WHITE PAPER

The Rapid Evolution and Growing Threat of DDoS Attacks

With attacks becoming more targeted, sophisticated, and frequent, every business needs to remain vigilant.

No company flies under the radar for distributed denial-of-service (DDoS) attacks anymore. Cybercriminals – bent on extortion, hacktivism, or revenge – can easily target any organization with large and sophisticated attacks. That's why every digital-oriented business now needs a holistic defense against DDoS assaults.

One of the Internet's Earliest Attack Types

On July 22, 1999, 114 compromised computers overwhelmed a single University of Minnesota computer with superfluous data packets and knocked it offline for two days.

This, according to MIT Technology Review, was the first documented DDoS attack.

In the weeks and months that followed, major players – from CNN to Amazon – went offline as hacktivists and other cybercriminals saw how easy these attacks were to launch. All it took was a few lines of code.

DDoS became a threat to any business with an online presence.

Attacks Grow in Scale and Sophistication

DDoS defenses have come a long way since 1999. But so have criminals. Today's DDoS threat actors have dozens of attack vectors to leverage and inexpensive attacker toolkits, plus countless vulnerable devices on the internet to amplify their campaigns. In 2016, attackers took down a large portion of the internet using compromised security camera DVRs.

Since then, hundreds of millions more unprotected IoT devices have come online. The coming 5G revolution promises hundreds of millions more. Just imagine the strength and size of attacks fueled by 5G's exponential improvements in speed, capacity, and latency.

Also growing in leaps and bounds: the number of unprotected and unmaintained servers on the internet that criminals can hijack for amplification and reflection attacks. Many of these servers – and the criminals know their IPs – can multiply spoofed requests by a factor of more than 50,000.

24/7 Emergency DDoS Mitigation and Protection

Existing Akamai customers threatened with a DDoS attack should contact the Akamai Security Operations Command Center (SOCC).

If you are not an Akamai customer, but need emergency protection, complete the form on our **DDoS Hotline Page**, or call **+1-877-425-2624** for immediate assistance.

No Industry Is Immune to DDoS Attacks

Today, Akamai mitigates thousands of DDoS attacks every year.

In some cases, the motives appear obvious. A gamer may use DDoS attacks to slow down networks and gain a competitive advantage against rival players. College students once used targeted DDoS attacks to frustrate an ISP's customers and drive business to a competitor.

Sometimes, however, the motives are more complex or elusive. We've seen criminals use DDoS attacks to distract incident response teams in one part of an organization while they attempt a less obvious attack in another.

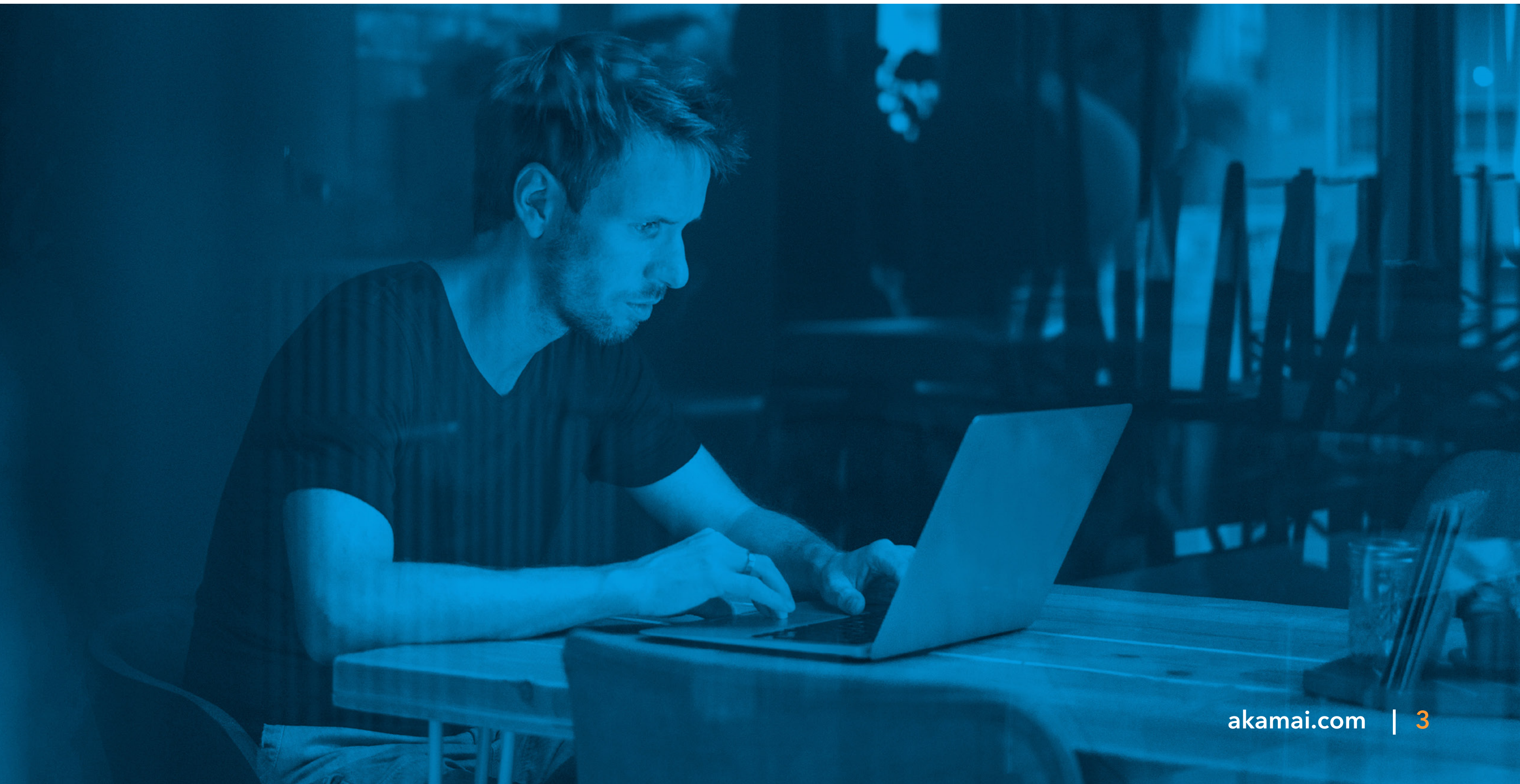
For malicious actors who don't have the skills, there are "DDoS for Hire" businesses on the darknet. Prices start at $5 for a 5-minute attack and increase to $400 for 24 hours. If someone's got a bone to pick, they can spend $200 or $300 and cost a company millions.

2020 Brought Larger and More Sophisticated Attacks

In the first half of 2020, Akamai stopped massive attacks of 1.44 Terabit per second (Tbps) and 809 million packets per second (Mpps), the largest Mpps attack on record.

Though mitigated in under a second, these attacks reflect a trend toward more 100 Gbps or greater attacks. Many use unique, complex combinations of multiple vectors. They want to overwhelm or circumvent defenses, and consume incident response resources.

Attacks that require at least some human-driven mitigation — not just automated responses — are also on the rise.



Enter the Largest DDoS Extortion Campaign in History

In August 2020, the Akamai Security Intelligence Research Team issued an alert, warning that companies in diverse industries had received DDoS extortion emails. Attackers threatened to cripple operations, inferring that the businesses would face huge downtime and heavy financial losses if they didn't pay a ransom in Bitcoin.

Only a few weeks later, the FBI reported that thousands of organizations around the world had received similar extortion emails. The attackers would swarm in and threaten businesses in one industry, then pivot to another, and then another. The highly organized attackers often came back to threaten previous targets.

The Better Your Defenses, the Less Likely You'll Be Attacked

Cybercriminals are like any criminals. They "case the joint," looking for a weakness. For DDoS, that means looking at the intended victim's DNS, web applications, and internet-facing data center assets.

If this reconnaissance reveals vulnerable resources, sites, or services, cybercriminals may move in. If it reveals hardened defenses, they often move on.

In fact, among new Prolexic emergency turn-up customers that were attacked before routing onto the platform, the vast majority were not hit again once Prolexic defenses were in place. To a cybercriminal, Prolexic-defended targets may not be worth their time, especially when there's low-hanging fruit elsewhere.

How a Holistic DDoS Defense Works

Akamai provides DDoS defense in depth through a transparent mesh of dedicated edge, distributed DNS, and cloud scrubbing mitigation solutions with over 175 Tbps of total network capacity. These purpose-built clouds are designed to strengthen DDoS security postures while reducing attack surfaces. This end-to-end DDoS protection is architected to improve the quality of mitigation and reduce false positives, while increasing resiliency against the largest and most complex attacks.

Moreover, the solution can be fine-tuned to the specific requirements of your web applications and internet-based services.

Edge Defense

Akamai architected its globally distributed Intelligent Edge Platform as a reverse proxy to only accept traffic via ports 80 and 443. All network layer DDoS attacks are instantly dropped at the edge with a zero-second SLA.

For application layer events, including those launched via APIs, Kona Site Defender absorbs the attacks, while simultaneously granting access to legitimate users.

DNS Defense

Akamai's authoritative DNS service, Edge DNS, also filters traffic at the Edge. Unlike other DNS solutions, Akamai specifically architected Edge DNS for availability and resiliency against DDoS attacks. Edge DNS also delivers superior performance, with architectural redundancies at multiple levels, including name servers, points of presence, networks, and even segmented IP Anycast clouds.

Cloud-Scrubbing Defense

Prolexic protects entire data centers and hybrid infrastructures from DDoS attacks – across all ports and protocols – with 20 global scrubbing centers and 8.2 Tbps of dedicated DDoS defense. This capacity is designed to keep internet-facing assets available – a cornerstone of any information security program.

As a fully managed service, Prolexic can build both positive and negative security models. The service combines automated defenses with expert mitigation from Akamai's global network of SOCCs. Prolexic also offers an **industry-leading** zero-second mitigation SLA via proactive defensive controls.

How Prolexic Stopped a Record-Setting Attack

June 2020's 809 Mpps attack was the largest packets-per-second (PPS) attack ever seen across the internet. Unlike the more common bits-per-second attacks, which try to overwhelm the inbound internet pipeline, PPS attacks set out to exhaust network gear in the data center or cloud.

This formidable attack involved a massive number of source IP addresses. More than 96% of those had not been observed in attacks before. The attack also grew from 418 Gbps to 809 Mpps in just two minutes.

Fortunately, the targeted organization was a Prolexic customer, backed by a zero-second SLA. The Akamai SOCC worked with this customer to understand its peacetime traffic baseline profiles and put controls and security policies in place to block DDoS attacks — instantly.

Schedule a Custom Threat Briefing Today

Visit akamai.com/ddos-briefing

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone — and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 04/21.