ANAPAYA

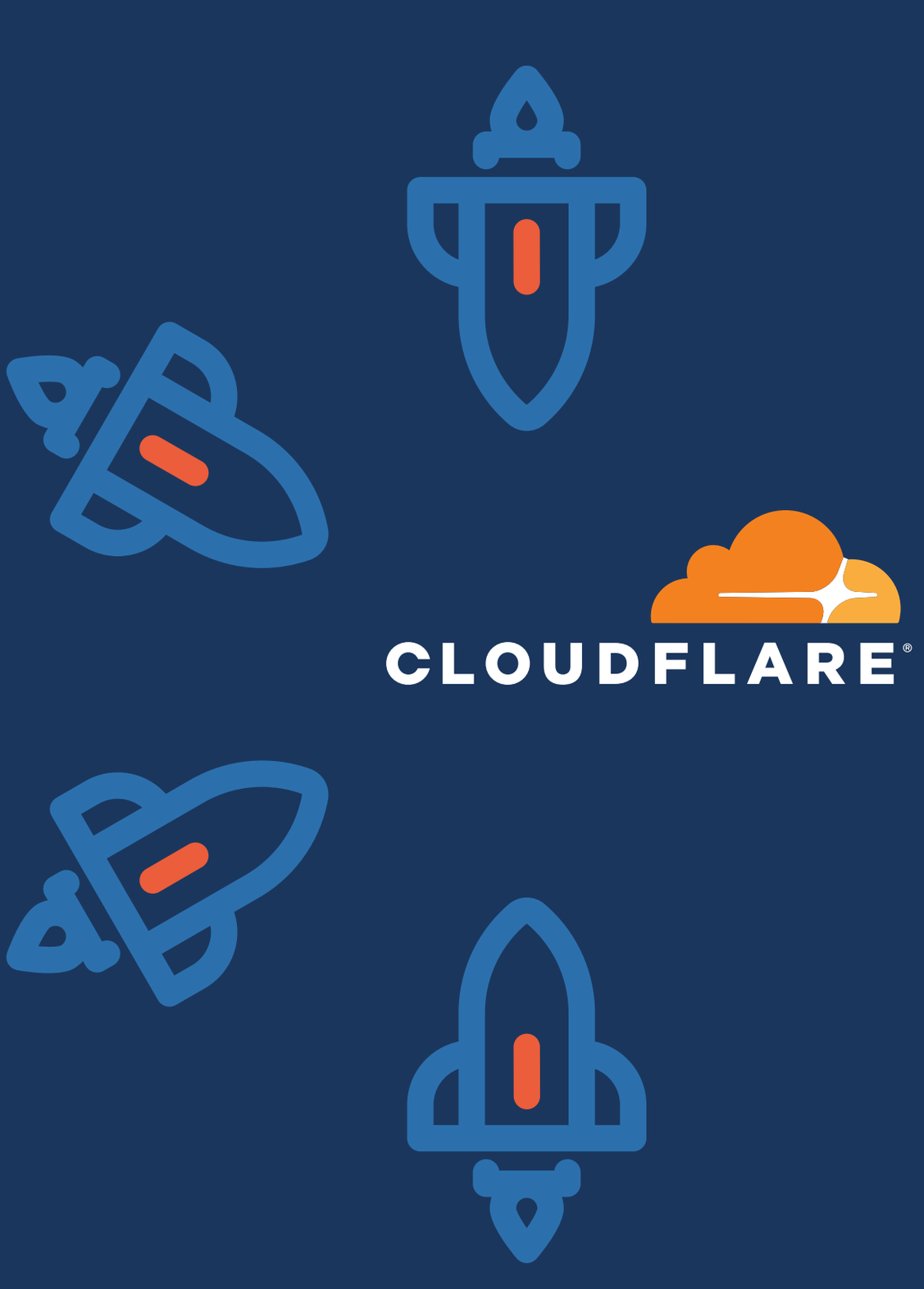
DDoS Attacks

THROUGHOUT TIME

FEBRUARY 2023

THE CLOUDFLARE DEFENSE [1]

Cloudflare witnessed an unprecedented surge in DDoS attacks in February. They endured a series of hyper-volumetric threats that reached a staggering average of 50 to 70 million requests per second. **The most potent attack exceeded 71 million rps, setting a record for the largest HTTP DDoS assault in history - 35% higher than the previous record.**



Without Cloudflare's timely and effective defense mechanisms, the repercussions of **these attacks could have been catastrophic, affecting a variety of online services** ranging from gaming providers to cloud computing platforms.

DDoS attackers have displayed a bold trend of coupling DDoS attacks with ransom demands, a trend that has continued into 2023. **Had these attacks been successful, the financial and reputational damage to affected businesses could have been monumental,** affecting not only the targeted companies but also their customers and users who depend on their services.

NOVEMBER 2022

MICROSOFT AZURE ATTACKS [2]

In November 2022, Microsoft withstood an enormous DDoS onslaught targeting an Azure customer in Asia. **This attack hit a peak throughput of 3.47 terabits per second (Tbps) and a packet rate of 340 million packets per second, setting the record for the largest attack ever reported in history.** The attack originated from approximately 10,000 sources across multiple countries.

Later in December, Microsoft fended off **two more attacks surpassing 2.5 Tbps, both aimed at Asian customers. The first was a 3.25 Tbps UDP** attack extending **over 15 minutes**, while **the second was a 2.55 Tbps UDP flood,** lasting a little **over five minutes.**

Despite the severity of these attacks, Azure's DDoS protection platform successfully absorbed and mitigated the assaults. Had the attacks been successful, countless websites and digital services would have been down, leaving them open to further attack.

FEBRUARY 2021

THE EUROPEAN GAMBLING COMPANY ATTACK [3]

In one of the most significant extortion schemes, a **European Gambling Company** was targeted by **three of the six largest volumetric DDoS attacks ever recorded by Akamai, peaking at an unprecedented 800 gigabits per second. The attackers utilized** a **novel attack vector based on Datagram Congestion Control Protocol (DCCP), known as protocol 33,** designed to **circumvent defenses against traditional Transmission Control Protocol (TCP)** and **User Datagram Protocol (UDP) traffic flows.**

The financial implications were substantial, and the company's reputation was significantly damaged. With estimates potentially **reaching tens of millions of euros in lost revenue, coupled with customer dissatisfaction and trust issues,** this event marked a concerning evolution in the methodology of DDoS attacks, highlighting the necessity for ever-evolving cybersecurity measures.

FEBRUARY 2020

THE AMAZON ATTACK [4]

aws Amazon Web Services reported mitigating a **2.3 terabit per second DDoS attack** on one of its customers.

While AWS did not disclose which customer was targeted by the attack, the attack used hijacked Connection-less Lightweight Directory Access Protocol (CLDAP) web servers. CLDAP has continued to be used in multiple DDoS attacks in recent years.

SEPTEMBER 2017

THE GOOGLE ATTACK [5]

Google suffered one of the **longest-lasting and largest DDoS attacks** on thousands of its servers in 2017. The attack lasted **six months and peaked at a breath-taking 2.5 terabits per second.** The attack was traced to **three different Chinese ISPs**, and was **four times larger** than the record-breaking 623 Gbps attack from the open-source botnet a year earlier.

Google has been tight-lipped on the cost, but the cost of a DDoS attack for a company like Google to be over **$2 million per day, $360 million in total.**

OCTOBER 2016

THE MIRAI DYN ATTACK [6]

Dyn, a major DNS provider had their services flooded by a massive **one terabit per second traffic flood** rendering a number of high-prole websites including **Amazon, HBO, Twitter, Reddit, PayPal, Netflix, Shopify** and **Airbnb,** inaccessible. The attack was based on open-source malicious code that **enabled anyone with modest IT skills** to mount a DDoS attack without much effort.

Sites like Shopify are estimated to have lost **$12,000 per hour,** while larger sites like Amazon could have **lost $30 to $50 million per day.**

APRIL 2015

THE GITHUB ATTACK [7]

GitHub – a platform for software developers – was hit with a **politically motivated attack** that **lasted several days** and **adapted itself around DDoS defenses and mitigation strategies.**

The attack used Baidu, China's most popular search engine, to target projects aimed to circumvent Chinese state censorship.

The attack lasted for **nearly a week.**

NOVEMBER 2014

THE OCCUPY CENTRAL DDoS ATTACK [8]

The attack was executed using not one, but **five botnets at 500 gigabits per second** to completely block Occupy Central's web hosting services, affecting Apple Daily and PopVote.

The attack was linked to the Chinese government, but also provided cover for hackers who extracted Occupy Central's personal staff details. These details were later used in other cyberattacks.

FEBRUARY 2014

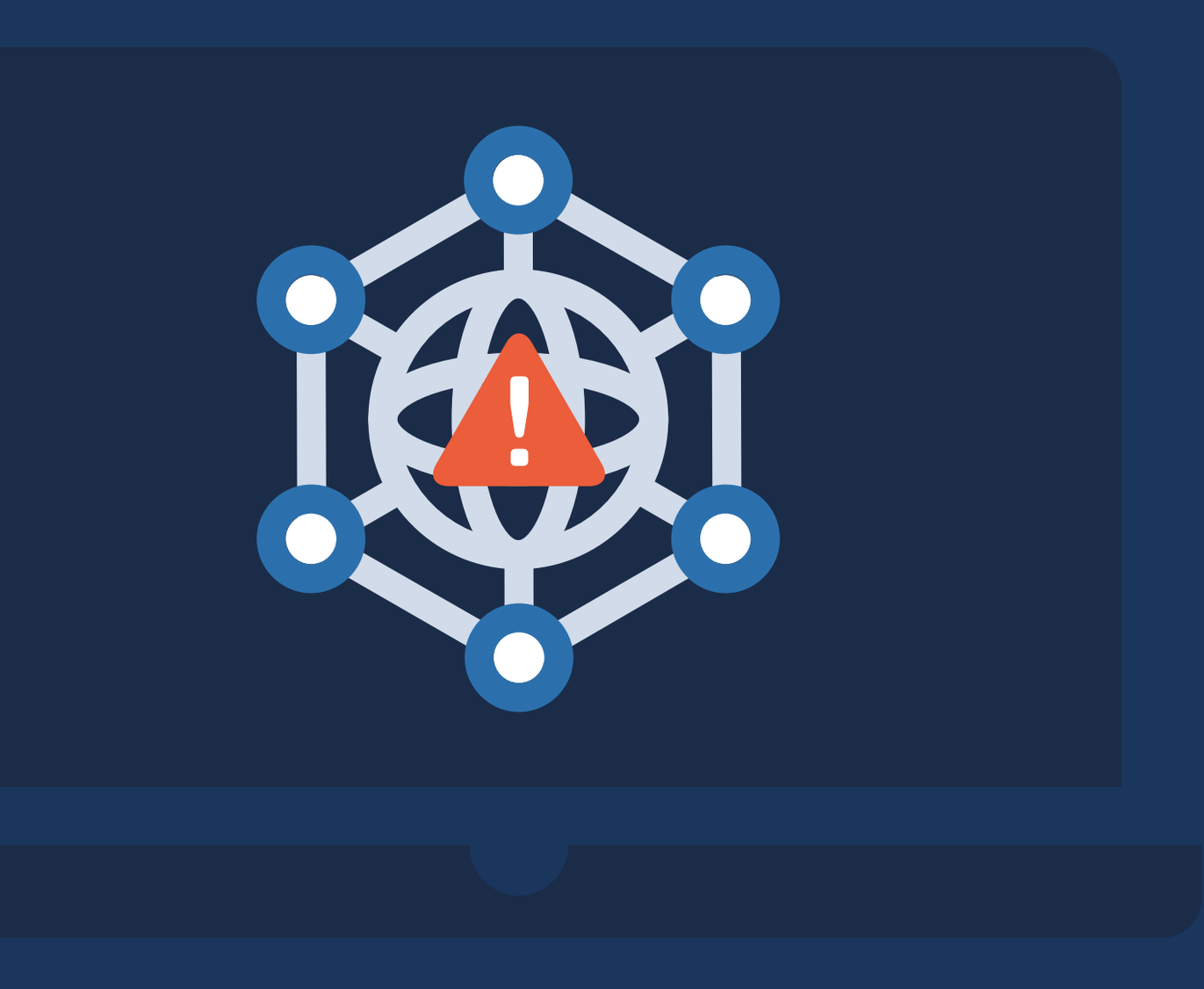
THE CLOUDFLARE ATTACK [9]

Cloudflare, a **cybersecurity provider and content delivery network**, had its **entire network significantly degraded** from a **400 gigabits per second DDoS attack**. Shortly after the attack, the U.S. Computer Emergency Readiness team explained NTP amplication attacks are ***"especially difficult to block"*** because ***"responses are legitimate data coming from valid servers"***. [10]

The cost of migrating Cloudflare's services was estimated at about **$370 million**. [11]

MARCH 2013

THE SPAMHAUS ATTACK [12]



Spamhaus, a nonprofit anti-spam organization, had its **website and large parts of its email services knocked offline** by an unprecedented **300 gigabits of traffic per second** DDoS attack, despite having DDoS protection already in place.

The attack caused major issues for LINX, the London Internet exchange, and locked users out of Spamhaus' services.

MARCH 2012

THE SIX BANKS ATTACK [13]

Six major US banks were targeted by a wave of DDoS attacks in the early months of 2012. **Bank of America, JPMorgan Chase, U.S. Bank, Citigroup, Wells Fargo, and PNC Bank** were all victims of a **60 gigabit per second DDoS** attack carried out by hundreds of hijacked servers, making cyber security measures at the time useless.

The attack resulted in **millions of dollars in lost revenue**, expenses, customer service issues, and trust in online banking.

APRIL 2007

THE ESTONIA ATTACK [14]

Estonia was **brought to a standstill** when **major services** were rendered completely dysfunctional following a massive DDoS attack.

Many consider this event to be the **first act of cyber warfare** committed by Russia.

Estonia faced lost productivity, opportunity cost, remediation, and the acquisition of alternative web hosting at emergency rates estimated to be in the **billions of €**[15]. This ordeal led to the creation of **international laws for cyber warfare,** which are still used today.

How Anapaya Prevents DDoS Attacks

DDoS attacks can be daunting—but there is a solution that tackles the threat of DDoS attacks as we know it.

Anapaya prevents DDoS attacks by operating on an isolated network with paths hidden from the rest of the internet. This makes a SCION abled network unreachable for DDoS attacks. Additionally, the fast-failover capability allows for continued connection in the case of a DDoS attack while companies can avoid data routes they deem high risk, such as routes through countries with histories of DDoS attacks.

Visit www.anapaya.net

ANAPAYA

Sources

[1] Cloudflare DDoS attacks *reached 50 to 70 million requests per second*
[2] Microsoft DDoS attacks *targeting an Azure customer in Asia*
[3] *Large volumetric DDoS attack on* European Gambling Company
[4] ZDNet, *AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever*
[5] ZDNet, *Google says it mitigated a 2.54 Tbps DDoS attack in 2017, largest known to date*
[6] A10 Networks, *Five Most Famous DDoS Attacks and Then Some*
[7] Cloudflare, *Famous DDoS attacks | The largest DDoS attacks of all time*
[8] Forbes, *The Largest Cyber Attack In History Has Been Hitting Hong Kong Sites*
[9] A10 Networks, Five Most Famous DDoS Attacks and Then Some
[10] Cybersecurity & Infrastructure Security Agency, *NTP Amplification Attacks Using CVE-2013-5211*
[11] Reuters, *DDoS cyber attacks get bigger, smarter, more damaging*
[12] Computer World, *Update: Spamhaus hit by biggest-ever DDoS attacks*
[13] A10 Networks, *Five Most Famous DDoS Attacks and Then Some*
[14] Cloudflare, *Famous DDoS attacks | The largerst DDoS attack of all time*
[15] Wired.com, *Hackers Take Down the Most Wired Country in Europe*