FROM THE FRONTLINES:
HOW A MULTINATIONAL BANK HANDLED A RANSOM THREAT AND SSL-BASED ATTACK

In 2016, the financial services industry suffered 44 million cyber-attacks, more than any other industry. Everything from hacktivist-motivated attacks to Internet of Things (IoT) assaults targeted leading banks, financial service institutions, and markets, resulting in hundreds of millions in lost revenue.

Perhaps more than any other industry, security professionals at financial service firms truly are on the frontlines of today's cyber-attacks, combating everything from ransomware to SSL-based attacks. In this piece, a senior network architect at an EMEA-based international banking group shares his notable experiences protecting his organization's network perimeter from cyber security threats.

Managing the Ransom Reality

Cyber ransom is a growing threat across industries, and we have experienced this phenomenon firsthand. In November of 2015, our organization received a typical ransom email from the Armada Collective, which was quickly followed by a teaser flood attack that the bank proactively mitigated. We actually detected and mitigated the teaser flood attack before we discovered the email, which had been sent to an unattended mailbox while the company was closed. With a hybrid DDoS mitigation solution in place, the flood attack had no impact and was immediately diverted to a scrubbing center for cleanup.

Our organization is geographically separated from the rest of the world. This has implications on both the organization's ability to protect itself (for instance, in terms of latency in times of diversion) and also limits the ability of hackers to use volumetric attacks; hackers can't get even half a terabyte of traffic here. For us, a teaser attack may bring 300 megabytes of traffic. As a safety precaution, when we receive a flood attack and ransom note, we divert network traffic to the scrubbing center of our DDoS mitigation vendor, Radware, before the ransom payment deadline. We believe that hackers executing the ransom attack will observe the traffic being diverted and will realize the futility of launching a teaser attack. We also believe that it sends a clear signal to Armada Collective and other ransom groups. By taking powerful and decisive action, we send the message that we won't be victimized.

In April of 2016, we received another ransom email purporting to be from Lizard Squad. Because we communicate frequently with our local banking risk management association, we learned that the emails were from a copycat. Since we identified it as a hoax, we decided not to divert traffic. However, we did receive a small teaser attack and relied on Radware's Emergency Response Team of experts for support.

Facing the Camouflaged Traffic Flood

Since 2016, the diversity of attack vectors has increased and the bank has experienced a fourfold increase in burst attacks. At the same time, attacks lasting more than an hour are decreasing. The trend seems to be shifting toward very short, "hit and run" assaults.

Yet not all attacks are burst attacks. In September 2016, we received an attack that was relatively small (only 2-3 Gbps) but lasted over four hours and gradually evolved in several stages. First, we noticed that some of the attacks were ping-back attacks. We experienced attacks of 16,000 SYN connections which were mitigated via our on-premises DDoS protection appliance. After the Half-SYN attack, there was an HTTP flood with about 2,000 sources in the attack, which was also successfully mitigated. However, we had difficulty mitigating the full HTTPS flood attack. It was the first time we experienced an encrypted attack, highlighting the need for dedicated protection against encrypted attacks that leverage SSL standards to evade security controls.

Normally the bank faces UDP fragmented attacks followed by a DNS reflective attack. In this case, we were hit with a typical SSL attack that we were not prepared to mitigate. Typically attacks only last three to four minutes and immediately follow each other, but this SSL attack lasted an hour and a half, putting our defenses under tremendous stress because of the computing resources the attack consumed. In fact, we generated so much response load that it pushed our outbound connection to its limit; it tripled our usual throughput.

Lessons Learned

1. **Experience has taught us the benefits of behavioral analysis over rate-limiting analysis.**
   In the past, the bank tested a DDoS mitigation solution that leveraged rate-limiting technology and discovered that using behavioral analysis provided a significant advantage since it doesn't block legitimate traffic, thereby allowing us to maintain our service levels.

2. **The importance of time to mitigation.**
   By having the ability to develop attack signatures in real-time, we have been able to mitigate attacks in as little as 20 seconds. Our traffic pattern during the day is heavy and at night it's quieter, so we had to do some fine tuning to reflect different behavioral traffic patterns at different times of the day.

3. **The advantages of a single vendor hybrid DDoS protection solution.**
   Now the baseline on our perimeter and the baseline on the Radware scrubbing center are identical. As a result, we can mitigate attacks faster versus another solution that would have to reanalyze traffic in the cloud again, or require a lot of manual tuning to reach the same protection level.

4. **Let the experts deal with attacks.**
   Knowing we are backed up by Radware's Emergency Response Team, we can focus on our daily tasks knowing that we can rely on their expertise within seconds. It means the bank isn't required to have that expertise in-house, which is important since the attack landscape is always evolving. Access to this level of expertise should be part of any response and business-continuity strategy.

Our networking team preferred no form of Border Gateway Protocol (BGP) on-ramping or off-ramping. Nor did they want a security application that would interfere with any routine decisions. We suggested leveraging Radware's Cloud DDoS Protection and a flow monitor that is deployed out-of-path so the bank's IT security team only engages with larger attacks that cross certain bandwidth thresholds. That all takes time and short, low-bandwidth attacks could "fly under the radar." With the behavioral engine, we can detect smaller, shorter attacks. With another DDoS mitigation solution, we would never have detected those attacks.

Tips for Financial Service Security Professionals

In this part of the world, there is a belief that hard-to-detect attacks do not represent a critical threat, but for a bank, nothing could be further from the truth. We feel the most effective way to protect our organization's infrastructure in the event of an attack is to have protection installed in-line. This eliminates the need to analyze events and reroute traffic and eliminates any infrastructure obstacles to successfully mitigating an attack. There's increased visibility because the solution is always on. With automated attack mitigation—including behavioral analysis that delivers continuous visibility and forensics—we'll never be left vulnerable to evolving DDoS attacks. Detect where you can; mitigate where you should.

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.