DATA SHEET

The new approach to **DDoS security** for the **Fintech Industry**

Crunching the Numbers Against the DDoS Threat

It's no accident that DDoS threat actors are more interested in Fintech companies than ever before. Recent studies illustrate the significant targeting of the financial sector, marking a substantial increase in attacks within the **Europe, Middle East, and Africa (EMEA) region.**

Notably, there has been a **40%** surge in DDoS attacks comparing 2022 to 2023 in the EMEA region. **Cyprus** remains one of the most frequently attacked countries in Europe, underlining the necessity for cloud-compatible automated DDoS protection due to its concentration of financial companies and Forex brokers. Moreover, the cryptocurrency industry in the **Asia Pacific** continues to face relentless DDoS attacks in 2023.

A single hour of downtime costs can sometimes cost companies from **$1 million** to over **$5 million** per hour, with the added legal fines, fees, or penalties. This, in addition to increased (after the fact) DDoS security investments combined with cyber insurance premium increase.

The Main DDoS Challenges in Fintech?

Rapid Innovation: Fintech's rapid pace of technological evolution presents a challenge in keeping up with the latest cyber risks and defenses. The constant innovation and evolution create an environment where security postures evolve swiftly, leading to potential misconfigurations in deployed DDoS protections, thus heightening vulnerabilities.

Regulatory Compliance: Adhering to highly regulatory standards diverts resources and time away from DDoS security, causing a strain on Fintech companies. Compliance measures such as performing red team tests often fall short in covering the entirety of DDoS attack surfaces, as they typically cover less than 1% of the online services posture and do not provide full visibility and insights into the full DDoS vulnerability gap.

Third-Party Risks: Fintech firms heavily rely on third-party vendors for critical services, exposing them to additional cybersecurity concerns. These external providers may become targets for DDoS threat actors, potentially resulting in data breaches or other security vulnerabilities.

Here are some examples of successful and damaging DDoS attacks that got past the best mitigation systems, despite heavy DDoS protection investments.

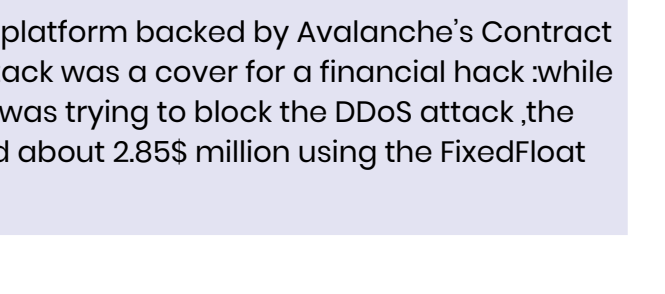
Are Fintech companies prepared enough to prevent DDoS attacks?

Country	Company	The Attack
		2023
USA	Stars Arena, backed by Avalanche	Stars Arena ,a social platform backed by Avalanche's Contract Chain - The DDoS attack was a cover for a financial hack :while the mitigation team was trying to block the DDoS attack ,the attackers transferred about 2.85$ million using the FixedFloat exchange service.
		2022
USA	Loopring	Loopring) LRC ,an Ethereum Trading Platform (was attacked immediately after its value was on the rise.
Switzerland	Swissquote	The online trading platform confirmed that its servers were the target of" a massive DDoS attack"
Hong Kong	Ifinex Inc.	The massive ransom DDoS attack resulted in requests for the cryptocurrency Tether's website increasing from 2,000 to 8,000,000within a few minutes.
USA	Solana Cryptocurrency	The attack ,the fourth in 12 months ,was likely caused by the constant creation of empty transactions on the network that act as congestion material and put the network offline.
Unknown	LooksRare NFT Marketplace	Hours after its launch ,the LooksRare website was inaccessible because of a DDoS attack .Some users could not connect their wallets and list their NFTs.

Why Are DDoS Attackers Interested in Fintech Companies?

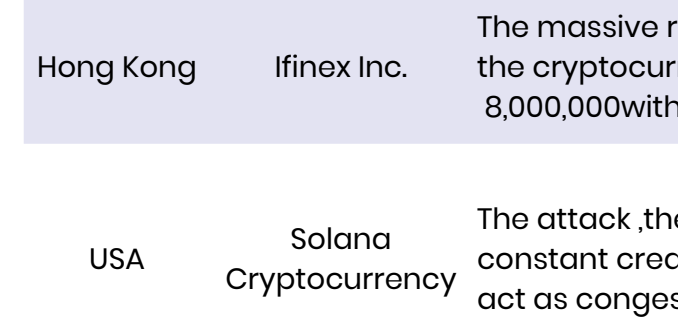
Ongoing Accessibility

Fintech companies' round-the-clock services, often accessible via mobile platforms, make them prime targets for DDoS attackers seeking to disrupt operations and damage reputations. A successful DDoS attack will quickly lead to downtime, and a tarnished reputation can be hard to repair after the fact.



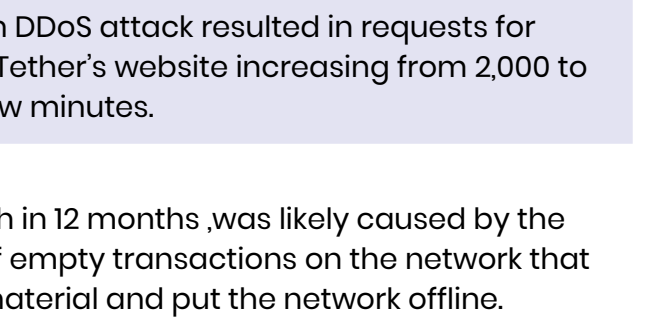
Constant Vulnerability

Frequent technological updates in the Fintech sector amplify DDoS risks, requiring constant reconfiguration of protections. Misconfigurations in the DDoS protections deployed remain the leading reason for successful and damaging DDoS attacks.



Data Protection and Ransom Incentives

Fintech companies house significant amounts of sensitive data, attracting DDoS attackers aiming to disrupt operations and potentially demand ransom. As a DDoS attack that shuts down operations may be a smoke screen for another malicious cyberattack, a Fintech company might end up paying the ransom demand that sometimes accompanies a DDoS attack.



Heightened Competition

Rising competition in the Fintech sector, especially within the cryptocurrency market, intensifies the risk of DDoS attacks launched by rival companies seeking to disrupt competitors' operations. Services like DDoS-for-hire further enhance these risks.

What Should Fintech Companies Do Against DDoS Attacks?

No matter which protection services are deployed, Fintech companies are highly exposed to DDoS attacks and the only way to remain DDoS resilient is to adopt non-disruptive DDoS testing and gain continuous and complete visibility into the DDoS security posture.

With patented non-disruptive DDoS testing, MazeBolt RADAR™ identifies volumetric, low and slow, carpet bombing, and multi-vector attacks, validating all targets and services, against all known attack vectors to identify all vulnerabilities. Only through identifying vulnerabilities and prioritized remediation can Fintech companies prevent a damaging DDoS attack, and eliminate the damaging time-to-mitigation (TTM) SLAs and the need for emergency response scenarios.

RADAR is a paradigm shift in DDoS protection: from reactionary to preventative remediation. This is the new approach to DDoS security: Preventative, Proactive, automated Protection