radware

White Paper

Combating Encrypted Web DDoS Threats

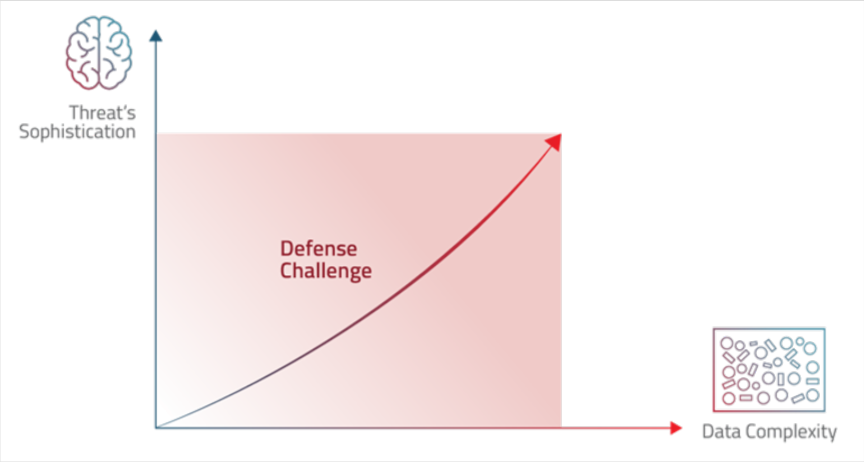
Table of Contents

Challenges

Looking at cybersecurity trends over the past five years, there are two fundamental defense challenge areas that amplify the success of attackers, especially within the DDoS attacks category: the sophistication of the systems which generate the threats, and the data complexity which allows attackers to stay hidden. Bad actors leverage both to their advantage.

Figure 1:

Threat Sophistication & Data Complexity



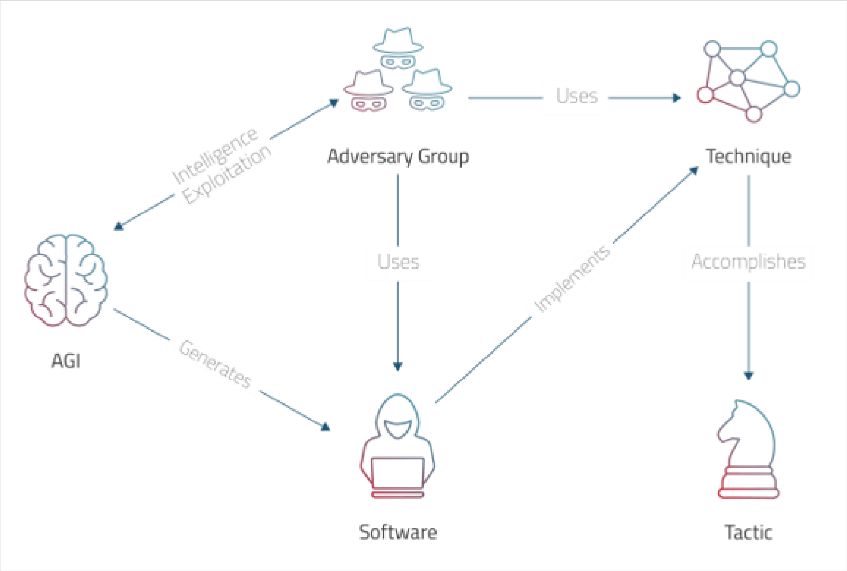
The Threats Playground

Bad actors and their "backup" organizations invest a lot of time and money to elevate the level of attack sophistication. This has become a new playground for offensive and defensive operations for individuals, organizations and nations. Consequently, we are seeing great progress in cyberattack tactics, techniques and technologies that support it. These tactics and techniques serve as a strategy, and it is evident that there is a methodical approach to execution and ongoing updates.

Below is Radware's Extended MITRE ATT&CK model, illustrating the cyberattack playground and the operations under the hood:

Figure 2:

Attack Playground



Bad actors' strategy can be explained based on the above MITRE ATT&CK diagram, extended with what we at Radware see as additional factors that are integrated into it, such as artificial general intelligence (AGI).

The adversary groups leverage hundreds of attack techniques and sub-techniques that serve their malicious intent. These are defined in the model as "Tactic".

They use software—meaning attack tools, as well as legitimate applications and systems—to implement malicious intent techniques that take them through the shortest and safest path to their goal.

The adversary groups select techniques and tools that are most effective against the target environment. This includes various environments such as enterprise networks, mobile networks, industrial control systems (ICS), cloud infrastructure and other systems.

For Web DDoS attacks, additional environmental factors are taken into consideration. These factors include the distributed nature of the protected web service and the ecosystem services supporting it, such as a content delivery network (CDN) service.

The tactic is typically defined as the attacker's intent, in the context of a DDoS threat, which the model refers to as "Impact."

Examples of Web DDoS attack techniques that bad actors use to accomplish the impact tactic include:

Dynamic Content — CDNs are highly effective for caching static content like images and scripts. However, for dynamic content, which changes frequently based on user interaction or real-time data, CDNs forward the requests to the origin server to ensure the most up-to-date content is delivered.

Attackers use this fact to make sure that the content of the attack reaches the origin server directly, thus bypassing the CDN edge network layer and exhausting the resources of the target web service much more effectively.

Origin Fetch Policies — Some CDNs allow content creators to define specific rules or policies for when content should be fetched from the origin server rather than serving it directly from the edge cache.

Attackers may glean or obtain this information, enabling them to adjust the timing and content of their attacks for maximum impact on the target web service.

Application Exhaustion Flood — Adversaries may target resource intensive features of applications to cause a denial of service, denying availability to those applications. For example, specific features in web applications may be highly resource intensive. Repeated requests to those features may be able to exhaust system resources and deny access to the application or the server itself. This process is listed as MITRE ATT&CK technique T1499.

Anonymous Proxies — Anonymous proxies serve as intermediaries between users and the internet. By masking the user's IP address and filtering incoming data, these proxies make online activities less traceable.

In general, and particularly for Web DDoS threats that cannot be easily spoofed, the use of anonymous proxies helps attackers conceal their true identity by routing the attack traffic through various proxy servers. This makes it more challenging for defenders to trace the origin of the malicious traffic and adds an additional layer of anonymity.

Vulnerability-based Techniques — Various additional attack techniques are employed to execute Web DoS impact, and among them is the exploitation of specific application vulnerabilities. One notable vulnerability known as HTTP/2 Rapid Reset allows attackers to orchestrate DDoS attacks using a relatively modest botnet infrastructure. By leveraging this vulnerability, attackers can generate enormous amounts of requests that can overload almost any application that supports HTTP/2.

These attack techniques often yield temporary effectiveness until the underlying vulnerabilities are identified and patched.

Attack Techniques Powered by AGI

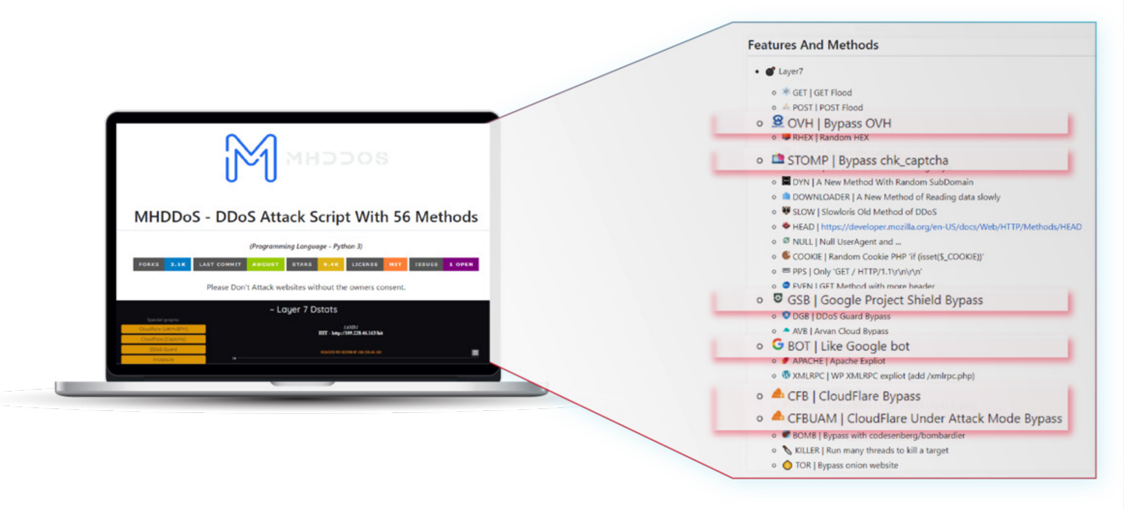
Unfortunately, the impressive progress made in the field of AGI is already being used by bad actors to elevate both the frequency and sophistication of cyberattacks.

Attack Sophistication

With respect to Web DDoS attacks, attackers are elevating detection and mitigation challenges through the following behavioral characteristics:

- **Randomization** — They often involve randomized HTTP methods and header values, so pre-defined detection and mitigation rules will be rendered ineffective.
- **Appearing legitimate** — Cybercriminals often mimic the patterns of behaviors of typical web transactions, making it challenging to differentiate between genuine and malicious activity.
- **Amplification** — Amplification involves attackers utilizing anonymous proxy networks and cloud resources to increase both the volume and frequency of their attacks.
- **Encryption** — Attacks are often concealed within encrypted TLS web traffic, so finding anomalies within the plan data becomes either impossible or would require data decryption. This would compromise privacy, requiring more compute resources and added latency.

Web DDoS tools are more accessible than ever. The MHDDoS attack tool, both well-known and effective, seamlessly integrates an array of methods to bypass common protection mechanisms. The red methods shown in red are bypass methods it uses against protection.



MHDDoS - DDoS Attack Script With 56 Methods

(Programming Language - Python 3)

Please Don't Attack websites without the owners consent.

~ Layer 7 Dstats

Features And Methods

- Layer7
  - GET | GET Flood
  - POST | POST Flood
  - OVH | Bypass OVH
  - RHEX | Random HEX
  - STOMP | Bypass chk_captcha
  - DYN | A New Method With Random SubDomain
  - DOWNLOADER | A New Method of Reading data slowly
  - SLOW | Slowloris Old Method of DDoS
  - HEAD | https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/HEAD
  - NULL | Null UserAgent and ...
  - COOKIE | Random Cookie PHP 'if (isset($_COOKIE))'
  - PPS | Only 'GET / HTTP/1.1\r\n\r\n'
  - EVEN | GET Method with more header
  - GSB | Google Project Shield Bypass
  - DGB | DDoS Guard Bypass
  - AVB | Arvan Cloud Bypass
  - BOT | Like Google bot
  - APACHE | Apache Expliot
  - XMLRPC | WP XMLRPC expliot (add /xmlrpc.php)
  - CFB | CloudFlare Bypass
  - CFBUAM | CloudFlare Under Attack Mode Bypass
  - BOMB | Bypass with codesenberg/bombardier
  - KILLER | Run many threads to kill a target
  - TOR | Bypass onion website

Malicious Intent A.I.

The impressive progress that AI-powered data engines have made in the past few years is leveraged by bad actors.

Specifically, the ability of AGI to generate and update pieces of code to create malicious-intent applications is used to accelerate the development of high-quality and sophisticated malware and bot agents.

Beyond that, AGI is leveraged to design engines that generate patterns of application transactions that look authentic. They adapt behavioral patterns based on the attack targets, considering factors such as application types and the behavior of individual identities or identity types towards the target application.

These capabilities are used broadly for social engineering-based attacks such as spearphishing, fabricating text messages (and even voice clips) to look authentic, ATO threats and Web DDoS attacks.

The ability to use AGI to create bot agents, and generate patterns of data that looks legit is changing the "playground" that defenses are required to work in. And it basically means that we must fight malicious intent AI with a more positive type of AI!

Data Complexity

Beyond the threat sophistication outlined above, there are a few major data-related trends that are used by attackers to further elevate the defense challenge.

The shift of DDoS attacks to the application layer is a major challenge that brings us into a new world of discourse.

New Universe of Discourse

As bad actors aim to conceal attacks within legitimate patterns of data, finding data patterns that differentiate between the bad and the good is a challenge. When dealing with data within the network layer, attackers have the freedom to conduct their attacks with a selection of parameters within a limited universe of discourse, i.e., layer 3 to layer 5 communication protocols' fields and values. We say "limited" because the number of parameters, and their permutations, that are available for defining the pattern of attack is at the scope of a few hundred.

The shift of attackers into the application layer alters the rules of the game, as the available data permutations defining attack patterns in the application layer content domain reaches in the hundreds of thousands and beyond.

Concealing attacks within regular application patterns has always been a challenging task for attackers. With the advancements in AI highlighted in Figure 2 and the expanded universe of discourse within the application layer, attackers now possess enhanced capabilities to better employ tools to conceal their activities.

Considering all of the above, attempting to analyze and classify a unique malicious intent pattern during an attack poses a significant challenge, both in terms of the necessary compute resources and speed. This grants attackers a significant advantage over defenders.

Data Encryption

An additional layer of complexity arises from the fact that the majority of application layer attacks today are encrypted, typically via transport layer security (TLS).

Data encryption allows attackers to hide themselves better. Bad actors understand very well that many organizations are cautious about sharing encryption keys with third-party security systems. This prioritizes the protection of privacy and keeps security systems blind to many types of attacks.

Additionally, termination of TLS typically incurs increased compute resources and potential latency in web services, both of which organizations aim to minimize.

All this contributes to the complexity of identifying and mitigating Web DDoS attacks in time to stop them.

In August 2022, Google Cloud confirmed it blocked "the largest layer 7 DDoS attack at 46 million rps," which was aimed at an unnamed Google Cloud Armor customer. A blog post revealed Google observed an increase in frequency in DDoS attacks over the past few years.

https://www.techtarget.com/searchsecurity/news/366542236/Microsoft-DDoS-attacks-caused-M365-Azure-disruptions

Attackers make use of these three main factors to challenge defenses:

Strategy

Bad actors strategically plan their operations by adapting principles borrowed from the physical battlefield. They transform and extend these principles to suit the needs of malicious cyber operations.

Defenders need to adopt a similar strategic approach, but with a superior level of sophistication, to win in this cyber war.

Intelligent Arsenal

AI, and specifically AGI, is utilized to implement attack techniques. AGI is leveraged to develop very sophisticated attack tools and generate attack patterns that pose challenges for timely detection.

Making a "too late" decision remains a pivotal factor enabling the success of cyberattacks.

Data Complexity

The shift towards application-level DDoS attacks occurred for various reasons. One of the main motivations is the integration of malicious cyber actions into a new universe of discourse: the application content layer. This expansive "universe", coupled with the fact that 99% of communication is encrypted, generates complex content patterns that are challenging to predict, allowing bad actors to effectively conceal their operations.

Behavioral-based Defense

In the broader sense, defense strategy needs to be comprehensive, which means it needs to cover attacks at all the threat layers, including network DDoS attacks, application DDoS attacks and encrypted application attacks.

In terms of protection technologies, there is no one-stop-shop for all these layers of threats. However, we have identified defense strategy principles that are very similar across the layers and follow them consistently:

Data Abstraction

Data abstraction is a crucial aspect in addressing the challenge of data complexity. Radware employs patent-based methods for data classification, particularly at the application content layer. This approach allows the derivation of high-value analytical parameters, a challenging task within a large universe of content parameters. The data classification process serves to reduce noise and false positives, amplifying the ability to effectively characterize malicious application behaviors at scale.

Real-Time Signature (RTS)

We should always remember that no two attacks are the same. Relying on static rules that represent a fixed signature to block attacks usually renders defenses useless. The RTS approach analyzes and characterizes every attack in real-time, generating dynamic signatures to effectively mitigate the ever-changing nature of cyberthreats.

Active Analytics

Passive data analytics focuses on observing and analyzing data, while active data analytics involves interacting with the data or system to extract information and potentially influence outcomes. It is crucial to assume that advanced attackers may eventually find ways to hide themselves in a manner that passive analytics processes would fail to identify. Therefore, employing active analytics methods, such as application challenge-responses, becomes necessary to compel attackers to expose their identity or malicious patterns, conceptually mirroring the investigative approach used in identifying suspect individuals.

Radware's Encrypted Web DDoS Protection

Radware offers behavioral-based encrypted Web DDoS protection, aligning with the aforementioned defense strategy principles. It automatically detects and mitigates encrypted Web DDoS attacks without the need for data decryption, ensuring full privacy preservation.

The protection system is characterized by the following key attributes:

Behavioral-Based Detection

The system incorporates an adaptive behavioral-based engine that adapts the normal behavioral patterns during non-attack times. It identifies anomalous behavior based on both rate and rate-invariant traffic parameters.

This behavioral engine enables the accurate identification of encrypted Web DDoS attacks.

Mitigation Through Real-Time Signatures

Applies classification technology to the encrypted traffic layer upon detecting an anomaly. It dynamically generates a real-time signature that adapts to the specific characteristics of the attack as it morphs, ensuring accurate and timely mitigation.

Superior Performance and Low Latency

Uses unique protection algorithms that allow it to stay agnostic to the application requests rate. It employs the latest high-grade hardware to protect against encrypted DDoS attacks at large scale without introducing unnecessary latency or impacting application performance.

No Data Decryption

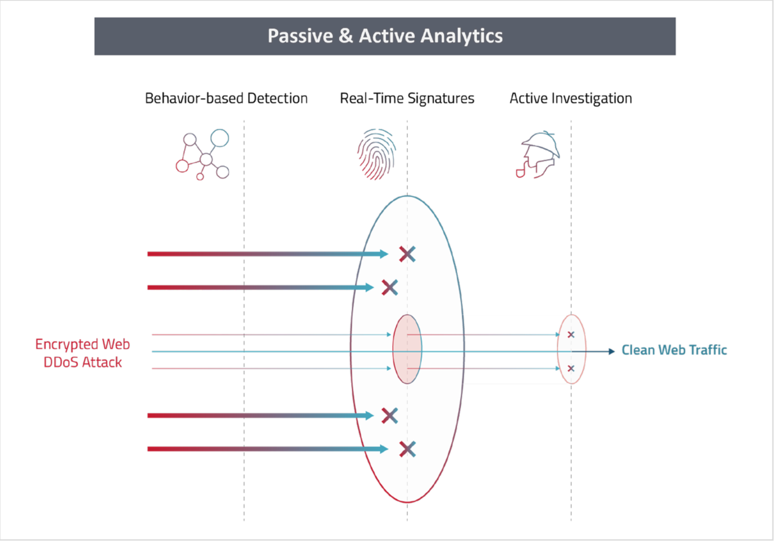
Enables detection and mitigation of Encrypted Web DDoS attacks with no decryption. This ensures the maintenance of customer confidentiality, meeting both local and industry regulatory requirements and upholding customer privacy.

The Process Behind the Promise

The system utilizes three key layers of defense, as illustrated in the figure below:

Figure 3:

Encrypted Web DDoS protection layers



Behavioral-Based Detection

The behavioral-based detection engine incorporates a data classification process that extracts rate and rate-invariant parameters from the encryption TLS layer.

Its adaptive nature allows it to learn normal behavioral patterns during peacetime, establishing baselines accordingly. Once sufficient data is collected, the engine automatically shifts into detection mode.

In this mode, it identifies deviations of the rate and rate invariant parameters from the baselines, indicating a behavioral anomaly that can be categorized as a Web DDoS threat.

High Analytical Value Data Parameters: The data classification process ensures that the system is not susceptible to false positive alarms, commonly triggered by unexpected legitimate traffic spikes, as seen in “flash crowd” scenarios. This resilience is attributed to rate-invariant parameters, which remain unaffected by application request rates.

Upon anomaly detection, a process that takes seconds, the protection system enters a characterization state. During this phase, the system activates the Real-Time Signatures engine to identify an accurate pattern for use in attack mitigation.

Real-Time Signatures

During the characterization state, a process is initiated to identify anomalous patterns known as real-time signatures (RTS) within the TLS layer. These signatures, used for mitigating the attack, are generated within seconds.

Real-time signatures technology employs a patented data classification process, transforming data elements within the TLS layer into a parametrized dimension. This transformation enables the system to effectively identify anomalous behavioral patterns within the “noisy” data associated with malicious web transactions.

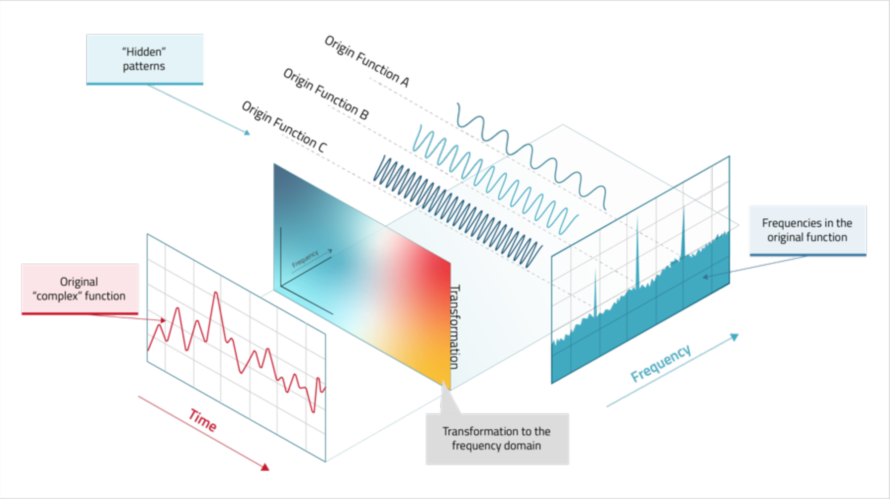
Encrypted Web traffic that matches the RTS is then filtered out until traffic towards the target web service normalizes.

To illustrate this transformation method, let’s draw an analogy to the well-known and successful Fourier Transform. This analogy will help explain how data abstraction can effectively unveil hidden patterns within complex data, pinpointing the origin of Web DDoS attacks.

The following figure illustrates the process:

Figure 4:

Data Transformation Analogy



The motivation behind this transformation involves a mathematical procedure that converts a “complex” function from the time domain into the frequency domain. In our analogy, we can liken this process to the previously described data classification process, which transforms data elements within the TLS data complexity layer into another parametrized dimension.

The transformation reveals precise patterns referred to as “hidden origin functions” in the figure. Each of these functions is described via a discrete frequency and can be considered one of the fundamental elements that compose the original complex function.

In our analogy, we can view these origins as potential RTS that unveil origin patterns within the encryption TLS layer during an attack.

The RTS classification process, having learned normal RTS patterns during peacetime, can, upon anomaly detection, differentiate between anomalous RTS patterns and genuine ones, effectively setting the final RTS accordingly, as highlighted before, without the need for data decryption.

This data abstraction technology reveals attack patterns that even attackers are not aware of, making it a very effective mitigation technology.

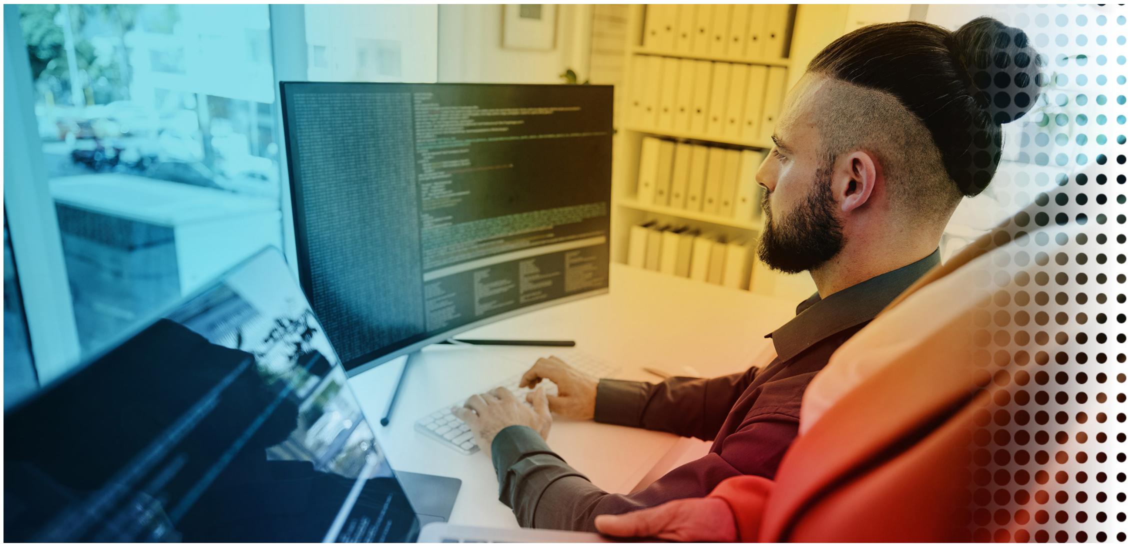
Active Analytics

As mentioned earlier, active data analytics involves interactions with the data or system to extract information and potentially influence outcomes. In situations where passive data analytics methods, such as RTSs, are insufficient for mitigation, the protection automatically switches into active analytics methods.

This involves a challenge-response process requiring the use of TLS keys for data decryption.

It’s important to note that decryption and challenge-response actions are selectively applied only to suspicious sessions during an attack, thereby minimizing the data decryption operation.

The challenge methods include various techniques such as HTTP redirect, Java-based challenges, and more. These challenges are escalated as needed to authenticate web transactions and effectively mitigate the Web DDoS attack.

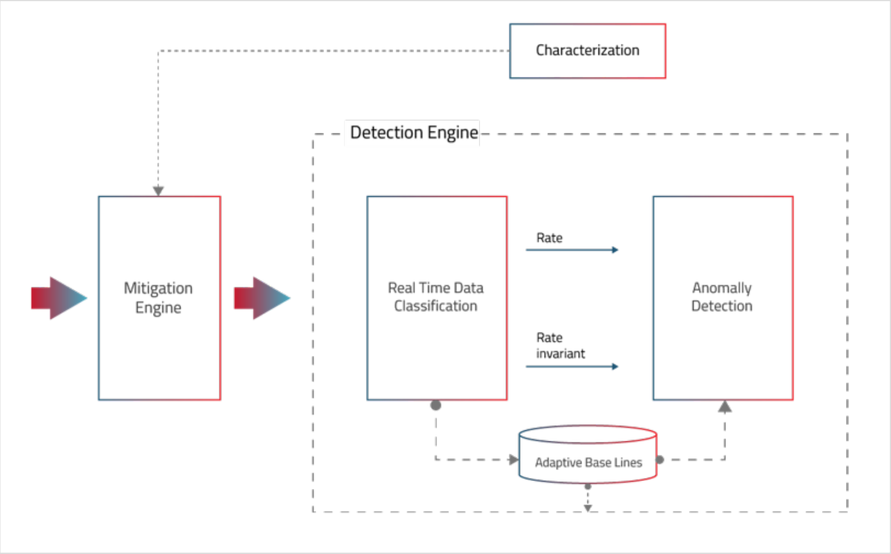


System Modules

As illustrated below, the encrypted Web DDoS protection system is comprised of the following key modules and decision-making processes:

Figure 5:

System Modules



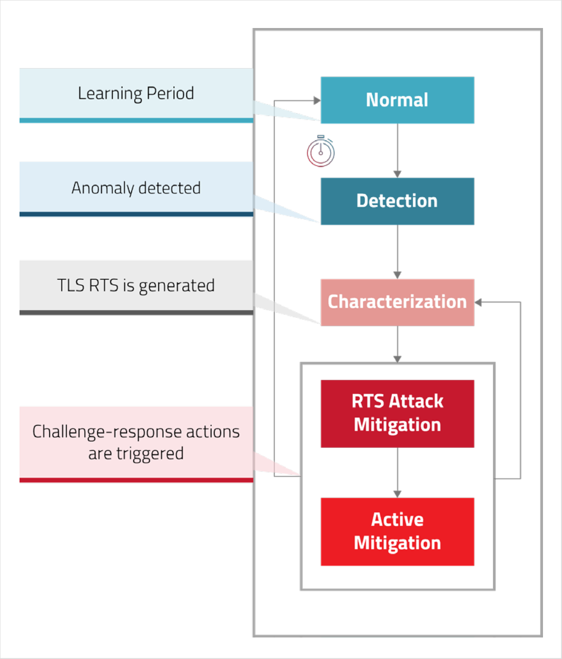
Detection engine

Real-time Data Classification — The engine extracts rate and rate invariant behavioral parameters such as:

- Rate of TLS handshakes
- Rate of TLS handshakes per TLS fingerprint
- Distribution of TLS fingerprints

TLS fingerprints are based on TLS parameters like TLS version, Cipher suites, Cipher suites length, Extension fields and values, and more.

Protection systems go through the following operational states:



Adaptive Baselines — During non-attack periods, the system adapts baselines representing normal patterns of the behavioral parameters. Rate-invariant baselines are established as Probability Distribution Functions of TLS fingerprints and other parameters.

Anomaly Detection — Once sufficient baselines are established, the anomaly detection engine assigns anomaly weights to each traffic parameter. It correlates the weights to identify anomalies indicative of an encrypted Web DDoS attack.

Characterization

Upon detecting an anomaly, learning halts and the system enters a characterization state. In this state it classifies TLS layer traffic parameters and generates real-time signatures that characterize the ongoing attack.

Mitigation Engine

This engine executes two types of mitigations actions:

- **RTS Attack Mitigation** — Blocks any transaction matching the RTSs.
- **Active Mitigation** — Applies challenge-response actions if RTS mitigation is insufficient for complete attack mitigation. The active mitigation process requires the use of TLS keys for decryption.

Closed-Feedback

The protection system automatically identifies changes in attack patterns, re-initializes the characterization state, and generates new real-time signatures for mitigating the evolving attack. Once no anomaly is detected, the system automatically terminates all mitigation actions, signaling the end of the attack.

Attack Mitigation Power

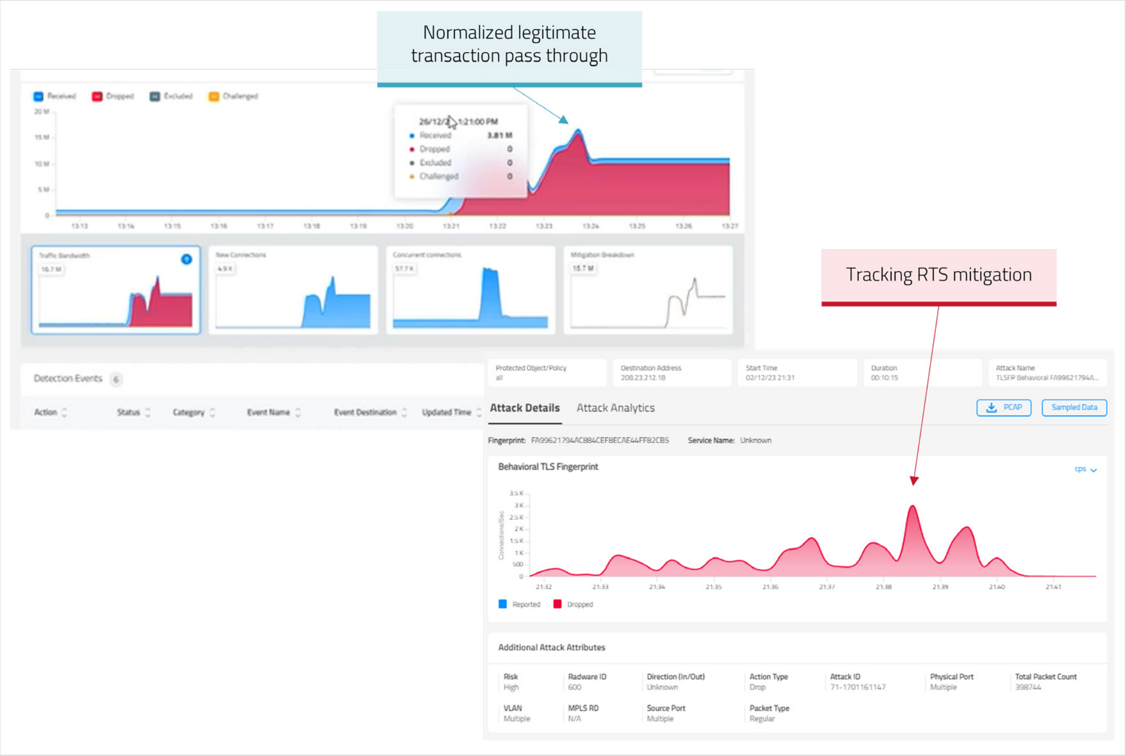
Web DDoS attacks have escalated to unprecedented levels, with attackers generating millions of requests per second, overwhelming web service infrastructures. Utilizing anonymous proxy networks and infecting a vast number of cloud and endpoint resources, malicious actors can launch powerful DDoS campaigns that impact even the most extensive web service cloud infrastructure, such as occurred with Microsoft Azure.

Countering these high-volume application-based DDoS attacks is crucial. Radware's detection and mitigation algorithms are designed to be application request rate-agnostic, enabling the protection system to mitigate encrypted Web DDoS attacks at rates exceeding dozens of millions of requests per second. This capability ensures that the protection can effectively mitigate even the largest web services sites against attacks of any size.

Security Operation

The system's security operation dashboards ensure complete visibility into the anomaly detection process, real-time signatures identified and used for mitigation, and actionable investigation dashboards that facilitate quick root-cause analysis. Security analysts can observe the effectiveness of mitigation and employ manually defined filters for proactive defense.

Below are a few examples of the security operation monitors:



Normalized legitimate transaction pass through

Tracking RTS mitigation

26/12/2 1:21:00 PM
- Received 3.81 M
- Dropped 0
- Excluded 0
- Challenged 0

Detection Events 6

Action | Status | Category | Event Name | Event Destination | Updated Time

Protected Object/Policy: all
Destination Address: 208.23.212.18
Start Time: 02/12/23 21:31
Duration: 00:10:15
Attack Name: TLSFP Behavioral FA99621794A...

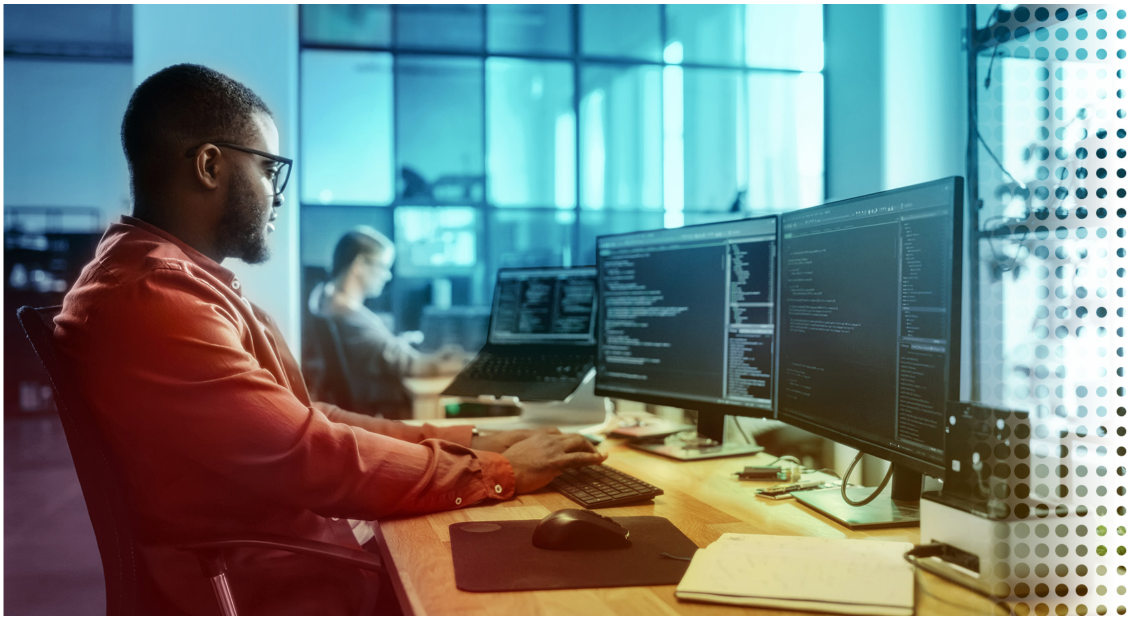
Attack Details | Attack Analytics

Fingerprint: FA99621794AC884CEF8ECAE44FF82CB5 Service Name: Unknown

Behavioral TLS Fingerprint

Additional Attack Attributes

Risk	Radware ID	Direction (In/Out)	Action Type	Attack ID	Physical Port	Total Packet Count
High	600	Unknown	Drop	71-1701161147	Multiple	398744
VLAN	**MPLS RD**	**Source Port**	**Packet Type**			
Multiple	N/A	Multiple	Regular			



Summary

Radware proudly introduces the first system designed to combat encrypted Web DDoS attack without the need for decryption.

Our patented methods empower the protection system to detect and mitigate threats at the highest scales, all while maintaining customer privacy.

Key capabilities include:

Behavioral-Based Detection

Hands-off behavioral engine accurately identifies encrypted Web DDoS attacks, ensuring effecting threat detection.

Mitigation Through Real-Time Signatures

The dynamic generation of real-time signatures adapts to the specific characteristics of the evolving attacks, ensuring accurate and timely mitigation.

Superior Performance and Low Latency

Innovative protection algorithms allow the system to remain agnostic to the application requests rate, ensuring effective mitigation for the largest web services against attacks of any size.

Upholding Customer Privacy

Detection and mitigation of encrypted Web DDoS attacks occur without decryption, ensuring the highest level of customer confidentiality. This approach aligns with both local and industry regulatory requirements.

Experience automation powered by these innovations, significantly reducing the time to resolve threats from days and hours to seconds. Our system sets a new standard for security, providing robust protection while respecting user privacy.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.