ALSTON&BIRD LLP

CYBER ALERT

A Publication of the Security Incident Management & Response Team

WWW.ALSTON.COM FEBRUARY 12, 2013

Evolving DDOS Attacks Provide the Driver for Financial Institutions to Enhance Response Capabilities

By: Kimberly K. Peretti and Maki DePalo

Summary

Distributed Denial-of-Service (DDoS) attacks[1] are not a new method employed by cyber criminals to inflict damage on victim entities' networks. In fact, DDoS attacks were one of the first types of online crimes to appear in the dawn of the Internet age.[2] In the past several years, however, cyber threat actors have rekindled this attack to produce two new variants, both of which specifically target the financial services sector.

The first variant employs the DDoS attack merely as a diversion technique. In this method, which became noticeable in late 2011 and continues to present day, criminals conduct a DDoS attack on a victim website in order to divert attention and distract bank personnel from the underlying purpose of the attack—to steal online banking credentials and conduct unauthorized wire transfers. To execute this attack, criminals have used a commercially available crimeware kit—known as Dirtjumper—that can be bought and sold on criminal forums for only $200.[3]

While the purpose of the first type of DDoS is to increase the chance of successful financial fraud, the purpose of the second variant, which is the focus of this article, appears to be in line with the more traditional purpose of a DDoS—to disrupt services by rendering the website inaccessible to legitimate users. The new variant, however, is unprecedented in terms of its size, its industry focus, the attack vector it employs, its longevity and its potential source.[4] At the same time, the response to these attacks has been extraordinary in terms of industry collaboration and information-sharing to mitigate the impact of

---

1 *Guide to Intrusion Detection and Prevention Systems*, National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf (Distributed Denial of Service attacks typically involve significantly increased bandwidth usage or a much larger number of packets or connections to or from a particular host than usual).

2 Tony Smith, "Mafiaboy Pleads Guilty," *The Register* (Jan. 19, 2001), http://www.theregister.co.uk/2001/01/19/mafiaboy_pleads_guilty/ (The 16-year-old Canadian hacker known only as Mafiaboy launched attacks against Yahoo, Amazon, eBay and many other high-profile sites in 2000 using DDoS attacks).

3 *Fraud Alert – Cyber Criminals Targeting Financial Institution Employee Credentials to Conduct Wire Transfer Fraud* (Sep. 17, 2012), http://www.ic3.gov/media/2012/FraudAlertFinancialInstitutionEmployeeCredentialsTargeted.pdf.

4 Nicole Perlroth and Quentin Hardy, "Bank Hacking was the Work of Iranians, Officials Say," *New York Times* (Jan. 8, 2013), http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0.

the attacks.[5] Given the combination of first-time factors contributing to this variant's successes and because this new breed of cybercrime may be merely a sign of what awaits financial institutions in 2013, all financial institutions—small, mid-tiered and large alike—are advised to take this opportunity to review, reexamine and enhance their security incident response capabilities.

The New DDoS Variant

Beginning in mid-September 2012 and continuing over a six-week period, a dozen financial institutions were successfully targeted by a group initiating a series of sophisticated DDoS attacks against these banks' websites.[6] Most of the attacks were preannounced by the group claiming responsibility for the attacks—Izz ad-Din Al-Qassam Cyber Fighters (QCF).[7] QCF claimed its motive was to stop widespread and organized offenses to Islamic spiritual and holy issues and, in particular, remove an offensive video from the Internet.[8] Some sources, however, attribute the group's activities to the government of Iran responding to prior alleged U.S. cyber attacks on its systems and networks.[9]

Approximately one-and-a-half months later, the QCF allegedly initiated a second campaign of attacks. This wave, which started as early as December 11, 2012, targeted many of the same banks and a few additional institutions with similar DDoS attacks.[10] Indeed, the group claimed, based on a numerical sequence of "likes and dislikes" to Internet content it deems objectionable, that the attacks would continue for at least 14 months.[11] However, seven weeks later on January, 29, 2013, the group claimed victory when the objectionable content was apparently removed from one of the sources on the Internet.[12]

This DDoS variant is significantly and substantially different from previous types of DDoS attacks in several ways. First, the volume of network traffic used to commit the attacks was substantial. In the first campaign of attacks, it was reported that some banks were hit with a flood of traffic peaking at 65 gigabits-per-second (gbps).[13] Given that this volume is magnitudes above previous DDoS attacks, and that a mid-size business may only have the capacity to process 1 gbps of network traffic,

---

5 Tracy Kitten, "DDoS: Lessons from Phase 2 Attacks," *Bank Info Security* (Jan. 14, 2013) http://www.bankinfosecurity.com/ddos-attacks-lessons-from-phase-2-a-5420/op-1.

6 Tracy Kitten, "Bank Attacks: 7 Steps to Respond," *Bank Info Security* (Oct. 23, 2012) http://www.bankinfosecurity.com/bank-attacks-7-steps-to-respond-a-5221.

7 Nicole Perlroth, "U.S. Banks Again Hit by Wave of Cyberattacks," *The New York Times* (Jan. 4, 2013), http://bits.blogs.nytimes.com/2013/01/04/u-s-banks-again-hit-by-wave-of-cyberattacks/ (QCF referred to this wave of attacks as Operation Ababil, which appears to be a Koran reference to the swallows Allah sent to attack an army of elephants dispatched by the King of Yemen to attack Mecca in 571 A.D.).

8 *Id.*

9 *Id.* ("There is no doubt within the U.S. government that Iran is behind these attacks," quoting James A. Lewis, a former official in the State and Commerce Departments and a computer security expert at the Center for Strategic and International Studies in Washington).

10 Tracy Kitten, "DDoS: Lessons from Phase 2 Attacks," *Bank Info Security* (Jan. 14, 2013), http://www.bankinfosecurity.com/ddos-attacks-lessons-from-phase-2-a-5420/op-1.

11 Softpedia, "al-Qassam Hackers Create Equation to Determine Duration of Attacks on US Banks" (Jan. 8, 2013) (Risks of cyber-attacks against U.S. banks are escalating in 2013. The Izz ad-Din Al-Qassam Cyber Fighters group opened Year 2013 by posting a message on January 1, 2013, and warned: "Rulers and officials of American banks must expect our massive attacks! From now on, none of the U.S. banks will be safe from our attacks.").

12 Claes Bell, "Hackers halt attack on bank websites," Bankrate.com (Jan. 31, 2013) http://www.bankrate.com/financing/banking/hackers-halt-attack-on-bank-websites/.

13 Tom Field, "Bank Attacks: What Next, Bank Info Security," *Bank Info Security* (Oct. 12, 2012), http://www.bankinfosecurity.com/blogs/bank-attacks-what-next-p-1371/op-1.

this enormous influx of traffic is significant and problematic.[14] The high-volume network traffic of this size can overwhelm most of a victim's network infrastructure, and slow its response time to web inquires, if not grind it to a halt altogether.

Second, the attacks were aimed at institutions in the financial services sector. Both the first and second campaigns targeted large financial institutions, while more recent attacks have targeted a broader range of institutions, including smaller banks and credit unions. [15] Although there is no evidence that these attacks have compromised customer accounts, QFC claims its attacks cost U.S. banks $30,000 for every minute their websites were down.[16]

Third, the attacks used a network of compromised web servers—nicknamed "brobot"—in contrast to the more traditional DDoS, which uses a network of compromised individual "zombie" computers—known as a "botnet."[17] By using web servers, which have significantly larger bandwidth than individual computers, fewer compromised computers are needed and the capability for massive traffic exists to flood the victims' systems making it unresponsive to legitimate requests.[18]

Finally, industry experts have identified a layer of variability and persistence of tactics, particularly in that the toolkit allows attackers to react to defenses and modify attack strategy quickly.[19] New attack vectors have also increased the effectiveness of strikes, partly because they utilize bilateral strikes against both Internet service providers and victim banks at the application level.[20] Certainly, if the suspected source of the attack is true, the ability of the bad actors to draw upon unlimited resources in changing their tactics "on the fly" is not without reason.

Industry Response

Industry experts attribute an important contribution to minimizing the impact of the attacks to sharing critical threat data in near- to real-time both within the financial services sector and between government and the private sector.[21] The Financial Services Information Sharing and Analysis Center (FS-ISAC), the designated operational arm of the Financial Services Sector Coordinating Council, was particularly effective in this regard by providing a mechanism to collect threat intelligence and alert participating members with reports containing anonymized information.[22] The FS-ISAC issued a fraud alert the day fol-

---

14 Nicole Perlroth and Quentin Hardy, "Bank Hacking was the Work of Iranians, Officials Say," *New York Times* (Jan. 8, 2013), http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0.

15 Robert McGarvey, "Cyber Fighters' DDoS Hits Two Credit Unions," *Credit Union Times* (Feb. 6, 2013), http://www.cutimes.com/2013/02/06/cyber-fighters-ddos-hits-two-credit-unions?ref=hp.

16 Claes Bell, "Hackers halt attack on bank websites," Bankrate.com (Jan. 31, 2013), http://www.bankrate.com/financing/banking/hackers-halt-attack-on-bank-websites/.

17 Content Management Systems Security and Associated Risks, United States Computer Emergency Readiness Team (Jan. 24, 2013), http://www.us-cert.gov/cas/techalerts/TA13-024A.html (unlike earlier attacks that were launched from workstations, the recent attacks have utilized web servers, exploiting their vulnerabilities in popular content management systems).

18 "Distributed Denial of Service Attacks," *Cisco, The Internet Protocol Journal* Vol. 7, Num. 4, http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html.

19 Don Jackson, "DNS Amplification Variation Used in Recent DDoS Attacks," *Dell Secureworks* (Feb. 2, 2009), http://www.secureworks.com/cyber-threat-intelligence/threats/dns-amplification/.

20 Tracy Kitten, "DDoS: Lessons from Phase 2 Attacks," *Bank Info Security* (Jan. 14, 2013), http://www.bankinfosecurity.com/ddos-attacks-lessons-from-phase-2-a-5420/op-1.

21 Despite recent attacks that utilize new technology and attack vectors, extraordinary industry collaboration and information-sharing seem to have made a significant stride in defending the U.S. financial institutions from such attacks. The second campaign of attacks appears to have made less of an impact than the first wave. Tracy Kitten, "DDoS: Lessons from Phase 2 Attacks," *Bank Info Security* (Jan. 14, 2013), http://www.bankinfosecurity.com/ddos-attacks-lessons-from-phase-2-a-5420/op-1.

22 Tracy Kitten, "Regulator Warns of DDoS, Fraud Link," *Bank Info Security* (Dec. 21, 2012), http://www.bankinfosecurity.com/regulator-warns-ddos-fraud-link-a-5379/op-1; Tracy Kitten, "DDoS: Lessons from Phase 2 Attacks," *Bank Info Security* (Jan. 14, 2013), http://www.bankinfosecurity.com/ddos-attacks-lessons-from-phase-2-a-5420/op-1.

lowing the first attack and, a few days later, raised awareness in the U.S. banking industry by changing its cyber threat level from "elevated" to "high."[23] In addition, technology and DDoS mitigation service providers have also provided a significant role in releasing new tools and mechanisms to plug the holes exploited by attackers.[24]

Some institutions also reached out directly to the government for assistance in the response. Utilizing an established process known as "Request for Technical Assistance" (RTAs), banks reach out to their regulators who, in turn, reach out to the U.S. Treasury Department to draw upon the appropriate resources in the federal government, including the Department of Homeland Security (DHS) and the National Security Agency (NSA), to provide the requested assistance.[25] It appears that at least some banks have requested support from the NSA.[26] The DHS has also spoken publicly about its ability to help financial institutions to defend against DDoS attacks.[27]

Regulator Response

On December 21, 2012, the Office of the Comptroller of the Currency (OCC), an independent bureau of the U.S. Department of the Treasury, released an alert to CEOs of all national banks, federal branches and agencies, and associated interested parties, calling for a heightened sense of awareness and offering risk mitigation information in response to this series of sophisticated DDoS attacks.[28]

In the alert, the OCC reiterated its expectations that financial institutions have risk management programs in place to identify evolving threats to online accounts and adjust technology safeguards appropriately.[29] Further, banks are expected to ensure that an effective incident response approach with sufficient staffing is in place and proactive due diligence reviews are conducted to identify and mitigate risks imposed by potential DDoS attacks.[30] The regulators also encourage participation in information-sharing organizations such as the FS-ISAC.[31]

Conclusion

In the wake of this unprecedented variant of a traditional cybercrime attack, financial institutions of all sizes should take the opportunity to review, reexamine, improve and expand their incident response capabilities. Of course, every situation varies and there is no "one-size-fits-all" response to any incident. However, building upon lessons learned from responding to these particular attacks, institutions may want to consider:

---

[23] Tracy Kitten, "Bank Attacks: 7 Steps to Respond," *Bank Info Security* (Oct. 23, 2012), http://www.bankinfosecurity.com/bank-attacks-7-steps-to-respond-a-5221/p-2.

[24] Don Bailey and Dark Reading, "Prolexic Releases Threat Advisory To Detail Massive DDoS Threat From itsoknoproblmebro," *Security Dark Reading* (Jan. 3, 2013), http://www.darkreading.com/threat-intelligence/167901121/security/news/240145479/prolexic-releases-threat-advisory-to-detail-massive-ddos-threat-from-itsoknoproblembro.html.

[25] Ellen Nakashima, "Banks Seek NSA Help Amid Attacks on Their Computer Systems, *The Washington Post* (Jan. 11, 2013), http://articles.washingtonpost.com/2013-01-11/world/36272281_1_banks-ddos-nsa.

[26] *Id.* (the NSA's assistance usually entails a small team that advises a company on how to repair its system and strengthen and test its defenses to prevent repeat occurrences.)

[27] Eric Chabrow, "DHS Helping with DDoS Defense," *Bank Info Security* (Jan. 16, 2013), http://www.bankinfosecurity.com/dhs-aiding-banks-on-ddos-attacks-a-5424/op-1.

[28] Information Security: Distributed Denial of Service Attacks and Customer Account Fraud, Office of the Comptroller of the Currency, U.S. Department of the Treasury (Dec. 21, 2012), http://www.occ.gov/news-issuances/alerts/2012/alert-2012-16.html.

[29] *Id.*

[30] *Id.*

[31] *Id.*

- developing a structure and mechanism to intake early warning signals and integrate them into an immediate response;
- participating in information-sharing within the sector and with external parties (vendors, regulators and law enforcement);
- testing response plans to ensure that outside parties, such as DDoS mitigation service providers, are able to deliver services as planned and anticipated;
- building a threat/defense matrix into incident response plans for certain threats, such as DDoS attacks; and
- employing a layered defense with multiple tactical defense options.

In addition, financial institutions may want to consider expanding their arsenal of possible responses with creative solutions, such as:

- cross-industry collaboration (e.g., developing joint strategies with ISPs and information technology and telecommunication providers);
- employing active defense technologies;
- exploring informal and formal (i.e., legal) mechanisms to pursue intermediaries caught in the cross-fire; and
- exploring informal and formal mechanisms to dismantle the bad actor infrastructure.

Our attorneys have been counseling financial institutions on these and related issues for a number of years. Our Security Incident Management & Response (SIMR) Team has many attorneys who are thought leaders in the security preparedness and response space, including responses to complex, technical attacks from sophisticated and persistent bad actors. Please contact any of the attorneys below to learn more.

James A. Harvey | 404.881.7328 | jim.harvey@alston.com

Kimberly K. Peretti | 202.239.3720 | kimberly.peretti@alston.com