Visionary Online Bank Thwarts Major DDoS Attack and Extortionists with Akamai Prolexic Routed

> The Akamai solution minimizes the risk that we'll be unable to service our customers due to criminal attacks. This frees us from worrying about being the target of an attack and facing legal penalties, allowing us to focus on our business.
>
> — **Andreas Hellwig,** CTO, Fidor TecS

The Situation

Launched in 2009, Fidor Bank is a 100% online bank with a vision to be the European leader for online and mobile "community banking". The digital banking platform used by Fidor Bank was implemented by Fidor TecS AG, which continues to develop and operate the platform. Through Fidor's website, the bank's more than 35,000 customers can manage virtual currencies, check rates and connect with other banking customers. Fidor Bank is the first bank in the world where the social interactions of customers determine the overdraft interest: the more Facebook Likes, the lower the customer's interest rate. Customers are rewarded in other ways for their community participation, such as earning cash bonuses for answering other customers' finance-related questions. Another first, Fidor enables customers to see all account holdings – everything from savings and investments to precious metals and virtual currencies – on a single page.

The Challenge

Starting Friday, October 24, 2014, Fidor was the target of several large Distributed Denial-of-Service (DDoS) attacks launched by extortionists. The bank became aware of the first attack due to its 24/7 monitoring and alerting system. After analyzing the attack pattern, the bank implemented measures to block ports on its routers and redirect traffic. The next day on Facebook, Fidor published the extortion email sent by the attackers, which threatened to increase the intensity of the Internet attack on the bank's website if it did not transfer 4,000 Euros as BitCoins. When the bank did not pay up, the attack pattern changed and the load increased to over 85 Gbps, overwhelming Fidor's firewall and the servers in its data centers. Ultimately, the attacks led to the bank's services being offline for about eight hours. According to Andreas Hellwig, CTO for Fidor TecS, "The bank employed offline emergency processes, allowing customers to fulfill banking via phone, and used social media channels and other websites to communicate with customers. However, we knew we needed to find a way to prevent and mitigate future DDoS attacks."

The Goals

Fidor Bank needed to meet three key requirements to support its objectives:

- **Mitigate all DDoS attacks.** The bank wanted to prevent all future DDoS attacks so it could ensure uninterrupted services for its customers.
- **Augment in-house expertise.** Fidor Bank wanted to tap into cybersecurity expertise to better understand the current and future threat landscape.
- **Satisfy the authorities.** The bank needed to prove to government agencies in Germany that it was taking all necessary security measures.

Company

Fidor Bank
Munich, Germany

www.fidor.de

Industry

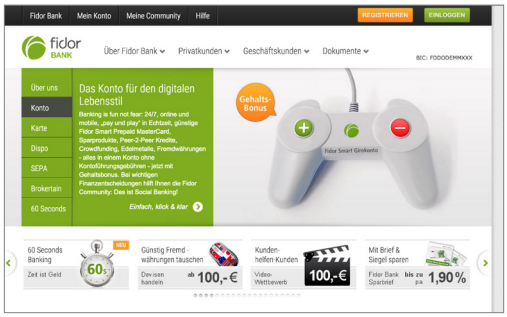
Financial Services

Solutions

- Akamai Prolexic Routed deployed in an Always On configuration

Key Impacts

- Stopped 85 Gbps DDoS attack within 30 seconds
- Discouraged future attacks from extortionists
- Eliminated worry about criminal attacks and downtime
- Gained access to expert insights and guidance about cybersecurity
- Satisfied authorities with acceptable security measures



Fidor Bank

Why Akamai

Choosing a Proven Solution

Because of the public nature of the bank's response to the attack, many Internet security vendors reached out to Hellwig. Ironically, it was on the 2015 roadmap for Fidor to engage a professional DDoS protection provider, so Hellwig and his colleagues were already well aware of Akamai. "We prioritized our evaluation and ultimately chose to use Akamai's Prolexic Routed solution deployed in an Always On configuration, as well as the Application-Based Monitoring option," he explains.

Hellwig selected the solution for a number of reasons, including Akamai's experience with large-scale attacks, the structure and worldwide presence of Akamai's global scrubbing centers, and a recommendation from another large German bank. It also appreciated Akamai's quarterly State of the Internet reports, along with the relationship between Akamai and the Bundesamt für Sicherheit in der Informationstechnik (BSI), a government department for Information Security in Germany.

Immediately Stopping DDoS Attacks

As a cloud-based service, Prolexic Routed provides protection against DDoS attacks and has allowed Fidor to scale as required.

The day after implementing the Akamai service, Fidor received a second email from the extortionists announcing another big DDoS attack. Within a few hours, the bank's data center was hit by an attack measuring over 85 Gbps. This time, Prolexic Routed completely mitigated the attack within 30 seconds. Once the attackers realized Fidor had implemented a solution and successfully thwarted the attack, they stopped attacking.

As Hellwig explains, "The Akamai solution minimizes the risk that we'll be unable to service our customers due to criminal attacks. This frees us from worrying about being the target of an attack and facing legal penalties, allowing us to focus on our business."

Gaining Professional Support for Cybersecurity Threats

Simultaneous to deploying Prolexic Routed, Fidor hosted a roundtable to discuss criminal DDoS attacks. Panelists included German local police, Bavarian police, and experts from Akamai's advanced advisory service. According to Hellwig, Akamai brought specialized knowledge and expertise to the discussion, and confirmed that Fidor had made the right choice. "This advisory service provides expert insights and guidance, keeping us up to date and safe from new attack types, helping guarantee the availability of our online services today and in the future."

Satisfying Expectations

German regulations require Fidor to report all criminal and cybersecurity issues to authorities and BSI. In addition, Fidor is audited annually to prove it is taking all necessary security measures. "Akamai is respected DDoS protection in the banking world, which bolsters our reputation with authorities. By using this solution, we can show that we are doing all that is expected of a bank to protect against cybersecurity issues," says Hellwig.

Going forward, Fidor plans to take advantage of the Application-Based Monitoring solution that is focused on monitoring application-layer (Layer 7) traffic, including SSL-encrypted traffic, and tracks 25 unique dimensions. "This will make it possible for us to monitor and identify the sophisticated application-layer 7 abuses, service attacks and malicious activities that can cause downtime," concludes Hellwig.

About Fidor Bank

FIDOR Bank AG (http://www.fidor.de) is an internet-based direct bank, licensed in Germany, and a B2B bank for innovative banking and community software solutions. Private and corporate customers use the Fidor Smart current account with its classic and innovative finance apps as their main bank account. The banking middleware Fidor OS enables the bank's B2B partners to profit from novel functionalities and a community solution for a global target group of digital natives.

Akamai FASTER FORWARD

As the global leader in Content Delivery Network (CDN) services, Akamai makes the Internet fast, reliable and secure for its customers. The company's advanced web performance, mobile performance, cloud security and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise and entertainment experiences for any device, anywhere. To learn how Akamai solutions and its team of Internet experts are helping businesses move faster forward, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 40 offices around the world. Our services and renowned customer care enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on www.akamai.com/locations.