Akamai

Largest European DDoS Attack on Record

“

On Thursday, July 21, 2022, Akamai detected and mitigated the largest DDoS attack ever launched against a European customer on the Prolexic platform.

This blog was co-written by Max Gebhardt.

The risk of distributed denial-of-service attacks (DDoS) has never been greater. Over the past several years, organizations have encountered a deluge of DDoS extortion, novel threats, state-sponsored hacktivism, and unprecedented innovation in the threat landscape.

And attackers are showing zero signs of relenting.

On Thursday, July 21, 2022, Akamai detected and mitigated the largest DDoS attack ever launched against a European customer on the Prolexic platform, with globally distributed attack traffic peaking at 853.7 Gbps and 659.6 Mpps over 14 hours. The attack, which targeted a swath of customer IP addresses, formed the largest global horizontal attack ever mitigated on the Prolexic platform.

Attack breakdown

The victim, an Akamai customer in Eastern Europe, was targeted 75 times in the past 30 days with horizontal attacks consisting of UDP, UDP fragmentation, ICMP flood, RESET flood, SYN flood, TCP anomaly, TCP fragment, PSH ACK flood, FIN push flood, and PUSH flood, among others. UDP was the most popular vector observed in both record spikes.

After five days, the attack campaign reached peak PPS (659 Mpps) at 4:44 AM UTC (Figure 1).

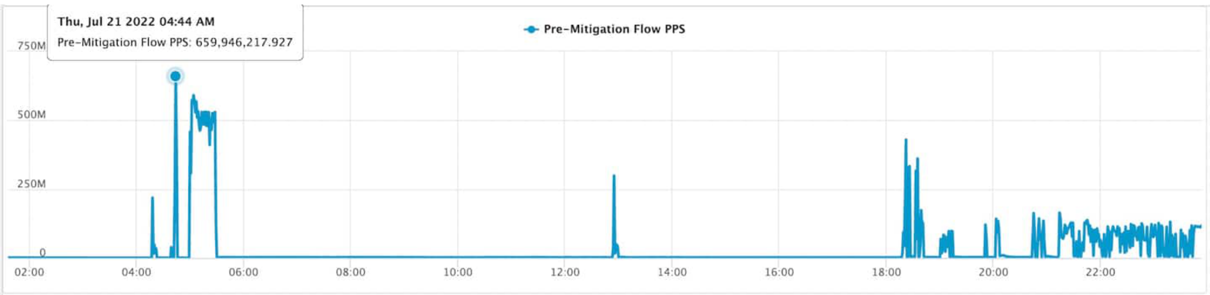

Fig. 1: Spike in PPS attack traffic

Attack volume subsequently ramped up to 853 Gbps at 6:40 PM UTC (Figure 2).

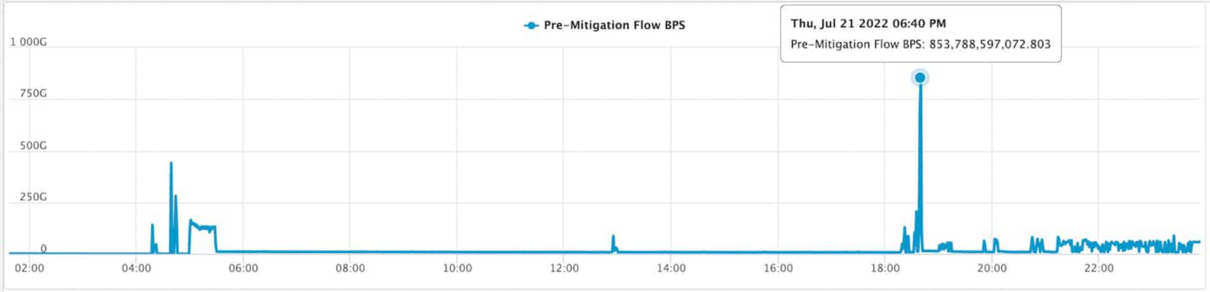

Fig. 2: Spike in BPS attack traffic

Distributed attack traffic suggests bad actors were leveraging a highly-sophisticated, global botnet of compromised devices to orchestrate this campaign (Figure 3). No individual scrubbing center handled more than 100 Gbps of the overall attack.

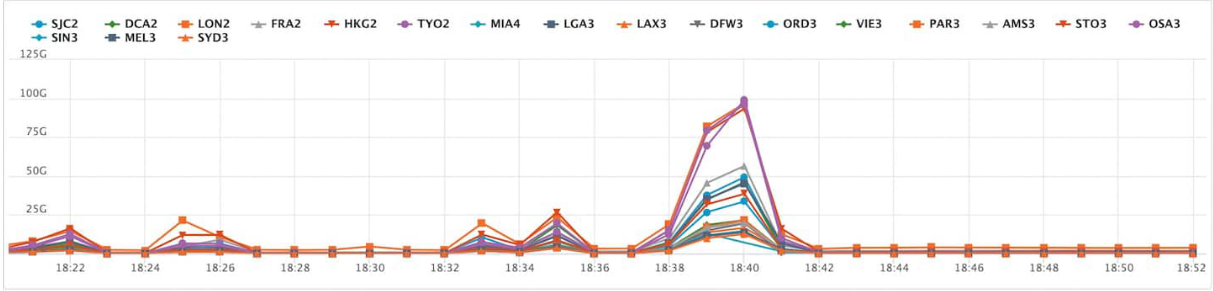

Fig. 3: Regional distribution of BPS attack traffic

Mitigation strategy

Without the right defenses, even a robust, modern network would likely collapse under an assault of this magnitude, making any online business that’s reliant on that connection completely inaccessible, which can jeopardize consumer trust, result in financial loss, and have other serious ramifications.

To thwart the attack and safeguard our customer, Akamai Prolexic employed its industry-leading combination of technology, people, and processes to pre-mitigate the assault with no collateral damage thanks to our proactive defense posture for this customer.

- Platform: a dedicated defense capacity that scales to several times the size of the largest publicly reported attacks

- People: more than 225 frontline responders across 6 global locations with decades of expertise who mitigate the most sophisticated attacks for the world’s largest, most-demanding organizations

- Process: optimized DDoS incident response plans through custom runbooks, service validation, and operational readiness drills

In the wake of heightened operational risk, having a proven DDoS mitigation strategy is imperative for online businesses to thrive. To stay ahead of the latest threats and learn more about Akamai's DDoS solutions, employ the recommendations below.

Under attack?

Visit this link for 24/7 emergency DDoS protection.

Recommendations for mitigating DDoS risk

- Immediately review and implement Cybersecurity and Infrastructure Security Agency (CISA) recommendations*

- 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 runbook to deal with catastrophic events? Are the contacts within the playbooks updated? A playbook that references outdated tech assets or people that have long left the company isn't going to help.