Financial Services Firms Defend Against Distributed Denial of Service Attacks and Data Breaches While Maintaining High Performance and Availability

Situation

During 2012 and 2013, large scale distributed denial of service (DDoS) attacks of up to thirty gigabits per second and up to 18 million requests per minute were launched against insurance companies, brokerage firms, credit unions, asset management firms, small banks, Canadian and European financial institutions, and thirty of the top fifty US banks. When these attacks (against sites not protected by Akamai) were successful in causing outages or performance degradation, the attacks continued for days at a time and were repeated week after week.

The Challenge

DDoS attacks against financial firms have continued to grow in size and frequency. The specific tactics and sophistication of the attacks have evolved rapidly. Outages have prevented customers and prospects from opening new accounts, viewing account and billing information, conducting online transactions, and accessing brand and product information. In other cases, while sites have technically been available during an attack, DDoS defense measures have caused response times to degrade up to 30 to 50 seconds, making sites effectively down from an end-user perspective.

Responding to outages and performance problems has pulled IT staff away from priority projects, causing delays in critical IT initiatives. Even worse, fraud attempts have increased during DDoS attacks because attackers realize that institutions are distracted while resources are being diverted to defend and repair impacts from DDoS.

Characteristics of the attacks include:

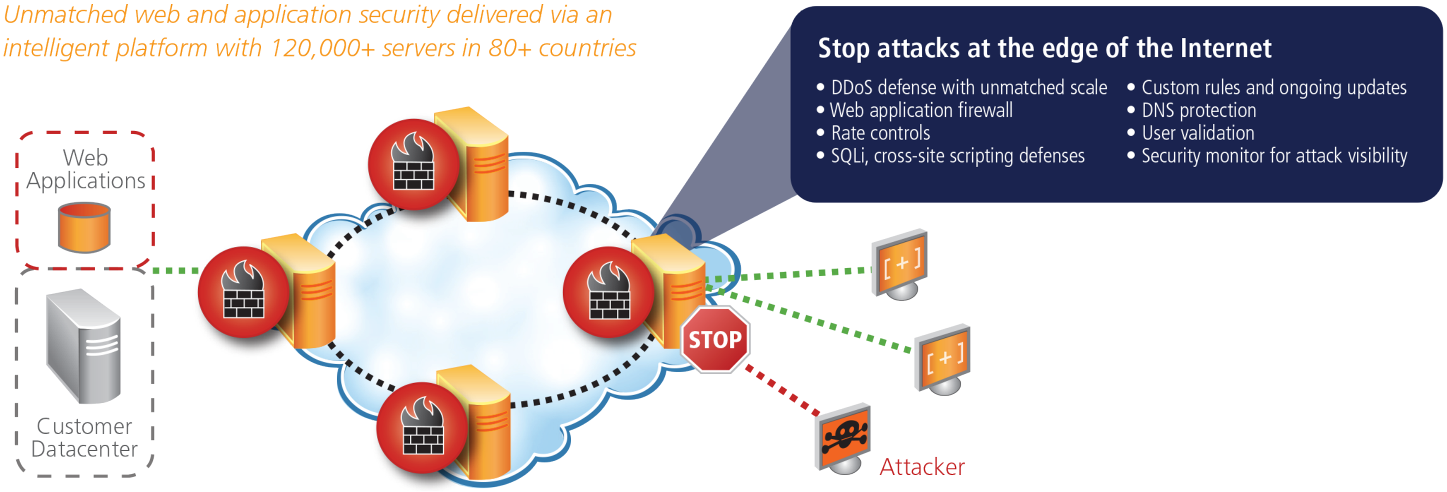
- Use of a growing army of compromised servers to grow attack volume (botnets)
- Volume: 18 million requests per minute, traffic levels of 30 gigabits per second, network flood traffic of up to 120 gigabits per second
- Attacks against DNS, SSL, content such as disclosure PDFs, home pages, mobile, and transaction sites
- Large scale burst probes in attempts to bypass rate-limiting controls
- Addition of valid argument names, random values, and random query strings
- Probing for 10-20 minutes on multiple targets, then piling on volume at targets where attacks work
- Attacks that extend over multiple days and through the weekend
- Attacking DDoS-distracted institutions to perform data and money exfiltration fraud

INDUSTRY
Financial Services

SECURITY SOLUTIONS
- Network and application level defenses
- Web application firewall
- DNS protection
- Dashboard for attack and defense visibility
- Support for security regulation compliance
- PCI compliant infrastructure
- Unmatched scale to stop high volume attacks
- 120,000+ cloud-based servers in 80+ countries

KEY IMPACTS
- Absorbed peak attack of 18 million requests/minute and 30 gigabits/second
- "Always on" to maintain 100% availability
- Maintained performance during attack
- Offloaded up to 99% of HTTP and SSL attacks at Internet edge, far from datacenter
- Prevented data breaches by stopping SQL injection and cross-site scripting
- Provided real time visibility into attack characteristics and defenses
- Prevented outages to reinforce customer satisfaction and brand

Unmatched web and application security delivered via an intelligent platform with 120,000+ servers in 80+ countries



Financial Firms Defend Against Cyber-Attacks

The Goal

Defend against large scale volumetric denial of service and data breach attacks in order to:

- Maintain 100% availability for web properties including new account sales, online transactions, customer service portals, mobile sites, and product and service information
- Maintain or improve fast page loads and responsive performance
- Prevent data breaches and protect personal and corporate information
- Enable staff to focus on priority projects versus diversion to attack-related efforts

Why Akamai

Akamai has successfully and consistently defended against some of the largest DDoS attacks on the financial services industry. In particular, Akamai provided highly effective defenses against a nine month campaign of large-scale DDoS attacks conducted in 2012 and 2013 against US financial institutions. During a variety of different DDoS attacks against web properties protected by Akamai, attackers were unable to cause outages or degrade performance.

In comparison, alternative defenses have often struggled with the volume of these large scale attacks. As a result, extended outages and serious degradation of performance has been observed, for example, degrading from 5 seconds or less of "normal" response time up to 50 seconds of response time. A number of institutions have asked Akamai to assist on an emergency basis when their established defenses have failed.

Akamai has been able to provide protection with no negative impact on site performance. In fact, new users of Akamai's "protect and perform" services have seen their performance improve because of Akamai's inherent route optimization capabilities.

Akamai's defensive capabilities are always turned on and natively in the traffic path to provide continuous protections. Some other types of DDoS defenses require manual intervention to reroute traffic and, during the delay before these defenses are turned on, an outage is likely to occur.

It is difficult to stop an attack of the large scale volumes (10-30 gigabits per second) experienced over the past year, within the facilities of a corporate datacenter. This difficulty has been demonstrated by outages of web properties at quite a few of the world's largest financial institutions.

Akamai's security services depend on a fundamentally different architecture, massively distributed, which employs more than 120,000 servers, positioned in more than 2,000 locations in 750 cities across 80+ countries, with direct connections to more than 1,100 of the world's major network carriers. By comparison, many competing service providers are limited to about five to thirty locations and this makes them highly vulnerable to bandwidth and throughput limitations during large scale DDoS attacks.

Akamai's scale is unmatched, as of June 1, 2013, its network delivered:

- 500 billion hits / day
- 19+ million hits / second
- 100 million page views / second
- 1,000,000+ concurrent streams
- Peak traffic of 10 terra bits per second of traffic on an average day, and can handle peaks of substantially more volume

Akamai is able to take the lessons learned from defending a host of individual customers and apply them across our entire customer base with, for example, security rule updates. The web security services offered by Akamai have many dimensions including:

- DDoS mitigation at network & application layers
- Potential offload of web traffic from datacenter of up to 99%
- Cached content served from Internet edge during attack
- Cloak datacenter to stop direct-to-origin attacks
- Web application firewall services:
  - Rate controls
  - Defenses against SQL injection
  - Defenses against cross-site scripting
  - Custom rules
- Threat defense rule update services
- SSL protection
- DNS protection
- User validation
- Adaptive caching
- Site failover
- Access control
- NetStorage
- Log delivery service
- Security monitor for visibility into attacks and defenses
- Compliance management: ISO Security Standard (27002)
- Ongoing professional services support for security optimization

Akamai FASTER FORWARD

Akamai® is the leading provider of cloud services for delivering, optimizing and securing online content and business applications. At the core of the company's solutions is the Akamai Intelligent Platform™ providing extensive reach, coupled with unmatched reliability, security, visibility and expertise. Akamai removes the complexities of connecting the increasingly mobile world, supporting 24/7 consumer demand, and enabling enterprises to securely leverage the cloud. To learn more about how Akamai is accelerating the pace of innovation in a hyperconnected world, please visit www.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 are designed to 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.