Internet.

The Response

The Mirai attacks served as a wake-up call regarding the dangers of insufficiently secured IoT devices. The response was multifaceted.

DDoS Attack Mitigation

Network operators and mitigation vendors worked to filter the malicious traffic and developed new techniques to identify and block traffic from Mirai-infected devices and to remove the devices from the Internet.

Community Collaboration

The source code for Mirai was publicly released, allowing security researchers to analyze its workings and develop better defenses to prevent the initial infection. In particular, several standards and guidelines for securing IoT devices were created.

Law Enforcement

The creators of the Mirai botnet were eventually identified and successfully prosecuted, demonstrating that perpetrators of large-scale attacks can be brought to justice.

Code Reuse

The botnet's creators released their software source code on a hacking forum. It has since been modified and reused to build other, more potent botnets.

NoName057(16) (2022-2025)

NoName057(16) was a pro-Russian hacktivist group that emerged following the 2022 invasion of Ukraine. This group operated a volunteer-driven botnet, primarily targeting websites in Ukraine and NATO countries. Unlike the high-volume attacks of Mirai, NoName057(16) often focused on application-layer attacks, which were less bandwidth-intensive but could still effectively disable a website by exhausting its server resources. Their attacks were often coordinated through a Telegram channel, where they directed their followers and reported on their “successes.”

The Response

Industry-wide coordination played a pivotal role in countering the activities of NoName057, with significant efforts culminating in what became known as Operation Eastwood.

Law Enforcement Cooperation with Industry

Cybersecurity firms, government agencies, and international law enforcement collaborated extensively to identify and apprehend individuals believed to be associated with the group.

Botnet Tracking

Threat intelligence sharing between public and private sectors enabled the tracking of botnet infrastructures and the discovery of key nodes used for command and control purposes.

Law Enforcement Takedown

Operation Eastwood marked a milestone in law enforcement efforts, resulting in the dismantling of several critical components of the botnet and the arrest of prominent members linked to its operations in multiple countries. These actions disrupted the group's ability to organize and execute coordinated attacks and provided a template for future collaborative approaches to cybercrime prevention.

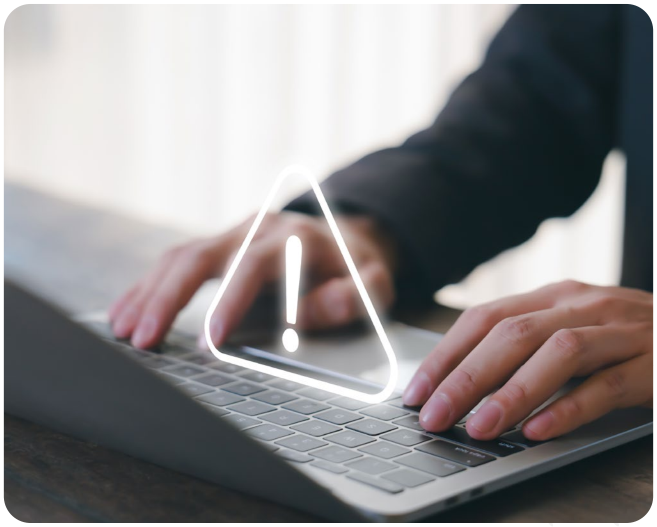
Feedback Loops in Fighting DDoS Campaigns

Defending against a large DDoS campaign isn’t about isolated mitigation efforts but about creating continuous feedback loops to gather intelligence on the attack platform and the operators behind it. Each attack provides critical data that can be analyzed to uncover their methods, infrastructure, and weaknesses. By leveraging this information, defenders can disrupt the attackers’ operations and make their campaign unsustainable. This cycle of attack, analysis, and counteraction is key to turning the tide against DDoS campaigns.

There are several information loops that need to be used to actively fight DDoS campaigns.

Attack Platform Footprint

The attack platform footprint refers to the composition and characteristics of the resources leveraged for executing DDoS attacks. This includes critical information such as the source IP addresses of attacks, types of devices used to create the DDoS platform, and the overall quantity of devices in the botnet. Source IP addresses play a pivotal role in enabling researchers to analyze command-and-control traffic, often shedding light on the operational mechanics of an attack. By examining these addresses, cybersecurity professionals can identify compromised endpoints, trace malicious activity back to its origins, and understand the bot's targets. Additionally, understanding the range and diversity of device types, which may include IoT devices, mobile phones, and servers, allows for a more comprehensive assessment of the botnet's capabilities and vulnerabilities. Mapping these footprints is essential for enhancing detection of compromised devices, streamlining incident response, and future takedown activities.



Vulnerabilities and Cleanup

If the attack platform was constructed by exploiting known vulnerabilities, researchers have the opportunity to analyze and pinpoint these weaknesses. This vital information can then be conveyed to the appropriate entities, including software vendors, device manufacturers, or Internet Service Providers (ISPs), to prevent additional devices from being compromised and added to the platform. Mitigation efforts may include the deployment of operating system patches, updated anti-malware definitions, Intrusion Detection System (IDS) signatures, or other security measures to address the specific vulnerabilities or to detect a new compromise. Additionally, collaborative efforts with organizations like Shadowserver can play a critical role in identifying susceptible systems and services, enabling timely remediation and reducing the risk of further exploitation.

Attack Techniques

Modern DDoS attack platforms are equipped with a suite of specialized techniques, all orchestrated through centralized command-and-control servers. These platforms allow threat actors to launch coordinated strikes that vary in complexity, ranging from simple volumetric floods to highly sophisticated application-layer attacks. By meticulously analyzing the attack scripts and automated tools used by these platforms, security researchers gain crucial insights into the evolving methodologies employed by attackers.

A deep understanding of these specific DDoS techniques—such as UDP reflection, SYN floods, or HTTP GET/POST floods—enables mitigation providers to refine and optimize their detection and traffic-scrubbing capabilities. This analysis allows for the development of tailored countermeasures designed to neutralize specific traffic patterns without impacting legitimate users. Furthermore, detailed examination of these attack vectors empowers organizations to recognize early indicators of compromise and anomalous traffic spikes. By identifying these precursors, potential targets can improve their proactive defense posture, ensuring they can respond promptly to mitigate service disruptions and minimize operational damage.

Indications and Warnings

Researchers play a pivotal role in identifying the early signals of DDoS attacks by actively monitoring underground forums, encrypted communication channels, and various digital platforms where threat actors congregate to discuss potential targets. These proactive monitoring efforts enable the timely detection of emerging threats, providing a critical window for security teams to implement robust mitigation strategies before an attack reaches its full, destructive potential.

Early indicators—such as sudden, unexplained increases in traffic directed toward specific systems or coordinated messaging within attacker communities regarding certain targets—serve as essential warnings that allow organizations to onramp to a mitigation provider in advance. Preparing for these specific vectors help organizations significantly minimize service disruptions and maintain operational continuity.

Attacker Mapping

Attacker mapping is a critical component of countering sophisticated cyber threats. By monitoring communications associated with attack campaigns, authorities can identify key individuals involved in their organization and execution. This intelligence allows law enforcement agencies to create targeted strategies, using Mutual Legal Assistance Treaties (MLATs) and Customs Mutual Assistance Agreements (CMAAs) to facilitate cross-border cooperation.

This international collaboration enables coordinated arrests of the creators and operators behind DDoS attack platforms. It also allows for the seizure of domains, servers, and other command-and-control infrastructure. Dismantling these essential components disrupts the operations of cybercriminal networks, making it significantly more difficult for them to resume their activities. Such coordinated efforts neutralize ongoing threats and diminish the capacity of these groups to launch future attacks. By targeting both the infrastructure and the individuals, these actions create a strong deterrent, contributing to greater cybersecurity resilience and protecting systems from potential harm.

Building a More Resilient Future

The history of DDoS campaigns demonstrates a constant cat-and-mouse game. As attackers build new platforms and methods to launch DDoS attacks, the defender communities unite to counter them. From the early SYN floods that led to best practices like ingress filtering (BCP38) to the massive botnets that spurred the development of cloud-scale mitigation, our defensive posture has been forged in the crucible of real-world attacks.

No single organization can solve the DDoS problem alone. The most effective defense is a collective one, built on several pillars:

- Proactive Defense: Implementing modern DDoS protection services that make use of extensive automation before an attack happens
- Collaborative Intelligence: Sharing threat data with peers and incident response groups to stay ahead of emerging threats
- Robust Infrastructure: Designing systems with resilience and scalability in mind, leveraging cloud mitigation platforms to clean attacks out of incoming network traffic
- Public-Private Partnerships: Working with law enforcement to disrupt the criminals and the infrastructure that enables these attacks

By learning from the past and working together, the global internet community can continue to build a network more resilient to the ever-present threat of DDoS campaigns.

About DigiCert® UltraDDoS Protect

UltraDDoS Protect is a cutting-edge solution designed to defend against the most sophisticated Distributed Denial-of-Service attacks. Utilizing advanced detection algorithms, real-time threat intelligence, and a robust mitigation framework, UltraDDoS Protect ensures that your digital infrastructure remains secure and operational, even under the most severe attack scenarios. Our solution is engineered to provide seamless protection without compromising performance, allowing businesses to focus on growth while we handle their security needs.

Take the next step toward securing your network. Contact us today to learn more about UltraDDoS Protect and how it can safeguard your mission-critical assets.

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management, to secure infrastructure, software, devices, messages, AI content and agents. Learn why more than 100,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com.