CORE

WHITE PAPER

High Performer
Mid-Market
SPRING 2023

Gcore Radar: DDoS Attack Trends

Q3–Q4, 2023

January 2024 | gcore.com

Executive Summary

As we enter 2024, we're pleased to present the latest Gcore Radar report, a twice-annual publication in which we release internal analytics to track DDoS attacks. Our broad, internationally distributed network of scrubbing centers allows us to follow attack trends over time. DDoS attack trends for the second half of 2023 reveal alarming developments in the scale and sophistication of cyberthreats. Notable changes to the DDoS landscape were the doubling of peak attack power into the mid-Tbps range, the targeting of specific industries with tailored strategies, and the globalization of attack sources.

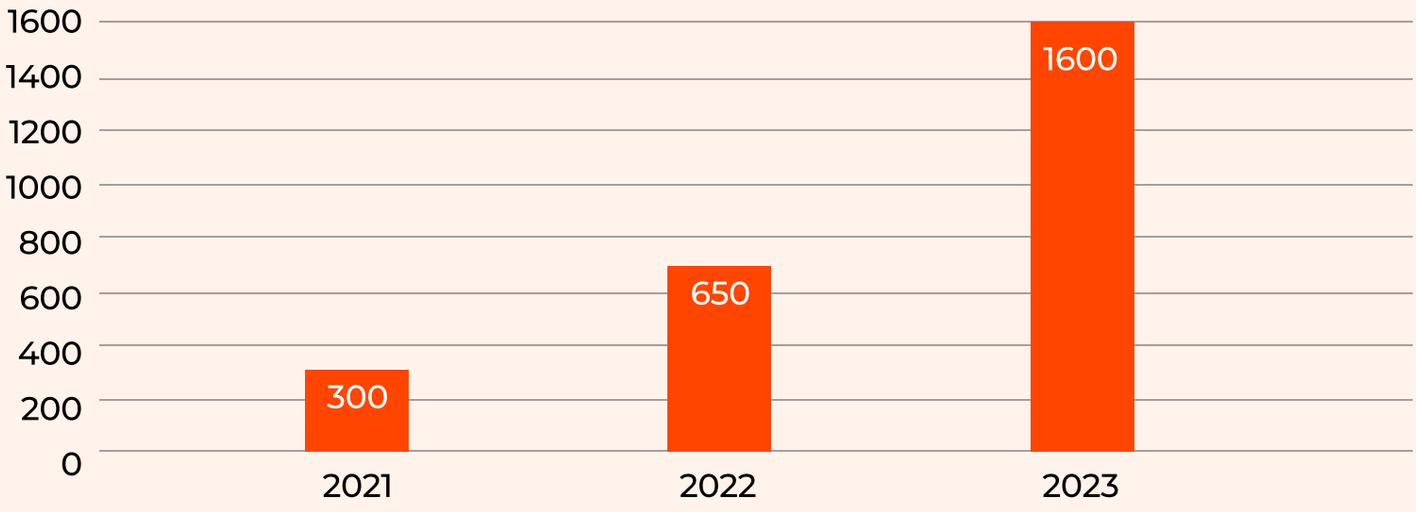
Unprecedented Attack Power

The past three years have brought about a >100% annual increase in DDoS peak (registered maximum) attack volume:

- In 2021, the peak capacity of DDoS attacks was 300 Gbps
- In 2022, it increased to 650 Gbps
- In Q1–Q2 of 2023, it increased again to 800 Gbps
- In Q3–Q4 of 2023, it surged to 1600 Gbps (1.6 Tbps)

Notably, the jump in H2 of 2023 means the cybersecurity industry is measuring DDoS attacks in a new unit, Terabits.

Maximum attack power in 2021–2023 in Gbps

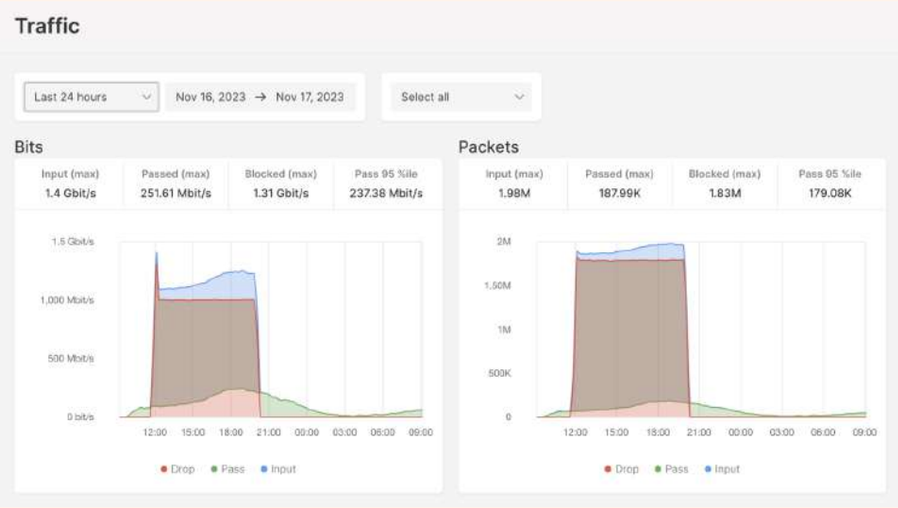


Graph reflecting increasing maximum peak attack volumes in 2021–2023 with 300, 650, and 1600 Gbps respectively

This illustrates a significant and ongoing escalation in the potential damage of DDoS attacks, a trend Gcore expects to see continue in 2024.

Attack Duration

The longest registered attack in H2 of 2023 lasted nine hours



We saw attack lengths varying from three minutes to nine hours, with an average of about an hour. Usually, short attacks are harder to detect as they don't allow for traffic analysis due to data scarcity, and since they're harder to recognize, they're also harder to mitigate. Longer attacks require more resources to fight, requiring a powerful mitigation response; otherwise, the risk is prolonged server unavailability.

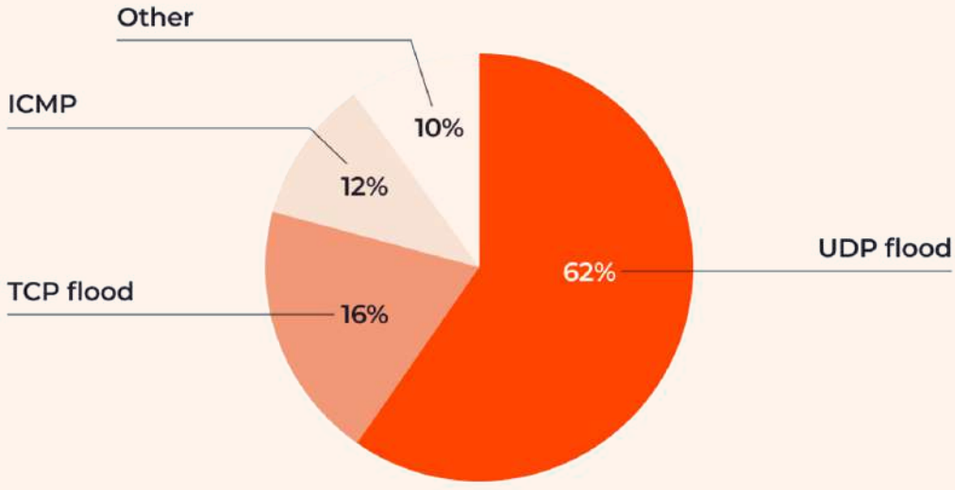
Predominant Attack Types

UDP floods continue to dominate, constituting 62% of DDoS attacks. TCP floods and ICMP attacks also remain popular at 16% and 12% of the total, respectively.

All other DDoS attack types, including SYN, SYN+ACK flood, and RST Flood, accounted for a mere 10% combined. While some attackers may use these more sophisticated approaches, the majority are still focused on delivering sheer packet volume to take down servers.

The variation in attack methods necessitates a multifaceted defense strategy that can protect against a range of DDoS techniques.

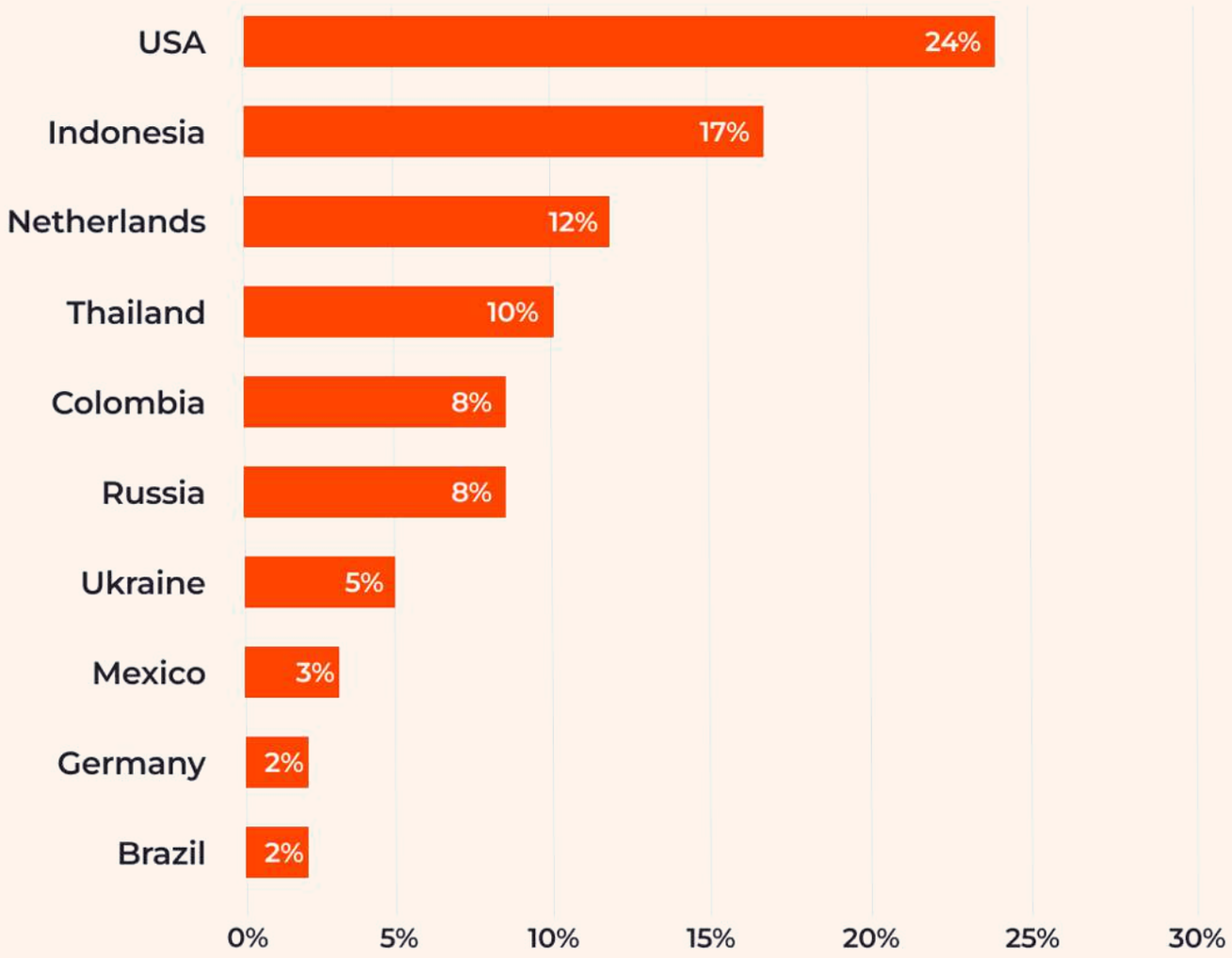
Dominant attack types in H2 of 2023



Global Attack Sources

This global spread of attack sources demonstrates the borderless nature of cyber threats, where attackers operate across national boundaries. Gcore identified diverse attack origins in the latter half of 2023, with the US leading at 24%. Indonesia (17%,) the Netherlands (12%,) Thailand (10%,) Colombia (8%,) Russia (8%,) Ukraine (5%,) Mexico (3%,) Germany (2%,) and Brazil (2%) make up the top ten, illustrating a widespread global threat.

Geographical attack source spread



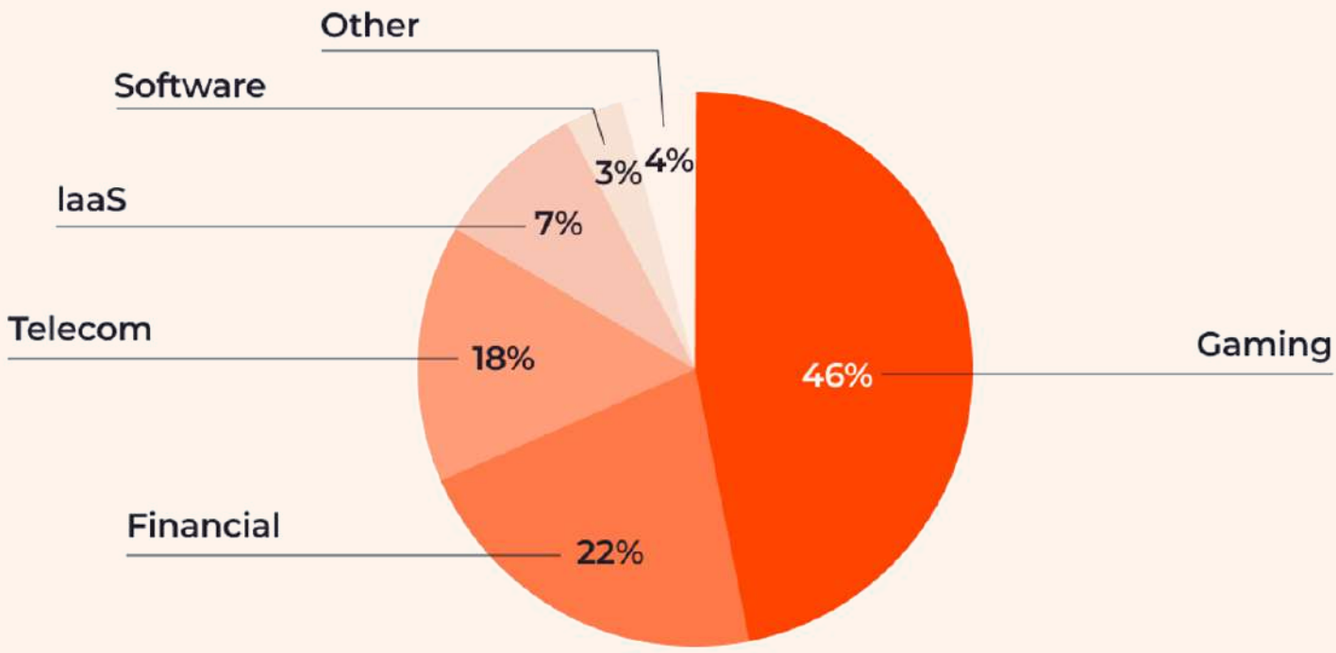
The geographic distribution of DDoS attack sources provides important information for creating targeted defense strategies and for shaping international policy-making aimed at combating cybercrime. However, determining the location of the attacker is challenging due to the use of techniques like IP spoofing and the involvement of distributed botnets. This makes it difficult to assess motivations and capabilities, which can vary from state-sponsored actions to individual hackers.

Targeted Industries

The most-targeted industries in H2 of 2023 highlight the impact of DDoS attacks across diverse sectors:

- The gaming industry remains the most affected, enduring 46% of the attacks.
- The financial sector, including banks and gambling services, came in second at 22%.
- Telecommunications (18%,) infrastructure-as-a-service (IaaS) providers (7%,) and computer software companies (3%) were also significantly targeted.

DDoS attacks by affected industry



Since the previous Gcore Radar report, attackers haven't changed their focus: The gaming and financial sectors are particularly interesting to attackers, likely due to their financial gains and user impact. This underscores a need for targeted cybersecurity strategies in the most-hit industries, like countermeasures for specific gaming servers.

Analysis

The data from the latter half of 2023 highlights a worrying trend in the DDoS attack landscape. The increase in attack power to 1.6 Tbps is particularly alarming, signaling a new level of threat for which organizations must prepare. For comparison, even a "humble" 300 Gbps attack is capable of disabling an unprotected server. Paired with the geographical distribution of attack sources, it's clear that DDoS threats are a serious and global issue, necessitating international cooperation and intelligence sharing to mitigate potentially devastating attacks effectively.

The range in attack durations suggests that attackers are becoming more strategic, tailoring their approaches to specific targets and objectives:

- **In the gaming sector**, for example, assaults are relatively low in power and duration but more frequent, causing repeated disruption to a specific server with the goal of disrupting the player experience to force them to switch to a competitor's server.
- **For the financial and telecom sectors**, where the economic impact is more immediate, attacks are often higher in volume with length highly variable.

Conclusion

This report serves as a timely reminder of the ever-evolving nature of cyberthreats. Organizations across sectors must invest in comprehensive and adaptive cybersecurity measures. Staying ahead of DDoS threats requires a keen understanding of the changing patterns and strategies of cyber attackers.

Gcore DDoS Protection has a proven record of repelling even the most powerful and sustained attacks. Connect Gcore DDoS Protection to protect your business from whatever the 2024 DDoS landscape brings.