Major Investment Banking Firm Protects Data Centers with the Arbor Networks® APS

Cyber Attack Campaigns

The wake-up call of attack campaigns targeting the financial sector were the Operation Ababil attacks of 2012. These were a coordinated mix of sophisticated application-layer attacks on HTTP, HTTPS and DNS alongside volumetric components on a variety of TCP, UDP, ICMP and other IP protocols. They were simultaneous, at high bandwidth, and targeted multiple financial companies.

"We felt that DDoS protection based solely in the cloud was only partial protection. We wanted more control of our online traffic and connections to the Internet. But what really sold us was the depth and experience of the Arbor Networks team. The more peers we spoke to, Arbor just kept coming up again and again."

Network Engineering Manager

The Business

A major Wall Street investment banking organization manages trillions in assets and providing investment strategies, wealth management, trading and market-making services through offices in over 30 countries. The success of their business—of their customers achieving their goals—depends upon reliable, secure online infrastructure and services. A McKinsey study, "Strategic choices for banks in the digital age," estimates that by 2018 42 percent of revenue will come from online or mobile channels.

Challenge

Like other financial institutions around the world, the company has increasingly been the target of coordinated, multi-stage attack campaigns. They also were aware of the Federal Financial Institutions Examination Council's (FFIEC) statement in April of 2014 calling attention to the threat posed by Distributed Denial of Service (DDoS) attacks. Forward-thinking networking, security and operations executives within the organization were looking for increased DDoS and attack campaign protection for their Internet-facing data centers. They realized they needed greater traffic insight and more rapid, flexible countermeasures than a Cloud Service Provider (CSP) solution alone could provide.

They needed more detailed, real-time insight and control of traffic to and from their data centers. The challenge was recognizing attack components quickly—such as the detection of traffic micro-bursts from data centers—and changing attack vectors. They needed in-line mitigation capabilities that could alert via their existing network management systems. Relying upon their CSPs to re-route and effectively scrub evolving attack vectors was acceptable for 'simple' volumetric attacks, but suboptimal against more sophisticated attacks that might include targeting the application-layer. Relying solely on cloud-based protection simply did not give them the control and protection they required.

Given the growing complexity of their infrastructure, applications and sheer volume of network traffic, automation and ease-of-use were also critical decision-making factors. They did not want to add staff to identify threats; any solution needed to automate as much of the 'analysis' and countermeasures as possible. Naturally, the tool could not take weeks to learn and needed to be relatively easy to use.

Timeline

The financial industry—particularly when it comes to choosing security solutions—relies heavily on shared experience, reputation and talking with their peers. For example, this organization contributes to and has executives who participate in the FS-ISAC (Financial Services Information Sharing and Analysis Center).

Arbor Networks APS

- Enhanced, Real-Time Traffic Visibility and Control
- Proactive DDoS Detection and, Configurable, Automatic Mitigation
- Full Suite of Attack Countermeasures
- ATLAS® Automated Threat Updates
- Built-in SSL Inspection, including SSL Negotiation Packets
- Inbound and Outbound Advanced Threat Protection
- Real-Time Reporting and Forensics

This firm had several solutions in their lab for evaluation as a DDoS protection solution, including a next-generation firewall and an Intrusion Prevention System (IPS) that had recently added "DDoS protection" to its roster of features. When one of their peers in the industry suffered a DDoS attack, the security leadership team took a closer look at the capabilities of these devices.

Fearing that they too could be the target of a DDoS attack, the organization decided to also evaluate purpose-built on-premise DDoS solutions. Their goal was to evaluate and have a solution in place in three months. Checking with their network of security professionals, including employees within the company that had implemented and used on-premise DDoS protection solutions, Arbor Networks was identified and contacted about its APS, which was selected for immediate lab trial.

What they quickly discovered in the lab was eye-opening. Most perimeter security devices operate with a fixed configuration that needs to be set once and then largely forgotten until changing needs require the configuration be revised. For example, most firewalls act as a policy enforcement device, and the configuration is the manifestation of that policy. It's similar to IPS where the configuration might be nothing more than instructing the device to block all known intrusions as matched by signature. Again, the device is installed, configured, and largely left unmonitored to perform its job.

DDoS attacks are fundamentally different; the point of a DDoS attack is to overwhelm the website with traffic that pretends to be legitimate. The attacker generates traffic that goes through much of the same motions as normal traffic would but ultimately results in no productive work and simply consumes resources. Maintaining the appearance of normal traffic allows the attack to bypass firewalls, as it meets the defined policy configuration, and typically does not make use of known exploits that would be detected by an IPS.

Unlike worms and automated scans, a DDoS attack generally represents a real human actively targeting the website or network under attack. And what makes DDoS attacks particularly difficult to mitigate is that there are many different ways an attacker can generate normal-looking traffic with the intent to overwhelm a website or network. So if an attacker is finding one particular method of DDoS attack doesn't work very well, they might try a different tactic or invoke multiple forms of DDoS attacks simultaneously.

Often the best defense against a human attacker evolving their DDoS attack is a human defender pushing back, armed with the best defense tools. When defending against an active DDoS attack, the defender needs to quickly analyze the attributes of the attack, understand how the attack is evolving, and then adapt the configuration to best mitigate the current form of the attack. They might need to repeat this process regularly while the DDoS attack is ongoing. And since the website or network might be overwhelmed with DDoS attack traffic, legitimate users might be unable to access the website or simply find it off-line. Restoring availability is critical, and time is of the essence.

The perimeter security devices under evaluation offered poorly integrated monitoring or security analysis and buried the configuration in the depths of the user interface or even in an arcane text file. If the user needed to respond quickly to an ongoing attack they struggled with a user interface that was not designed for use during an urgent security incident. Understanding that a single defense configuration might eventually be bypassed, they found that APS is designed to empower the defender with an optimized operations interface structured into a DDoS defense lifecycle workflow. APS directs the user from attack detection via alerting, to attack analysis through detailed traffic and packet analyzers, to defense adaptation, and finally post-attack investigation, all through a single and contiguous workflow. Time is saved and availability more quickly restored because the user has immediate and efficient access to powerful tools and methods to analyze and mitigate any DDoS attack.

Bottom Line

Based on their evaluation of APS' performance inline, and Arbor Networks' experience and reputation within the financial sector, the organization ordered additional APS solutions to protect their main US data centers. The process from when the Arbor Networks team was originally contacted to when systems had been evaluated inline and a decision made, took less than three months.

The company was convinced that APS could provide them with the required insight, analysis and real-time control needed to better protect their data center operations. They particularly liked the 'force-multiplier' effect Arbor Networks Spectrum™ had for their existing staff: the configurable threat alerts and automated countermeasures. The user interface was easy to use and integrated with their current network management system; it did not require additional staff nor extensive training of existing staff.

In the end, they decided that purpose-built was a better solution than relying on a new feature within an existing solution. After all, the very availability of their network, services and applications were at stake. That is true risk management.

ARBOR® NETWORKS

The Security Division of NETSCOUT

Corporate Headquarters

76 Blanchard Road
Burlington, MA 01803 USA

Toll Free USA +1 866 212 7267
T +1 781 362 4300

North America Sales

Toll Free +1 855 773 9200

Europe

T +44 207 127 8147

Asia Pacific

T +65 68096226

www.arbornetworks.com

SB/FINANCIAL/EN/0416-LETTER