CISCO
SECURE

Solution brief
Cisco public

Web DDoS Attacks:

How to Stay Protected

Contents

Solution brief

Russia's invasion of Ukraine on February 24, 2022, initiated a new era of cyber war. In response to alleged Russian cyber aggression against Ukraine, Ukraine established the IT Army of Ukraine, recruiting western hackers volunteering to conduct attacks against Russian targets. Initially, the cyber aggressions were limited to the two parties involved in the conflict, but soon they extended to additional targets.

Pro-Russian hacktivist groups, including NoName057, the Killnet cluster, Anonymous Russia, the Passion group, and others, started attacking targets in countries that were supporting Ukraine. More recently, religious groups including Anonymous Sudan and Mysterious Team Bangladesh joined the mix by launching cyber aggressions against targets who insulted Muslims.

These cyberattacks are focused on denial of service and defacement, and they involve hospitals, airports, utilities, government, financial services, and media sites around the world. No one is immune. These attack tactics started with high-volume, network-based flood attacks. Later, they evolved to more sophisticated multivector, application-level attacks that are hard to detect and mitigate.

OpIsrael and OpsPetir

According to an alert published on April 12, DragonForce Malaysia: OpsPetir, DragonForce Malaysia, a pro-Palestinian hacktivist group located in Malaysia, has returned for a third year with rebranded operations targeting Israel.

After being absent during the return of OpIsrael 2023, the threat group posted a press release to their forum on April 11 calling for all Muslim cyber warriors, human rights activists, journalists, and Malaysians alike to join their operation that was targeting Israel. OpsPetir officially began on April 12 at 9:30 p.m. (MYT), 2:30 p.m. Israel time, and its victims list includes major banks, universities, government sites, Israeli Post, hospitals, and other key targets.

Attack methods

User Pari Malam, aka Night Pari, has released a denial-of-service tool called CyberTroopers for OpsPetir. The obfuscated Python program includes functionality to download lists of free and open proxy and SOCKS services on the internet from freeproxy-list[.]net and proxyscrape[.]com.

The collected proxy and SOCKS services are leveraged to spoof and randomize the origin of the attacks and increase the complexity of detection and mitigation for Layer 7 application attacks. By exploiting the tool's TCP, UDP, and HTTP/HTTPS flooding capabilities, the group managed to disrupt and temporarily disable online services and websites across many banks, universities, critical infrastructure, and government services to draw attention to their political statement.

Pro-Russian hacktivists deploy sophisticated techniques

With well over a year of activity, pro-Russian hacktivists are getting more experienced, and their tools are growing more sophisticated. NoName057(16) is arguably one of the more sophisticated attackers. NoName distributes bots that are run by volunteers who attack victim websites with predefined GET and POST requests, while randomizing specific variables for each request.

The attack vectors randomize information but leverage legitimate arguments and parameters recognized by the website. Differentiating legitimate requests from illegitimate requests is much harder when compared to detecting attack vectors with random arguments appended, typically used by attackers to cut through CDNs.

New and disruptive web DDoS attacks

As seen in the recent attack campaigns, attackers are leveraging multiple types and vectors of attacks as part of one campaign, combining both network and application-layer attack vectors and leveraging new tools to create sophisticated attacks that are harder, and sometimes impossible, to detect and mitigate with traditional methods.

Using these new attack tools, attackers generate new types of HTTPS Flood attacks—also referred to as Web DDoS Tsunami attacks—that are more sophisticated and aggressive. These unique attacks are higher in volume with very high requests per second (RPS). They are encrypted and appear as legitimate requests. They leverage sophisticated evasion techniques to bypass traditional app protections, such as randomizing HTTP methods, headers, and cookies, impersonating popular embedded third-party services, spoofing IPs, and other key targets. Among the application-level attack methods seen in these recent campaigns were HTTPS GET, PUSH, and POST request attacks with changing parameters, behind proxies and dynamic IP attacks. All look like legitimate requests.

HTTP/S Floods, and in particular Web DDoS Tsunami attacks, are complex to mitigate. The attacks act at Layer 7, which means that most of the attack mitigation activities, and specifically inspecting the traffic, must be done after terminating the connection and inspecting the content. The attack mitigation processes that occur after the traffic are proxied and encrypted, and all are relatively heavy and expensive to maintain, especially at scale. This makes these attacks a very attractive technique for potential offenders to disrupt or impact online businesses and services.

Why current protections are ineffective

The move toward encrypted attacks and the increase in the scale and sophistication of these attacks raises the bar needed for detection. These changes essentially render network-based DDoS mitigation tools, as well as traditional on-prem and cloud-based Web Application Firewall (WAF) solutions, ineffective against these attacks.

Network-based DDoS protection solutions are simply unequipped to detect and accurately mitigate application-layer DDoS attacks. Detecting and mitigating such attacks require decryption of the attack traffic and deeper inspection into the L7 headers. As such, these attacks would go undetected by network-based DDoS protection solutions.

A standard WAF—whether on-prem or cloud-based—is an effective tool to protect applications from standard web-based threats (mainly OWASP Top-10). That said, it is failing to protect against these L7 DDoS threats for the following reasons:

Scale: The rate of some of these attacks, measured by RPS, is reaching new heights. Over the past year, several multimillion RPS attacks were observed by multiple third parties and publicly disclosed. The rates and volume of traffic are multiple orders of magnitude above the capacity of the on-prem solution.

In addition, if the on-prem WAF is actually an Application Delivery Controller (ADC) with integrated WAF, then the task is even more complex. This is because the ADC will be maxed out by trying to terminate and decrypt millions of new requests per second, not to mention apply any security inspection. As a result, the WAF/ADC itself will be overwhelmed by the attack and ALL the services behind it will fail—not only the attacked URL/domain/application. In this case, adding more capacity to the WAF will not help the situation as the attackers can always gain more RPS power by various means available to them.

Attack sophistication: These Layer 7 DDoS attacks appear as legitimate traffic requests and are constantly randomized (dynamic IPs and other parameters). As such, there is no predefined signature or a rule-based mechanism to provide based on a connection because the requests appear legitimate and do not contain any specific bad arguments. Therefore, only behavioral-based algorithms with self-learning and auto-tuning can cope with detecting and mitigating such attacks.

Morphing attacks: The dynamic nature of these new threats—the frequency in which they change and randomize vectors, source IPs, and other parameters, and sustain these changes over a long period of time—is unprecedented. To protect against such attacks, organizations need solutions that can quickly adapt in real time to the attack campaign. A standard on-prem or cloud-based WAF is not able to provide that.

The human factor: The sophistication of attack campaigns requires having security experts that can handle the complexity of the attacks and ensure the quality of protection is not compromised during an attack. Self-managed teams, limited in personnel, tools, and budgets, cannot cope with a 24x7 attack campaign. Also, on-prem tools are mainly rule-based and require definition of new rules for mitigation. The time it takes to analyze the attack and deploy a rule means significant downtime—lasting from minutes to hours—in every iteration of the attack. All of this and the continuous morphing of the attack result in continuous downtime.

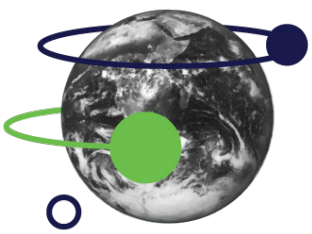
On top of this, additional traditional mitigation methods will not be successful in mitigating these attacks. Solutions that leverage rate-limiting techniques will not be able to accurately distinguish attack traffic from legitimate traffic and will block legitimate traffic. Similarly, blocking traffic based on the geographic location of its source (also known as geo-blocking) would be ineffective as the attacks leverage botnets that are globally distributed and often placed in the same country as the target itself.

What you need to stay protected

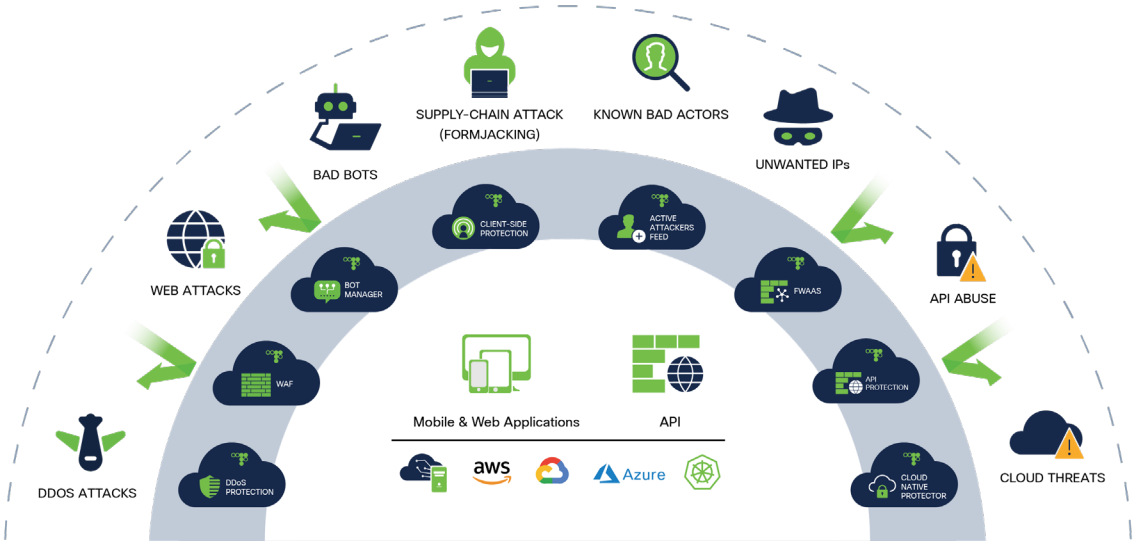
Comprehensive 360-degree cloud application protection

To protect against these new campaigns, organizations need to opt for a comprehensive, adaptive cloud application protection service—one that keeps them protected against threat vectors as the business grows and applications evolve, while eliminating management overhead and enabling the fastest time to protection.

Cisco® Secure Cloud WAF Protection is an industry-leading application protection solution. It combines best-of-breed WAF, bot management, API protection, client-side protection, and Web DDoS protection in a single solution. Secure Cloud WAF Protection is backed by a global Emergency Response Team (ERT)[1], which provides fully managed, comprehensive protection when under attack.



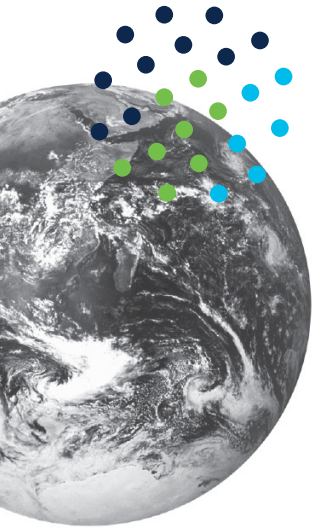
[1] Secure Cloud WAF Protection, Secure Cloud DDoS Protection, and Emergency Response Team services are provided through Cisco's global OEM partnership with Radware.



New advanced protection for web DDoS attacks

As part of Cisco Secure Cloud WAF Protection, web DDoS protection is uniquely designed to protect against newly emerging web DDoS Tsunami attacks that seek to overwhelm servers and load balancers with high RPS. Web DDoS protection, which is available in both Cisco Secure Cloud WAF Protection and Cisco Secure Cloud DDoS Protection, provides customers with advanced protection at the scale needed to combat these new threats.

Web DDoS protection provides the following:



1.Automated, accurate detection and mitigation with minimal false positives

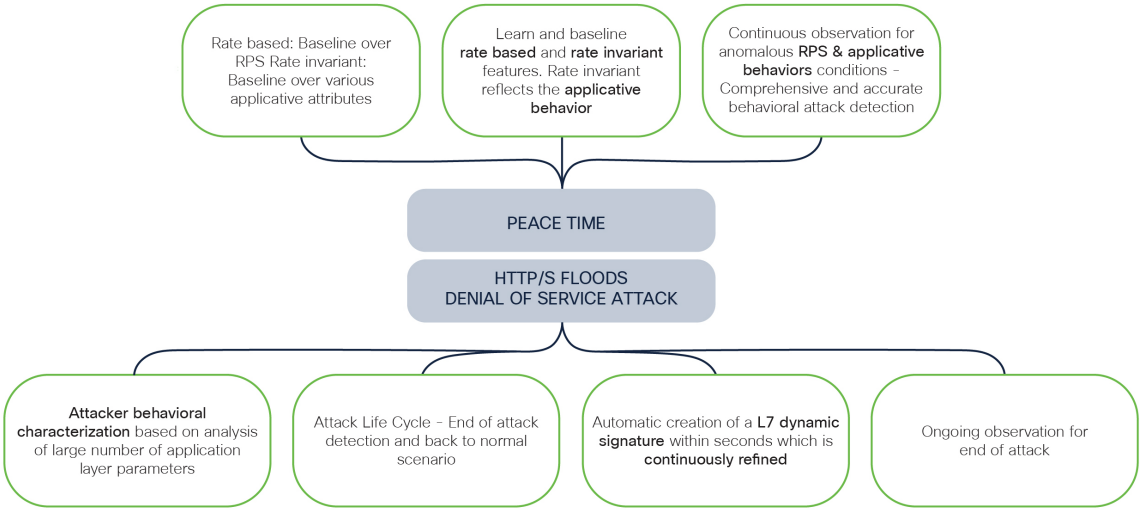
The solution leverages dedicated, behavioral-based algorithms with advanced learning capabilities designed to quickly detect and surgically block L7 DDoS attacks while minimizing false positives and not blocking legitimate traffic. In contrast to the common volumetric approach of most vendors, Cisco web DDoS protection utilizes L7 behavioral-based protection that can accurately distinguish between a legitimate surge in traffic (aka flash crowd) and a flood of attack traffic generated by adversaries and ensure that only malicious traffic is blocked—even during web DDoS Tsunami attacks.

2.Widest attack coverage protecting from the most advanced, zero-day attacks

Unique algorithms provide protection from a wide range of L7 DDoS threats including smaller-scale, sophisticated attacks, new L7 attack tools and vectors, and large-scale, sophisticated web DDoS Tsunami attacks.
The solution analyzes the advanced threats as well as their numerous variants, and it adapts to any attack patterns, randomization methods, and attack techniques (using proxies, impersonating legitimate bots, etc.).

3. Best protection for the high-RPS web DDoS Tsunami attacks

A combination of automated algorithms and high-scale infrastructure is needed to accurately protect against these high-RPS, sophisticated L7 DDoS threats.



Summary

Web DDoS attacks are increasing in scale and sophistication. As observed in the recent attack campaigns, attack tactics start with high-RPS flood attacks and then evolve to more sophisticated multivector, application-level attacks that are hard to detect and mitigate.

These new types of web DDoS Tsunami Floods are harder to detect and mitigate, making them extremely attractive techniques for potential offenders who want to disrupt or impact online businesses and services. Traditional WAF or network-based DDoS protection solutions are incapable of mitigating these L7 DDoS threats.

To protect against these new campaigns, organizations need to opt for a comprehensive, adaptive cloud application protection service that keeps them protected against threat vectors as the business grows and applications evolve, while eliminating management overhead and enabling the fastest time to protection.

Cisco's cloud web DDoS protection is uniquely designed to block these attacks—leveraging dedicated, behavioral-based algorithms to quickly detect and surgically block L7 DDoS attacks while not blocking legitimate traffic. The solution provides end-to-end application protection that allows organizations to manage and scale application security as the business grows, evolve application architectures, and expand cloud environments and services. It includes:

- **Comprehensive protection:** Multifaceted application protection suite, including WAF, API protection, L7 DDoS mitigation, and bot management.
- **State-of-the-art security:** The widest coverage against known threats and zero-day attacks based on advanced, patented, machine learning–based behavioral analysis technology that is implemented on L3 through L7 threats.
- **Reduced overhead:** Adaptive protection with automatic policy generation and 24x7 support through Radware's Emergency Response Team.
- **Centralized management and reporting:** Single location to manage and monitor the security of your applications, no matter where they are deployed.

For more information about Cisco Secure DDoS Protection, visit www.cisco.com/go/secure-ddos.