Neustar® Insights
The Recent DDoS Attacks on Banks: 7 Key Lessons

By Rodney Joffe, SVP and Senior Technologist, Neustar

What should banks large and small learn from the DDoS attacks that crippled websites and shook consumer faith in the industry?

Here's what one of the world's leading experts has to say.

neustar®
Real Intelligence. Better Decisions.™

Starting in mid-September, one of the largest and most sophisticated DDoS attacks ever targeted the titans of American banking. Initially, victims included Bank of America, JPMorgan Chase, Wells Fargo, PNC Bank, and U.S. Bancorp. In the weeks to come, others would also feel the pain. Websites crashed, customers were unable to make transactions and IT professionals and PR gurus went into panic mode. Leon Panetta, U.S. Secretary of Defense, said the attacks foreshadowed a "Cyber Pearl Harbor." While evidence still continues to emerge, the following lessons are clear enough. All spell danger, for banking and the world in general.

1. DDoS attacks have entered a dangerous new phase. A combination of size and intelligence marked these attacks. While they peaked at between 60 and 150 Gbps (most DDoS attacks are smaller than 1 Gbps), the assaults on banks involved only 2,000–3,000 computers, not the tens or hundreds of thousands we've seen in botnets before. The difference: most of the compromised systems were powerful business machines, rather than traditional home computers, with access to significantly more bandwidth to help flood connections. First, the attackers hit web resources with large numbers of HTTP (web) traffic and then moved on to DNS servers, which tend to be more vulnerable. The result was a curious hybrid: a highly strategic, brute-force attack that left its victims reeling. Clearly, the attackers were well acquainted with how the Internet works.

2. Who did it and why are less important than the fact it could be done. An Islamic group calling itself the Cyber Fighters of Izz ad-din Al Qassam claimed credit for the attacks, allegedly retaliating for an anti-Muslim video. While some suspect the hand of Iran behind these concerted strikes, no one has provided definitive proof of the culprits' identities or motives. It's possible a nation-state or terrorist cell is guilty. It's also possible for the proverbial basement genius to have done it. And that's the scariest part. Anyone with sufficient knowledge could have pulled this off. Whoever it was didn't need millions of dollars or a global support network. If you truly know how the Internet is architected, you can succeed in taking down whole industries, no matter who you are and whatever your reasons may be.

3. Brand reputations have suffered. So far, nobody has reported stolen data or major revenue losses, though of course most organizations are in no rush to admit such breaches. Unquestionably, however, America's largest banks have lost a measure of public trust. Online forums lit up as website outages dragged on. Bank customers wondered aloud about security readiness. Some feared for their data and ultimately their money. As September rolled into October, there were concerns about defaulting on mortgage payments and other monthly bills because customers couldn't log in to their bank accounts. While some banks did a good job of keeping customers apprised, no one had reassuring news. The best they could do was spin.

4. Traditional DDoS protection proved to be ineffective. Most companies rely on firewalls and intrusion detection/protection systems to repel DDoS attacks. Some even have their own DDoS mitigation appliances, though many lack the trained staff to wield them effectively. When banks got socked by malicious HTTP traffic, firewalls may have worked to a point but finally turned into bottlenecks. And when enormous amounts of bad DNS traffic showed up, it was game over. Traditional systems simply were not up to the task. Pipes got flooded, outages occurred and the cavalry was called in – third-party DDoS protection specialists with cloud-based solutions affording more bandwidth and a better chance of success.

5. Smaller banks weren't hit, but are more vulnerable. Think about it. The largest banks have the budgets to spend on DDoS protection. While their solutions couldn't stop these recent attacks, they can stop most – the 90% less than 1Gbps in size. Small banks, on the other hand, lack the protection to stop even these. A modest-sized attack can cripple their operations. This makes local and regional banks extremely vulnerable. Third-party solutions, especially affordable on-demand services, are a good bet for smaller players who cannot build their own.

6. The attacks demonstrated the need for holistic DDoS protection. It's not nearly enough to have a customized firewall or a mitigation appliance, especially one nobody has thought to tune in months. To repel today's attacks you also need enormous bandwidth, skilled mitigation staff and diverse technologies, a mix that stops both HTTP and DNS attacks along with the application-layer attacks that have become so popular. In other words, you have to be ready for anything. Building on the bank attacks, the next wave of DDoS will surely be comprehensive – in strategy, tactical skill and destructive power.

7. The Internet itself was the attackers' arsenal. Yes, for years now DDoS attackers have marshaled botnets to do their bidding. But the bank attackers showed an unprecedented understanding of the Internet's potential as a kind of weapons storehouse. Everything they needed was out there for the taking: high-capacity servers, bandwidth galore and information on the business networks in their crosshairs. The attackers showed great patience and impressive intelligence gathering. They clearly learned from past attacks and successful defenses. Their own success in taking down the nation's largest banks will prove to be an "Aha!" moment for aspiring miscreants. Knowing there is no protocol to stop attacks at their sources, future attackers likewise will plunder the Internet, cobbling together the resources and bandwidth to flood pipes, take down websites and leave business giants helpless.

Last thought: The banking industry leads the world in protection and security practices. If these attacks could happen to banks, they can happen to anyone. They truly are a when, not an if.

Rodney Joffe

Senior Vice President & Senior Technologist

Rodney Joffe is Senior Vice-President and Senior Technologist of Neustar, Inc. His responsibilities include defining and guiding the technical direction of the company's Neusentry™ security offering as well as heading the company's cybersecurity initiatives.

Joffe joined Neustar in 2006 after the acquisition of UltraDNS Corporation, a directory services company, he founded in 1999. Prior to founding UltraDNS, Joffe was the founder and CTO of Genuity, one of the largest Internet Service and Hosting Providers in the world. Joffe is frequently called upon to assist Federal authorities with regard to investigating and protecting against cyber-crime and cyber-terrorist activities. He regularly briefs the Executive and Legislative branches on these subjects. He is the co-chair of the FCC's CSRIC Network Security Best Practices sub-committee, and sits on the ICANN Security and Stability Advisory Committee (SSAC). Joffe participated on the planning committee for the DHS's CyberStorm II International Cyber-Terrorism exercise in 2008 and, in 2010 was a lead on the core scenario design team for CyberStorm III.

Joffe is also a founder and currently chairs the Conficker Working Group, acknowledged as a "BCP" (Best Current Practice) model for public/private partnerships for APT (Advanced Persistent Threat) mitigation. He has also provided guidance to and sits on four similar Threat Focus Cells geared towards other APTs.

FOR MORE INFORMATION

Call +1.877.367.4812
Online www.neustar.biz/enterprise

About Neustar

Neustar, Inc., (NYSE: NSR) is a trusted, neutral provider of real-time information and analysis to the Internet, telecommunications, information services, financial services, retail, media and advertising sectors. Neustar applies its advanced, secure technologies in location, identification, and evaluation to help its customers promote and protect their businesses. More information is available at www.neustar.biz.

21575 Ridgetop Circle, Sterling, VA 20166
+1 571 434 5400 / www.neustar.biz

V1-10/26/2012

neustar®
Real **Intelligence.** Better **Decisions.**™