corero
[NETWORK SECURITY]

Threat Research Note

Corero Network Security

ADAPTIVE STRATEGIES IN CONDUCTING DDOS ATTACKS

Huy Nguyen & Teressa Carlin

August 22, 2024

CONTENTS

I. Introduction

Over the last year and accelerating over the last few months, the cybersecurity landscape has experienced a significant rise in the quantity and magnitude of DDoS attacks sourced from botnets.

In addition to the still prevalent Mirai botnet, which was first seen in 2016, known for its suite of attack methods, MikroTik or RouterOS-based botnets are rapidly emerging as the major threat.

The Corero Threat Research team have analyzed the mechanisms by which MikroTik routers are used to launch DDoS attacks(1), as well as the attack methods employed by the Mirai botnet(2). As noted in our previous articles, the combination of numerous bots, the robust hardware of these devices, and the capabilities of the Traffic Generator tool has enabled attackers to generate these ever-growing volumes of DDoS traffic.

Defending against DDoS indeed feels like an endless war, where each battle requires a well-thought-out strategy, tactics, and resources to succeed. The dynamic nature of these attacks, combined with the increasing sophistication of attackers, demands that organizations continuously evolve their defenses.

Understanding why attack methods change and how attackers adapt their tactics is crucial for maintaining effective defenses over time. Sun Tzu says in The Art of War **"If you know yourself but not the enemy, for every victory gained you will also suffer a defeat."**

Here we take a comprehensive look at the characteristics of classic DDoS and how attackers are now able to create more robust strategies with the tools enveloped within the Mikrotik and Mirai botnets.

II. Attack Strategies

a. Adaptive Targeting

Traditionally attacks would target one or a few individual IP addresses and DDoS mitigation solutions focused their abilities on solving these attacks. Although not ideal, if no better method of mitigation was available and attacks were just too volumetric, then remote triggered black hole (RTBH) functionality could be used upstream to direct traffic to a blackhole, as a minimum way of preventing attack traffic from saturating downstream links.

In recent times "carpet bombing," referring to attacks which target an entire subnet rather than an individual IP address, is becoming the norm, but applying RTBH to an entire subnet is much less attractive than for a single IP address. This is not an acceptable option, especially when dealing with large prefixes such as /19 or /20. In such cases, it is impractical for an organization to implement this strategy effectively.

b. Resource Saturation

Classic resource saturation in DDoS attacks:

- **High-rate flooding**
  The attack involves a huge number of packets being sent at high rate to cause CPU and memory usage of devices and servers to spike and struggle to process traffic. Some examples of high-rate flooding attacks are SYN and ACK floods where packets have a small length, or a UDP flood with no or very small payload.

- **Bandwidth saturation**
  Attackers aim to saturate the available bandwidth of the targeted victim by sending a large volume of data, trying to clog the network pipes. Links can be filled up with attack traffic, leading to degradation or loss of service. UDP floods with large packet size and reflection amplification attacks are examples of attacks that can cause bandwidth saturation.

The two graphs below show attack traffic to the same target, switched from a high-rate to high-bandwidth strategy.

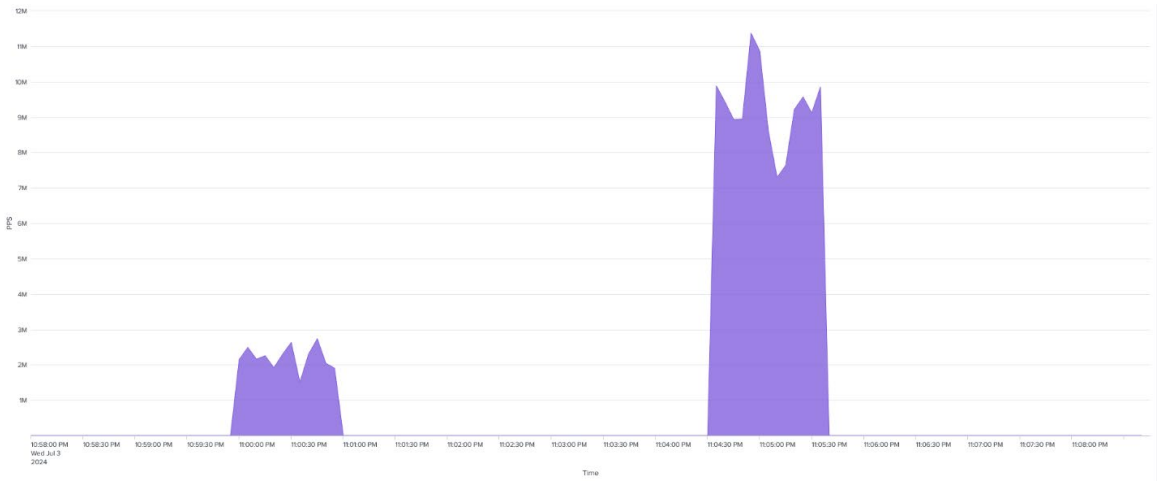

Figure 1: Attack traffic to a target in PPS

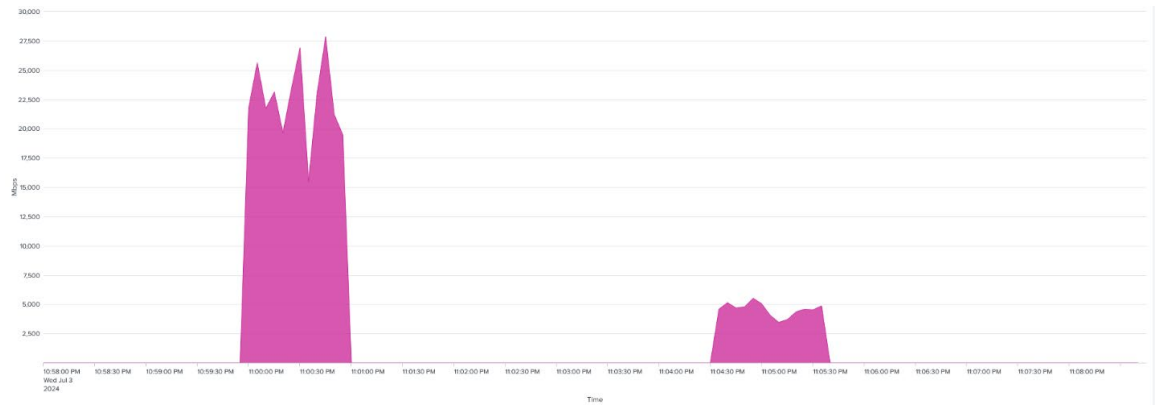

Figure 2: Attack traffic to a target in Mbps

Attackers change tactics to maximize the impact of their attacks, particularly when the initial attempts prove ineffective.

- **Switching between high-rate and high-bandwidth**
  Start with a high-rate attack and if observed that this causes minimal impact, then switch to a high-bandwidth approach and vice versa.

- **Analysis**
  Continual evaluation of the effectiveness of the attack, using metrics such as downtime or response time to gauge success.

- **Non-repetition attack patterns**
  Avoiding the same type of attack unless it has proven effective and to be resistive to defense measures.

- **Combining techniques**
  Utilizing a mix of high rate, high bandwidth and even application-layer attacks keeps defenders busy attempting to mitigate.

c. Duration

A sustained attack may be used when an attacker intends to cause significant damage and, at times, wants to demonstrate that the attack could escalate further. For instance, in a ransom DDoS, the attacker may aim to attack a victim for an extended time, causing a long downtime period and high cost to the victim, therefore increasing the likelihood that the victim will agree to pay the ransom demand. These attacks could last hours, days or even weeks.

Figure 3: Long duration attack

In other scenarios, the attacker may seek to avoid detection by launching burst attacks lasting only in a short amount of time. If the system resolution is insufficient or monitoring interval is infrequent, these attacks may not appear in charts, graphs, or monitoring systems. When the system cannot detect such attacks, then mitigation becomes challenging. This strategy causes victims to spend more time identifying the attack and developing mitigation mechanisms to defend against it. By the time the victim reacts effectively, the attacker may have already achieved their purpose – disrupt services momentarily.

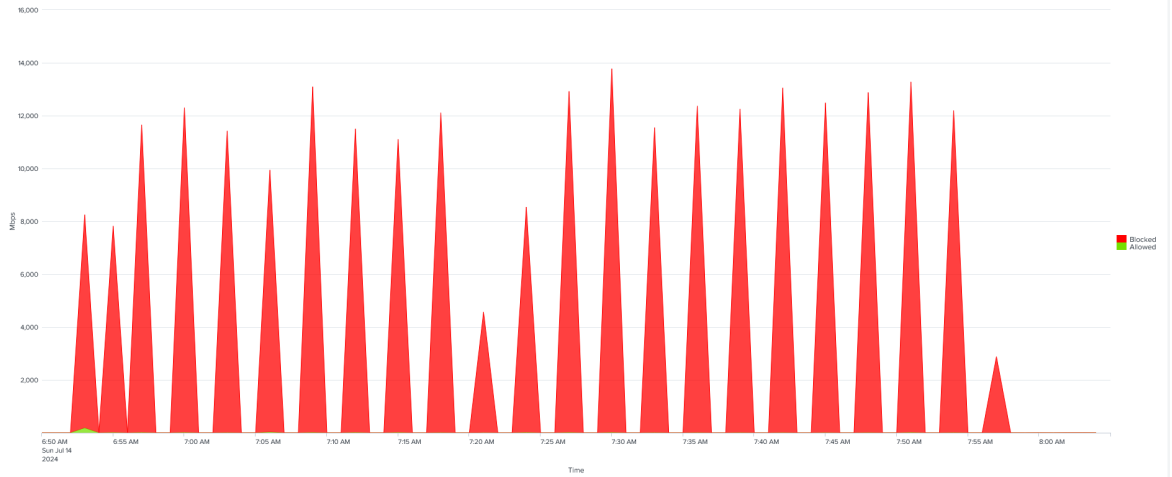

Figure 4: Burst attack

d. Variety of Attack Vectors

The method of attack, forcing the victim to start from scratch in their defense efforts. Attackers can switch from UDP to TCP, GRE, or other protocols. They may alter their approach from using static payload to random payload, change TCP flag from ACK to SYN, or from flood attack to reflection attack. On realizing that the current methods have become ineffective, other techniques are used or even employing multiple vectors simultaneously.

Capabilities and resources are more limited in other IoT botnets, but both Mirai and MikroTik have many options easily configurable for generating many traffic types, or even crafting packets. For example, it is becoming commonplace for traffic to be generated to look identical to packets used in gaming protocols, making it challenging to distinguish between legitimate and malicious traffic.

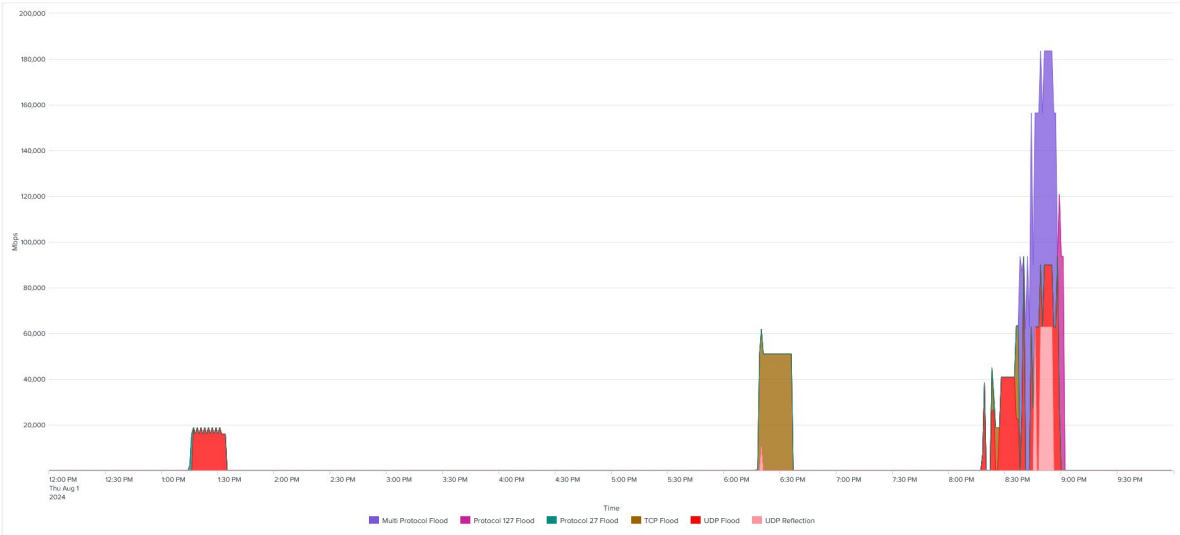

Figure 5: Attack vector changed for the same target

e. Source Distribution

In UDP flood attacks, source IP addresses can be spoofed and attackers often employ strategic decisions about when and how to spoof these addresses. For example, the attack below registered over 71% IP addresses appearing to originate from France. In such cases, implementing geo-blocking may not be a viable solution if legitimate clients are located in France.

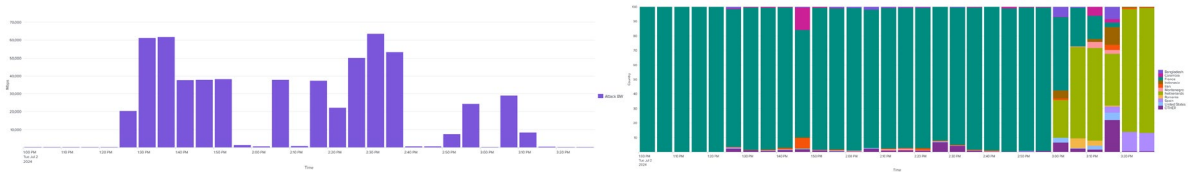

Figure 6 & 7: Source country ratio in an attack

Conversely, attackers may use a strategy where IP addresses are randomized, thereby increasing the complexity of defense mechanisms and source-based blocking may not be useful.

III. Mitigation

SmartWall ONE™ is a modular, platform-based, on-premises DDoS protection solution. It has been designed for flexible, adaptable deployment options that meet today's business and network needs and grows with you based on your needs. There is no denying that massive attacks can have an enormous impact.

Corero's Threat Research Team has developed a technique which detects and mitigates DDoS attacks from botnets. This solution is provided within the DDoS Intelligence Service and can significantly reduce the impact of such attacks.

Moreover, the DDoS Intelligence Service plays a vital role in defending against DDoS attacks by providing organizations with the necessary tools and information to proactively detect, mitigate, and respond to threats. By continuously monitoring and analyzing global threat data, these services offer insights into emerging attack vectors, tactics, and trends. This enables organizations to strengthen their defense by implementing countermeasures that address specific vulnerabilities and threats.

Additionally, with the ability to prevent new potential DDoS threats, organizations can minimize downtime, reduce financial losses, and protect their reputation.

IV. Reference

(1) https://www.corero.com/the-anatomy-of-a-mikrotik-routeros-based-botnet-attack/
(2) https://go.corero.com/hubfs/collateral/threat-research/corero-threat-research-mirai.pdf