No Financial Institution is Too Small a Target for DDoS Attacks

How to Prepare for and Defend Against the Ever-Present Threat

Contents

Brought to you compliments of:

Dell SecureWorks

Distributed denial-of-service (DDoS) attacks are prevalent and growing, especially in the financial services industry. According to a Ponemon Institute survey, 64% of banking IT professionals reported a DDoS attack in 2012, and 43% expected attacks to increase in 2013.[1] Yet the same survey found that only 30% of respondents said their banks are planning to implement anti-DDoS programs within the next six to 12 months.

Threat actors can create significant havoc with a single DDoS event. A survey by Neustar indicated that more than 80% of financial services firms estimate a loss of $10,000 per hour during a DDoS-related outage.[2] The same report found that:

- 38% of DDoS attacks last more than 24 hours.
- More than a third of attacks require six or more employees to mitigate.

These statistics amplify the need for financial institutions of any size to develop DDoS preparedness and remediation strategies. Cyberthreat actors don't discriminate — they target both large and small organizations and exploit weaknesses wherever they can.

[1] "More Than Half of Banks Hit by DDoS Attacks Last Year, Study Finds," Corero Network Security Inc., Jan. 23, 2013

[2] "DDoS Survey: Q1 2012 When Businesses Go Dark," Neustar Insights, 2012

Since September 2012, the top 50 financial institutions in the U.S. have been targeted by a well-organized DDoS campaign called Operation Ababil. These highly publicized attacks were a wakeup call for the industry to strengthen security controls beyond the network perimeter.

While Operation Ababil targeted large banks, smaller institutions are also in the crosshairs.

In June 2013, the Office of the Comptroller of the Currency (OCC), which regulates national banks, warned community bankers that any-sized organization is at risk. It noted that financial institutions with fewer than 250 employees have increasingly been targeted by DDoS attacks. The OCC's advisory followed similar warnings by other financial agencies:

- In February 2013, the Financial Services Information Sharing and Analysis Center issued an alert regarding an increase in DDoS attacks targeting smaller financial institutions.
- Concurrently, the National Credit Union Administration (NCUA) directed all federally insured credit unions to take measures to mitigate DDoS risks.

Case in point, a regional bank in San Francisco fell victim to a DDoS attack on Dec. 24, 2012. Organized cybercriminals distracted the bank's security team to take over an online business account. They were able to steal and launder nearly $1 million.[3]

In March 2013, Maine-based TD Bank and Cleveland-based KeyBank experienced DDoS attacks within days of each other. The attack on TD Bank created online and mobile outages. KeyBank's website remained functional, but users experienced slower response times.

DDoS Attack Tradecraft

DDoS attacks are designed to flood a Web server with traffic until it overloads and becomes unavailable to users. In 2000, Yahoo was a victim of one of the first attacks, which have since become commonplace. Anyone can go online now and literally rent a DDoS attacker for pennies per minute. Another option for those with ill intent is to obtain a DDoS malware kit and execute attacks themselves with relative ease, regardless of their technical savvy.

Common DDoS malware kits include Dirt Jumper, Pandora and Armageddon. Such tradecraft are created solely to execute DDoS attacks and are easily available in the cyber underground market.

If an organization isn't prepared in advance, there isn't much that can be done to stop a DDoS attack once it's started. Controls must be in place to handle the spike in traffic and requests, or service will be degraded and potentially disrupted.

10 Tips to Prepare for DDoS

No organization can completely eliminate the risk of a DDoS outage — even the most resilient network and security infrastructures have breaking points. The best way to mitigate the risk is to prepare for future attacks.

[3] "DDoS Attack on Bank Hid $900,000 Cyberheister," Krebs on Security, Feb. 19, 2013

The Dell SecureWorks Incident Response Team recommends the following tips to help organizations prepare for DDoS attacks:

1. Perform risk assessments to identify critical systems and downtime tolerance.
2. Create an incident response plan and test it regularly.
3. Consider an off-site host for disaster recovery to deflect high-risk targets away from your network.
4. Talk with your Internet service provider and/or Web hosting provider. Identify their risks, ensure proper traffic management controls are in place and determine what support they will provide in the event of a DDoS attack.
5. Implement security awareness training for network users.
6. Ensure that security controls are in place for systems used to process online transactions. Secure Sockets Layer should be used for authentication and transactions only.
7. Identify a plan to disable nontransactional activity.
8. Consider use of a DDoS mitigation provider.
9. Monitor the global threat landscape to understand the latest attack trends.
10. Have a plan to communicate to customers during a DDoS attack.

Ask for Help Early

Clearly, as the NCUA's warning highlighted, DDoS defense is all about preparation. Once an attack is under way, it's too late to defend against it.

Many financial organizations lack the in-house expertise to develop a DDoS incident response plan. According to a report by the Ponemon Institute, more than half of IT leaders at financial organizations say they lack the expertise or technology to prevent DDoS attacks.[4]

Outsourcing can fill the gaps. The Dell SecureWorks Preparedness Assessment process offers financial institutions of any size guidance based on deep experience and best practices.

Preparedness services consist of four main components:

1. Preparedness assessment
2. Instrumentation capabilities review
3. Tabletop exercise
4. Infrastructure stress testing

These steps will help you understand your organization's DDoS risk exposure so you can successfully mitigate future attacks. **To learn more, visit** www.secureworks.com/incident-response.

[4] "A Study of Retail Banks & DDoS Attacks," Ponemon Institute for Corero Network Security, December 2012