# The Relentless Evolution of DDoS Attacks

Craig Sparling & Max Gebhardt
June 23, 2022

> Ongoing innovation in the DDoS threat landscape subjects organizations to constant risks and highlights the need for uncompromising protection against the latest attacks.

Modern distributed denial-of-service (DDoS) attacks are practically unrecognizable when compared with those from 12, 10, or even 5 years ago because of constant innovation in the threat landscape. Defending against rapidly shifting attack vectors and record-setting attacks is crucial for protecting online infrastructure, but can be a daunting challenge for security teams that lack the right resources, expertise, or technology.

## Comparing yesterday's DDoS attacks with today’s

Figure 1 depicts the activity of more than 50 attack vectors over the past decade and encapsulates the rising complexity of DDoS.

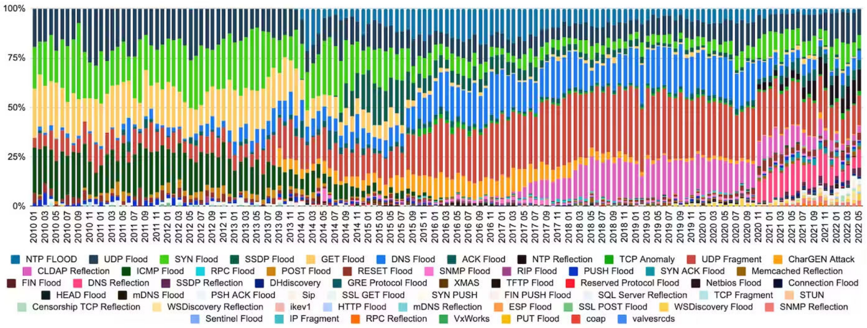

Fig. 1: DDoS activity over the past 10 years

Four notable headlines stand out:

1. The award for vector persistence goes to: UDP floods, SYN floods, and UDP fragmentation, which have existed since Akamai Prolexic’s inception on account of their

simplicity and reliability (Figure 2). They continue to be seen in force, often alongside other vectors.

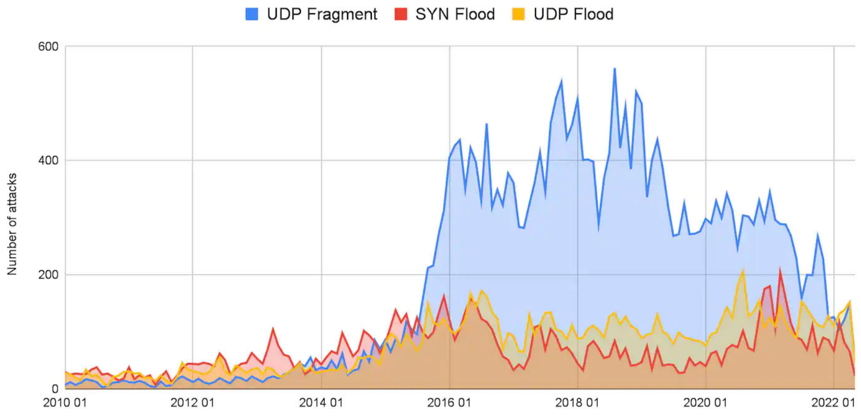

Fig. 2: UDP floods, SYN floods, and UDP fragmentation continue to be seen in force

2. Some once-prominent vectors have fallen out of favor: ICMP floods, which were popular as an easily accessible DDoS vector, don't pack nearly the punch as other vectors that allow amplification and reflection (Figure 3). Our largest ever ICMP-only attack was only 28 gbps. Those pings can add up, but the average ICMP attack is a mere 1.5 gbps, which is barely a trickle today, and they are almost exclusively used alongside other vectors. Across all ICMP attacks there is an average of two additional vectors.

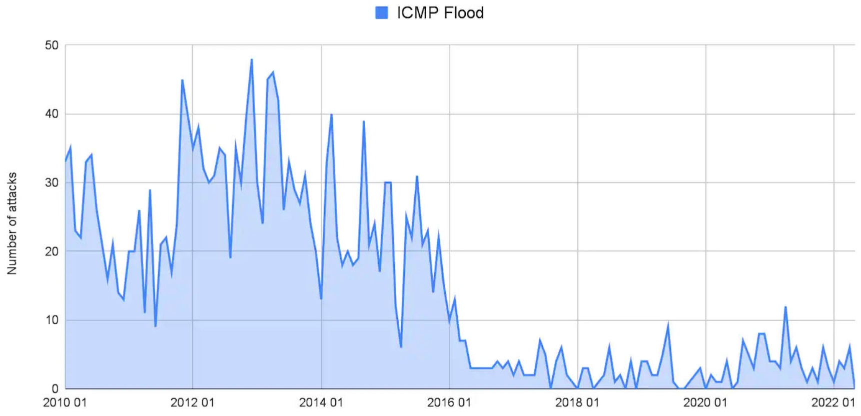

Fig. 3: ICMP attacks are no longer as popular as they once were

3. Other attacks have arrived on the scene and risen to prominence, only to fizzle out. The number of CharGEN attacks and SSDP floods grew from 2015 to 2018, but they are rarely observed today. This is likely due in part to better available reflectors, as well as fewer exposed servers using these exploitable protocols.

4. Furthermore, the use of CLDAP reflection, which emerged in late 2016 and peaked in 2018 as a top five vector, may be vanishing from the DDoS toolkit in response to improved filtering practices, diminishing novel reflectors, and shifting attacker preferences for newer, more cost-efficient vectors (Figure 4).

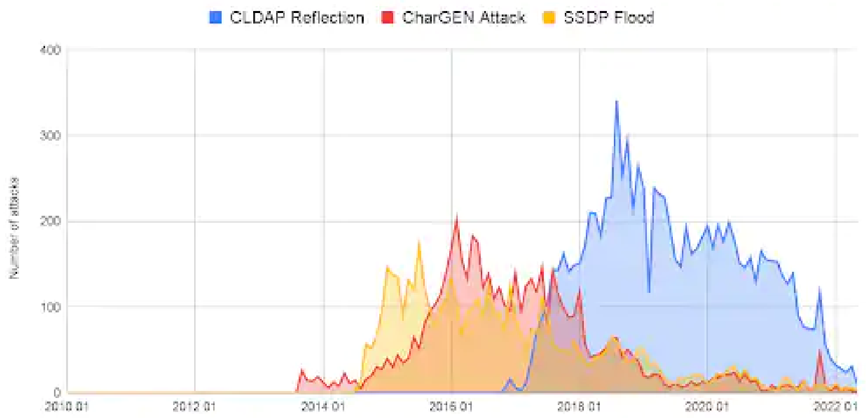

Fig. 4: CharGEN attacks, SSDP floods, and CLDAP reflections are rarely seen today

## The takeaway

The unmistakable takeaway from these four insights is that the threat of DDoS is evolving quickly. As shown in Figure 5, the top five vectors in 2010 represented **90% of all attacks, whereas today's top five only accounted for 55% of all attacks.** This shift underscores not only the increasing sophistication of the modern DDoS toolkit, but also the immense pressure on security teams to defend against a booming library of threats.

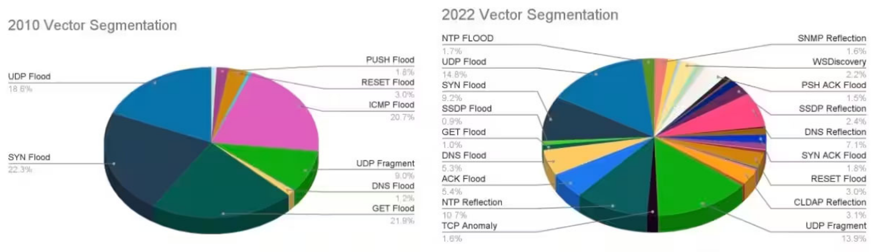

Fig. 5: Comparison of vector segmentation by year

In biology and business, whatever works best — whether it's a well-adapted physical trait or an effective product strategy — lives on and proliferates. Similarly, attack vectors that deliver the maximum impact for the smallest cost will invariably rise in popularity and outlive their peers. Attackers are constantly seeking new tools to maximize disruption and improve cost efficiency.

In the first half of 2022, we caught a glimpse of the evolutionary direction of DDoS when two menacing novel vectors hit our platform for the first time. One boasted an amplification potential of 65, the other a whopping 4.2 billion. So, what factors will ultimately determine the prevalence and survival of these new attack vectors?

## A closer look at today's novel DDoS threats

To answer, let's examine the threats in question:

- PhoneHome: A new reflection/amplification DDoS vector with a record-breaking potential amplification ratio of 4,294,967,296:1 It has been observed in the wild launching multiple DDoS attacks.
    - Potential: There is potential for huge amplification: a single, tiny, inbound packet can launch immense outbound attacks.

    - Limitations: Limited attack surface: With 2,600 of these in the wild, the congestion could be contained to the connections and power of those machines, and the malicious actors’ ability to recruit them.

- TCP Middlebox Reflection: This new amplification vector exploits middleboxes, such as corporate and national firewalls, to reflect traffic against a victim.

    - Potential: The middleboxes that are potential reflectors here are ubiquitous, measuring more than 18.8 million IPs according to research by ShadowServer. Most of these exposed services are, by their nature, powerful and have access to major connection hubs.

    - Limitations: Although the amplification factor here is a pedestrian 65, the upper limits aren’t readily apparent. Right now, attackers could be cataloging the available reflectors and testing how to reliably exploit them en masse. While generating requests to trigger the response packets from a single command and control may be limiting, generating requests from a botnet to the reflectors could increase the size to new records.

We don’t know if either of the above vectors will gain prominence or set new highs. What we can say for sure is that the path of evolution will continue onward, and there will be a next generation of threats on networks.

## Recommendations for keeping pace with evolving threats

Ongoing innovation in the DDoS threat landscape subjects organizations to constant risk and highlights the need for uncompromising protection against the latest attacks. To reduce the threat of DDoS-associated downtime and to outwit bad actors, consider doing the following:

- Review critical subnets and IP spaces, and ensure that they have mitigation controls in place.

- Deploy DDoS security controls in an “always-on” mitigation posture as a first layer of defense, to avoid an emergency integration scenario, and to reduce the burden on incident responders. If you don’t have a trusted and proven cloud-based provider, get one now.

- Proactively pull together a crisis response team and ensure runbooks and incident response plans are up to date. For example, do you have a playbook to deal with catastrophic events? Are the contacts within the playbooks updated? A playbook that references outdated tech assets or people who have long left the company isn’t going to help.

## More help and further DDoS-related resources

If you are currently under DDoS attack or threat of extortion, reach out to the Akamai DDoS hotline, 1-877-425-2624, for immediate assistance or click here to register for a custom threat briefing.

For more technical details and additional DDoS-related resources, please see the following blog posts and materials:

- REvil Resurgence? Or a Copycat?

- CVE-2022-26143: TP240PhoneHome Reflection/Amplification DDoS Attack Vector

- TCP Middlebox Reflection: Coming to a DDoS Near You

- DDoS Chart Toppers—BPS, PPS and RPS Greatest Hits

- Akamai SIRT Threat Advisory

- Unprecedented Levels of Ransom DDoS Extortion Attacks

*This blog was co-written by Max Gebhardt.*

DDoS Security Prolexic

Written by

Craig Sparling

Craig Sparling is a Product Manager in the Cloud Security business unit. Craig joined Akamai with the acquisition of Prolexic and specializes in attack detection, network monitoring, data visualization, and user interfaces. His passion is working for customers to understand their needs and creating powerful and intuitive solutions that solve their real-world problems.

Written by

Max Gebhardt

Max is a product marketing manager at Akamai, where he leads go-to-market strategies and messaging for the infrastructure security division. He blogs about threat research, market trends, customer challenges, and various cybersecurity solutions.