MEMCACHED REFLECTION ATTACKS:
A NEW ERA FOR DDoS

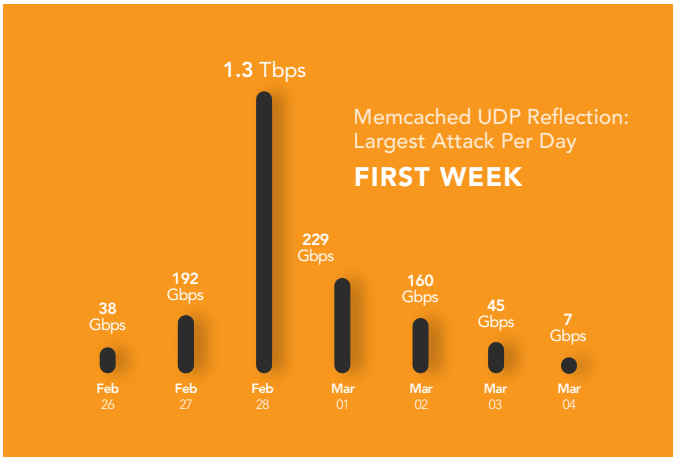
DDoS attack size doubled in early 2018 after attackers discovered and employed a new, massive DDoS reflection and amplification method with the potential to multiply their attack resources by a factor of 500K. The attack vector, called *memcached UDP reflection*, uses resources freely exposed on the internet — no malware or botnet required.

On February 28, 2018, the largest DDoS attack recorded to date targeted an Akamai customer with a record-setting 1.3 Terabits per second (Tbps) of memcached reflection DDoS traffic. The attack was more than twice the size of the previous record-setting DDoS attacks from Mirai internet of Things (IoT) botnets.

Akamai's Prolexic DDoS protection service mitigated the giant DDoS attack instantly upon receiving the customer's network traffic, filtering out all traffic sourced from the default port used by memcached, an open-source data caching tool. Clean traffic was returned to the customer's network from Akamai DDoS scrubbing centers in Europe, U.S., and Asia — with no further impact on the customer's operations.

Memcached, routinely used to improve query response times from disks and databases, has been turned into an internet weapon by attackers using reflection DDoS techniques. The first DDoS attack attributed to memcached reflection was observed only two days before the massive attack. At the time of the 1.3 Tbps attack, Akamai had already put in place automated mitigations to defend instantly against memcached attacks targeting our customers.

Within its first week, 19 memcached reflection DDoS attacks targeted Akamai customers across many industries.



Formidable 500,000 Amplification Factor and Packet Rate

Memcached reflection has an extraordinary amplification factor: A 210 byte request could trigger a 100 MB response directed at the target. By design, memcached data is delivered at a high rate of speed: Akamai measured the rate during this attack at 127 million packets per second (Mpps).

On an unprotected internet server, with the UDP communication protocol enabled by default, memcached will deliver its data to anyone who asks — including a spoofed IP address. Tens of thousands of servers on more than 1,000 ASNs participated in the 1.3 Tbps attack, and each delivered nearly 1 Gbps of attack traffic on average. Researchers estimate there are more than 90,000 memcached servers on the internet, of which more than 50,000 are currently vulnerable to being exploited as a reflector.

Expect More Memcached DDoS Attacks and Ransom DDoS

As the security community has seen with the continued popularity of other reflection DDoS vectors, relying on remote system administrators to patch, reconfigure, or remove vulnerable servers is unlikely to yield immediate results. Memcached DDoS attacks can be expected in the future.

With reflection DDoS attacks such as memcached, attackers do not need malware to infect and control bots in a botnet. Even unsophisticated attackers can launch an attack. Akamai has observed an increase in scanning to identify vulnerable memcached servers. More attackers will abuse more memcached servers to generate DDoS attacks of all sizes. In addition, memcached payloads are being used to deliver extortion messages; Akamai recommends against payment of any ransom.

DDoS Attacks Overwhelm Local Network Pipes

Few organizations, aside from a well-prepared cloud-based DDoS mitigation and content delivery network (CDN) provider such as Akamai, and the largest ISPs, have the available network capacity to maintain operations in the face of larger DDoS attacks, and certainly not an attack of this size. Network pipes into the data center and edge routing devices will be overwhelmed first, preventing onsite DDoS mitigation.

The Importance of DDoS Mitigation Planning

The Akamai customer hit by this record-setting DDoS attack was commendably well prepared, and as a result experienced an outage of less than 10 minutes prior to routing its traffic to Akamai for mitigation. The customer had engaged the Prolexic DDoS protection service in advance, and had developed and practiced a DDoS runbook, so personnel knew what to do and whom to call. Network traffic was monitored, and upon identifying the anomaly, personnel routed all network traffic to Akamai within a quick five minutes.

Why Akamai: Architected for DDoS Resilience

Akamai protects our customers against DDoS attacks with our CDN, the Prolexic network, and the distributed Fast DNS infrastructure. We make investments to constantly improve the DDoS resilience of these platforms.

At the highest level, Akamai's capacity planning model takes the largest DDoS attacks we can verify — and multiplies the traffic by a scaling factor to provide ample headroom as attacks grow in size. As a result, we are able to successfully mitigate the largest and most sophisticated DDoS attacks even when they double in size, including this one.

Our Adversarial Resilience team continually evaluates new threats and incidents to discover potential breaking points in Akamai systems, and works with engineering teams to implement automatic mitigations and to improve resiliency in all areas.

DDoS Resilience in the Content Delivery Network

Beyond capacity, we architect our CDN for availability and resiliency through adverse conditions — not just DDoS attacks. With more than 220,000 servers deployed around the world, Akamai CDN adjusts for the status of individual servers and automatically routes user traffic around outages and congestion. Each server provides DDoS defense, including rate controls, blacklists, and geo-blocking.

DDoS Resilience in the Prolexic Network

The Prolexic network is among the most powerful DDoS scrubbing services in the world. It consists of seven global scrubbing centers, more than 3.5 Tbps of capacity, and a team of 150 security professionals who protect against thousands of DDoS attacks every month. Each scrubbing center has multiple Tier 1 carrier connections, public peering with more than 500 peers, and high-performance traffic analysis and active mitigation at multiple layers of the OSI stack. We continue to add DDoS protection capacity.

DDoS Resilience in the Fast DNS Infrastructure

Akamai operates an authoritative DNS service — Fast DNS — for availability, speed, and DDoS resilience. We distribute the name servers assigned to our customers across more than 20 segmented DNS clouds to minimize the impact that DDoS attacks against any Akamai customer can have on others. Clusters of name servers and additional controls minimize the impact of localized DDoS attacks.

Conclusion

Akamai has defended against DDoS attacks for nearly two decades and has protected customers and maintained infrastructure availability, even while withstanding the largest DDoS attacks of the time. Akamai continues to investigate and report on new threats, and we continue to evolve our procedures and platform to stay ahead of those with malicious intent. We apply what we learn defending all of our customers to improve our protections. We are committed to providing Akamai customers with the most robust platform in the industry.

Review Your Own DDoS Resiliency

If you would like Akamai's help in reviewing your infrastructure resiliency, reach out to our **Professional Services organization** for a consultation by our Security Architects.

Learn more at **https://www.akamai.com/memcached.**