Banking on Availability

By: Nir Kshetri and Jeffrey Voas

Kshetri, Nir and Voas, J. (2017)." Banking on Availability", IEEE *Computer 50*(1), 76 – 80

Made available courtesy of IEEE: http://dx.doi.org/10.1109/MC.2017.22

***** © 2017 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.**

*****Note: This version of the document is not the copy of record.**

*****Note: Endnotes indicated with parentheses.**

Abstract:

Combating the growing threat to banks of distributed denial-of-service attacks will demand more than keeping pace in a technological arms race; it will also require greater information sharing among banks and other cybersecurity entities.

Keywords: DDoS | banks | cyberdefense | cyberextortion | financial cybersecurity

Article:

Images of the recent financial crisis in Greece included photos of closed banks and crowds of angry citizens and tourists who were incapable of withdrawing cash from ATM machines. When the banks finally opened, the lines of waiting customers were long, and the amount of cash withdrawals was limited to prevent runs on the banks. The lesson was clear: separating people from access to their money causes social panic and unrest.

The Greek situation was triggered by government bankruptcy, but similar crises can be caused by cyberattacks against the financial sector—including website disruption, payment-card fraud, and internal network infiltration. Many malware products to breach banking systems exist.(1) Banks are attractive hacking targets, not only for stealing money but also for acquiring highly sensitive private information about customers such as national identification and Social Security numbers as well as detailed histories of past payments. Successful cyberattacks can lead to the deletion of records, draining of account balances, and frozen (inaccessible) networks.

AN INDUSTRY UNDER ATTACK

Unsurprisingly, banks and other financial institutions experience a disproportionately high share of distributed denial-of-service (DDoS) attacks. Such attacks, which have targeted banks, online

casinos, e-commerce hubs, and other companies highly dependent on digital technologies for more than a decade,(2) have dramatically increased in recent years.(3) For example, between July 2014 and September 2015 a cybercriminal group called DD4BC (DDoS for Bitcoin) launched nearly 90 attacks against financial-services companies.(4) Many victims didn't pay pay ransom, but enough did to make the extortion profitable, spurring DD4BC copycats.(5,6)

Despite these threats, some banks have failed to appropriately enhance their cyberdefenses. A 2014 report by New York State's Department of Financial Services, which regulates banks and insurance companies, found that most institutions surveyed had suffered a successful cyberattack during the previous three years.(7) There are several reasons for this. Some banks, out of ignorance or willful neglect, continue to rely on older IT systems. In addition, increased mergers and acquisitions in the financial industry have forced the integration of distinct systems that birth new cybersecurity challenges. Finally, banks face a wide range of bad actors—from cybercriminals to publicity-seeking "hactivists" to terrorists to foreign entities conducting cyberwarfare and espionage.(8)

Realizing the seriousness of financial DDoS attacks on society, governments have begun to introduce regulations that spell out best practices, minimum standards, and crisis-response guidelines to ensure banking service availability and accessibility. For instance, US federal law requires banks and other financial institutions to monitor for DDoS attacks and have plans in place to mitigate against such attacks.(9) The Monetary Authority of Singapore's "4 × 4" rule requires banks, under penalty of fines, to correct an outage of online services in less than four hours and to have no more than four outages per year.(10) In June 2016, India's central bank issued a circular requiring banks to have a Cyber Crisis Management Plan in case of DDoS or other cyberattacks.(11)

FIGHTING BACK

Financial institutions are trying to adapt to the increasing frequency and diversity of cyberattacks. According to an April 2016 survey by the information services and analytics firm Neustar, 88 percent of financial-services respondents detected DDoS attacks in less than two hours and 72 percent responded to such attacks within the same amount of time.(12)

Like healthcare companies, banks have the responsibility of securing particularly sensitive personal information, and thus must enact robust countermeasures to ensure adequate confidentiality, integrity, and availability of their services and data. Of these three, we believe that availability deserves extra attention and is our focus here.

Lack of access to personal assets clearly creates customer dissatisfaction and affects a bank's brand and reputation. Further, service unavailability disproportionately affects a bank's bottom line compared to other businesses. An Incapsula-commissioned survey of IT managers from 270 North American organizations found the average cost of a DDoS attack to be $40,000/hour; 15 percent of respondents put the cost at under $5,000/hour and 15 percent estimated it to be over $100,000/hour.12 In contrast, the Neustar study found that DDoS attacks cost most banks about $100,000/hour, with more than a third of banks reporting even higher costs.(12)

In addition to the operating losses resulting from service unavailability, banks face stiff penalties from regulatory agencies. For example, after a botched software upgrade in June 2012 by the Royal Bank of Scotland prevented millions of customers in the UK from accessing their accounts, government regulators slapped the bank with £56 million in fines—on top of the £125 million in costs arising from the service disruption itself.(13)

Financial institutions commonly employ four strategies to address cyberattacks and maintain service functionality (see Table 1).

TABLE 1. Strategies to address cyberattacks.

Strategy	Example incident/context	Response	Source(s)
Use alternative communication and service channels.	Beginning 24 October 2014, the German online bank Fidor experienced a DDoS attack from cybercriminals demanding €4,000 in bitcoins to stop the attack. When the bank refused to pay, the extortionists significantly increased the network load, overwhelming the bank's firewall and disrupting services for about eight hours.	Fidor activated offline emergency processes that enabled customers to bank by phone. The bank used social media and other websites to communicate with customers—for example, it published the extortion emails on Facebook.	"Visionary Online Bank Thwarts Major DDoS Attack and Extortionists with Akamai Prolexic Routed," case study, Akamai, 2015; www.akamai.com/cn/zh/multimedia/documents/case-study/fidor-case-study.pdf.
Employ specialized DDoS monitoring and mitigation technology.	Banks implement this strategy as a preventive measure against future cyberattacks.	Akamai-Prolexic's 24/7 DDoS monitoring and mitigation service platform, Prolexic Routed, can defeat sustained 100-Gbps attacks. As of 2013, the highly rated service is used by 10 of the world's largest banks.	R. Shipley, "Prolexic DDoS Mitigation Services Review," *Top Ten Reviews*, 2 Oct. 2015; www.toptenreviews.com/business/internet/best-ddos-protection-services/prolexic-ddos-mitigation-services-review. "Prolexic Tracks More Than 47 Million DDoS Attack Bots Worldwide; Public Portal Now Available," *Dark Reading*, 7 May 2013; www.darkreading.com/attacks-breaches/prolexic-tracks-more-than-47-million-ddos-attack-bots-worldwide-public-portal-now-available/d/d-id/1139689?.
Work with related parties to minimize the impact on affected services.	HSBC, one of the world's largest banking and financial services companies, was hit by a DDoS attack on 29 January 2016, two days before the deadline for submitting self-assessment tax returns in the UK. Personal banking services were inaccessible on payday for many customers.	Taxpayers requiring information from HSBC were allowed to include estimates in returns to file by 31 January. HM Revenue and Customs—the UK's tax authority—gave affected consumers 12 months to amend the filing with correct information.	J. Goldman, "HSBC Internet Banking Disabled by DDoS Attack," *eSecurity Planet*, 1 Feb. 2016; www.esecurityplanet.com/network-security/hsbc-internet-banking-disabled-by-ddos-attack.html.
Pay ransom to halt cyberattacks.	In March–April 2016, a cyberextortion group calling itself the Armada Collective threatened to launch DDoS attacks against more than 100 online service providers, unless the targets paid the designated "protection fee" of 10.06 bitcoins, to increase daily by 10 bitcoins in the event of nonpayment.	More than $100,000 was sent to Armada-linked bitcoin addresses, but the threatened attack never materialized.	R. Brandom, "The DDoS Attack That Cried Wolf," *The Verge*, 26 Apr. 2016; www.theverge.com/2016/4/26/11512032/ddos-ransom-armada-collective-denial-of-service-threat.

Use alternative communication and service channels

To increase service resilience and mitigate network failures, banks can use alternative communication and service channels. For example, like many other banks, the Louisville, Kentucky–based Republic Bank lets customers access their accounts through both mobile apps and text banking if the website is ever down due to a DDoS attack or other source of disruption (www.republicbank.com/home/help/security/ddos). Banks also use social media such as Facebook and YouTube to increase customers' knowledge about and awareness of problems.(14) Some banks have a dedicated Twitter handle to help answer customers' queries and resolve complaints.(15)

Employ specialized DDoS monitoring and mitigation technology

In addition to implementing do-it-yourself IT techniques such as overprovisioning network bandwidth and rerouting malicious traffic to another location ("blackholing"), banks can purchase and install customized equipment that monitors network traffic for DDoS attacks and blocks them. Perhaps 5 percent of large banks have such products. Financial institutions that can't afford or lack the expertise to maintain in-house systems can outsource DDoS monitoring and mitigation to specialty providers such as Akamai-Prolexic, Verisign, and Corero Network Security.(16)

Work with related parties to minimize the impact on affected services

By attacking banks when customer services are most in demand—for example, around holidays—cyberextortionists can increase the probability of ransom being paid. To minimize attacks' impact at these times, banks can coordinate with related parties to reduce the criticalness and urgency of affected services, such as by using redundancy.

Pay ransom to halt cyberattacks

Reliable statistics aren't publically available, but it's well known that banks sometimes pay ransom to halt cyberattacks. According to the FBI's New York office, during April–July 2015, more than 100 companies in the financial-services sector experienced cyberattacks tied with ransom requests running in the tens of thousands of dollars.(17) One Gartner analyst has estimated that targeted institutions pay ransoms of $5 for every $100 worth of damage they could suffer if the extracted data were published.(18) Of course, customers ultimately pay this cost.

EMERGING COUNTERMEASURES

Under growing pressure from customers, shareholders, and government regulators, financial institutions are exploring new approaches to improve their cybersecurity. One strategy is to educate the public about the risks of cyberattacks and to promote awareness of ways to better protect personal data and the devices used to access it.(19) Another is to employ yet more communication and service channels as insulation against a breach or outage—given the rising frequency and severity of cyberattacks, it's a matter of when, not if, a given bank will be targeted.

On the regulatory front, lawmakers are increasingly concerned about cyberattacks against US financial institutions. In October 2014, leaders of the US Senate Committee on Banking, Housing, and Urban Affairs penned a letter to the nation's top financial regulators—the Secretary of the Treasury, Comptroller of the Currency, and chairs of the Federal Reserve, Federal Deposit Insurance Corporation, and National Credit Union Administration—requesting details on what specific steps were being taken to protect the financial system against cyberattacks.(20)

Cybersecurity is a top priority for New York's Department of Financial Services (DFS).(21) In September 2014, the DFS proposed a regulation that would require banks, insurance companies, and other financial institutions chartered in the state to establish and maintain a cybersecurity program, adopt a written cybersecurity policy, and designate a chief information security officer to implement, oversee, and enforce both.(22) The following month, in the in the wake of a high-profile cyberattack against JPMorgan Chase and other financial firms that compromised the data of 76 million households, DFS superintendent Benjamin Lawsky met with senior leaders of regulated entities to discuss their ability to withstand and prepare for cyberattacks by taking more proactive measures, such as tracking the vulnerabilities of third-party vendors, building cybersecurity expertise into their boards, and investing in cyberinsurance.(23) In December 2014, Lawsky announced that New York financial institutions would have to comply with stricter cybersecurity requirements during examinations.(24)

Greater information sharing is a central theme in emerging countermeasures. One problem for banks that outsource DDoS monitoring and mitigation is that such services "do not necessarily communicate with other companies that have not bought the same technology—or with other technology the same company has bought."(25) To address this problem, the not-for-profit Financial Services Information Sharing and Analysis Center (www.fsisac.com) has launched a new software platform, the Critical Infrastructure Notification System (CINS), that distills cyberthreat information into actionable intelligence to member companies worldwide nearly simultaneously. CINS is designed to make it more difficult for hackers to deploy the same malware against multiple banks.

When people are disconnected from their money, they quickly lose trust in the institution managing it. Successful DDoS attacks exacerbate this problem by disrupting service availability, making robust cyberdefense essential in this industry. Although most such attacks are financially motivated, the socioeconomic importance of banks also makes them an a top target for ideological or geopolitical hackers, in some cases armed with cutting-edge malware tools and abundant resources. Combating this threat will demand more than keeping pace in a technological arms race; it will also require greater information sharing among banks as well as between banks and government agencies, companies in other critical industries, and cybersecurity researchers. This in turn will require transforming the industry's long-standing culture of secrecy to one of greater transparency.

REFERENCES

1. N. Gamer, "Finance Industry: Money- Stealing Malware to Be Aware of," blog, Trend Micro, 16 Feb. 2016; blog.trendmicro.com/finance-industry-money-stealing-malware-to-be-aware-of.

2. N. Kshetri, “Hacking the Odds, ” *Foreign Policy*, 21 Oct. 2009; foreignpolicy.com/2009/10/21/hacking-the-odds.

3. P. Crosman, “Hackers to Bankers: Pay Up or We Attack Your Website,” *American Banker*, 23 Sept. 2015; www.americanbanker.com/news/bank-technology/hackers-to-bankers-pay-up-or-we-attack-your-website-1076912-1.html.

4. O. Solon, “Cyber-Extortionists Targeting the Financial Sector Are Demanding Bitcoin Ransoms,” *Bloomberg Technology*, 9 Sept. 2015; www.bloomberg.com/news/articles/2015-09-09/bitcoin-ddos-ransom-demands-raise-dd4bc-profile.

5. Arbor Security Eng. and Response Team, *DD4BC DDoS Extortion Threat Activity*, ASERT Threat Intelligence Report 2015-04, Arbor Networks, 2015; pages.arbornetworks.com/rs/082-KNA-087/images/ATIB2015-04DD4BC.pdf.

6. T. Martin-Vegue, “DD4BC Arrests Unlikely to Signal End to DDoS Extortion,” *CSO*, 19 Jan. 2016; www.csoonline.com/article/3023023/cyber-attacks-espionage/dd4bc-arrests-unlikely-to-signal-end-to-ddos-extortion.html.

7. A.M. Cuomo and B.M. Lawsky, *Report on Cyber Security in the Banking Sector*, New York State Dept. of Financial Services, May 2014; www.dfs.ny.gov/reportpub/dfs_cyber_banking_report_052014.pdf.

8. M. Arnold, “Banks Face Rising Threat from Cyber Crime,” *Financial Times*, 6 Oct. 2014; www.ft.com/content/5fd20f60-4d67-11e4-8f75-00144feab7de.

9. E. Messmer, “New Federal Rule Requires Banks to Fight DDoS Attacks,” *Network World*, 4 Apr. 2014; www.networkworld.com/article/2175847/network-security/new-federal-rule-requires-banks-to-fight-ddos-attacks.html.

10. “Reducing Threats to Availability in the Banking Sector,” BankingTech.com; www.bankingtech.com/151512/reducing-threats-to-availability-in-the-banking-sector.

11. R. Ravikumar, “Cyber Security Framework in Banks,” notification RBI/2015-16/418, Reserve Bank of India, 2 June 2016; www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0.

12. P. Crosman, “Banks Lose Up to $100K/Hour to Shorter, More Intense DDoS Attacks,” *American Banker*, 23 Apr. 2015; www.americanbanker.com/news/bank-technology/banks-lose-up-to-100khour-to-shorter-more-intense-ddos-attacks-1073966-1.html?zkPrintable=1&nopagination=1.

13. “RBS Fined £56M over Unacceptable Computer Failure,” BBC News, 20 Nov. 2014; www.bbc.com/news/business-30125728.

14. Cyberrisk in Banking: A Review of the Key Industry Threats and Responses Ahead, white paper, SAS Inst., Sept. 2013; www.sas.com/en_us/whitepapers/cyberrisk-in-banking-106605.html.

15. IBA Technology Awards: Reimagining Business Models, Ernst & Young, Feb. 2016; www.ey.com/Publication/vwLUAssets/EY_-_IBA_technology_awards-reimagining_business_models/$FILE/EY-IBA-technology-awards-reimagining-business-models.pdf.

16. P. Crosman, "How to Block a DDoS Attack," *American Banker*, 15 Apr. 2013; www.americanbanker.com/issues/178_72/how-banks-can-block-a-ddos-attack-1058300-1.html?zkPrintable=1&nopagination=1.

17. "FBI Says Banks Pay Hackers Ransom to Halt Attacks," BatBlue, 31 July 2015; www.batblue.com/fbi-says-banks-pay-hackers-ransom-to-halt-attacks.

18. T. Kitten, "DDoS Attacks against Banks Increasing," blog, BankInfoSecurity, 24 Aug. 2015; www.bankinfosecurity.com/ddos-a-8497.

19. "Local Banks Promote Cyber Security," WMUR News, 5 Oct. 2014; www.wmur.com/news/local-banks-promote-cyber-security/28957370.

20. "Johnson, Crapo Seek Information on Cybersecurity," press release, US Senate Committee on Banking, Housing, and Urban Affairs, 21 Oct. 2014; www.banking.senate.gov/public/index.cfm/democratic-press-releases?ID=0DD1C77A-A2C4-861B-300D-92D66F74A086.

21. K. Scannell, "NY Bank Regulator Targets Cyber Threat," *Financial Times*, 5 Oct. 2014; www.ft.com/content/5a981338-4cdf-11e4-a0d7-00144feab7de.

22. T. Quach, "New York Department of Financial Services Proposes Cybersecurity Regulation," blog, Proskauer, 7 Nov. 2016; privacylaw.proskauer.com/2016/11/articles/cybersecurity/new-york-department-of-financial-services-proposes-cybersecurity-regulation.

23. T. Kopan, "N.Y. Financial Chief Eyes Cybersecurity," *Politico*, 23 Oct. 2014; www.politico.com/morningcybersecurity/1014/morningcybersecurity15793.html.

24. G. Chon, "NY Bank Regulator Steps up Online Security Demands," *Financial Times*, 9 Dec. 2014; www.ft.com/content/fe9e020e-7fc9-11e4-acf3-00144feabdc0.

25. H. Kuchler, "US Financial Industry Launches Platform to Thwart Cyber Attacks," *Financial Times*, 24 Sept. 2014; www.ft.com/content/080092b2-437a-11e4-8a43-00144feabdc0.

NIR KSHETRI is a professor of management in the Bryan School of Business and Economics at the University of North Carolina at Greensboro. Contact him at nbkshetr@uncg.edu.

JEFFREY VOAS is *Computer*'s Cybertrust column editor and an IEEE Fellow. Contact him at j.voas@ieee.org.

DISCLAIMER

Any mention of commercial products or organizations is for informational purposes only; it is not intended to imply recommendation or endorsement by the authors, nor is it intended to imply that the products identified are necessarily the best available for the purpose.