the Availability Digest

www.availabilitydigest.com

DDoS Attacks on U.S. Banks Continue

January 2013

We introduced our October, 2012, Never Again article entitled, “Islamic Hacktivists Attack U.S. Banks,” with the following summary:[1]

> *The posting of the fourteen-minute anti-Islamic trailer “Innocence of Muslims” on YouTube in early September, 2012, did more than spark outrage and massive anti-American demonstrations against U.S. embassies throughout the Arab world. It launched cyberattacks against the largest American banks in retaliation for the film. Massive Distributed Denial of Service (DDoS) attacks took down the web sites of Bank of America, JPMorgan Chase, Wells Fargo, U.S. Bank, and PNC for a day each over a two-week period.*
>
> *The hackers vowed to continue the attacks until the “nasty movie” was removed from the Internet.*

And indeed, they have!

The Second Wave of Attacks

Izz ad-Din al-Qassam Cyber Fighters make no secret of their plans. They announce their attacks in advance, and the attacks have been so massive and so sophisticated that banks struggle to mitigate the impact on their web-based online services.

In a posting to Pastebin.com on December 10, 2012, the attackers announced the second wave of their hactivist campaign on major U.S. banks:

> “In [this] new phase, the wideness and the number of attacks will increase explicitly; and offenders and subsequently their governmental supporters will not be able to imagine and forecast the widespread and greatness of these attacks.”

The hactivists threatened five major U.S. banks with DDoS attacks starting immediately - U.S. Bancorp, JPMorgan Chase, Bank of America, PNC Financial Services Group, and SunTrust Bank. Each of these banks had suffered major DDoS attacks during Phase 1 of the group’s campaign from mid-September to mid-October along with five other banks – Wells Fargo, Regions Bank, HSBC, BB&T, and Capital One. During that campaign, each institution was warned ahead of time; and none were able to completely fend off the attacks.

The group was true to its word. SunTrust was hit on December 11th. Bank of America and U.S. Bank were attacked on December 12th. PNC was the target on December 13th for the second time that week. JPMorgan Chase and U.S. Bank also suffered attacks on December 13th.

[1] Islamic Hacktivists Attack U.S. Banks, *Availability Digest*; October 2012. http://www.availabilitydigest.com/public_articles/0710/bank_attacks.pdf

© 2013 Sombers Associates, Inc., and W. H. Highleyman

The second wave of the attacks continue on an even broader scope than the original attacks. Up to seven banks a day are targeted, but interestingly only on Tuesdays, Wednesdays, and Thursdays. The attacks are now in their sixth week.

On December 12th, FS-ISAC (Financial Services – Information Sharing and Analysis Center),[2] a government-mandated organization set up to warn banks of impending cyber- and physical attacks, issued a member advisory outlining precautions to take.[3] In part, the advisory stated:

> "Targeted institutions have been working together with members of the security community and with government partners to help defend against the attacks. Information pertaining to tactics and techniques has been shared among these parties and with the broader FS-ISAC membership. FS-ISAC has provided best practices to its members to mitigate risk from these types of attacks.
>
> "Financial institutions should ensure they have reviewed their Distributed Denial of Service (DDoS) detection and mitigation plans as well as recent threat intelligence shared by and through the FS-ISAC.
>
> "FS-ISAC is working with its members, its partners, and government agencies to monitor this threat, share information, and support members under attack."

The Izz ad-Din al-Qassam Cyber Fighters have repeated their vow to continue attacks until the U.S. removes the offensive video from the Internet:

> "The implementing of these attacks is because of the widespread and organized offends to Islamic spirituals and holy issues. If this offended film is going to be eliminated from the Internet, the belonging attacks also will be stopped."

Is Iran Involved?

No one knows. According to a report by the New York Times, Iran is to blame for the DDoS attacks against U.S. Banks. The conjecture of some government and security theorists is that the attacks are in retaliation for the Stuxnet attack presumably launched against Iran by the United States and Israel to destroy Iran's centrifuges that are being used to refine uranium.[4]

However, there is no conclusive proof that Iran is involved. The Iranian government has officially denied any involvement in the attacks, and issued the following statement:

> "Unlike the United States, which has, per reports in the media, given itself the license to engage in illegal cyber-warfare against Iran, Iran respects the international law and refrains from targeting other nations' economic or financial institutions."

The Increasing Attack Sophistication

The bank DDoS attacks have been massive. The well-publicized Anonymous attacks on companies supporting Internet censorship via the Stop Online Piracy Act (SOPA) flooded web sites with one gigabyte/second of traffic. The recent bank attacks have measured 70 Gbps and more.

[2] FS-ISAC: Financial Services – Information Sharing and Analysis Center, *Availability Digest*; October 2012. http://www.availabilitydigest.com/public_articles/0710/fs-isac.pdf

[3] FS-ISAC Talking Points Concerning Today's DDoS Attacks, *FS-ISAC White Alert*; December 12, 2012. http://docs.ismgcorp.com/files/external/121212_FINAL_Talking_points.pdf

[4] Stuxnet – The World's First Cyberweapon, *Availability Digest*; March 2011. http://www.availabilitydigest.com/public_articles/0603/stuxnet.pdf

© 2013 Sombers Associates, Inc., and W. H. Highleyman

When the bank attacks first began, initial reports indicated that a massive botnet had been organized by the hacktivists by getting hundreds of thousands of enraged users to volunteer their PCs as part of the botnet. This provided the capacity to flood banking web sites with such a mass of traffic.

New information now has surfaced that the attacks are even more sophisticated. It is not only volunteer PCs that are being used. Compromised data-center web servers are being turned into DDoS weapons. These servers have a great deal more networking and compute capacity than PCs and can generate a great deal more malicious traffic. To generate 70 Gbps of DDoS traffic requires 70,000 PCs, each with a 1 Mbps connection. Ten times this number of PCs might be required if many of the PCs are in underdeveloped countries with limited bandwidth resources. Only 70 servers with 1 Gbps of bandwidth capacity each are needed to generate the same amount of traffic.

Even worse, web servers are a source of legitimate IP addresses and typically have a trusted relationship with their endpoints. Malicious traffic looks like legitimate internal traffic, allowing it to bypass security mechanisms and making it difficult to use anti-spoofing mechanisms to block junk traffic.

The attackers have found that they can easily infect some servers that have inadequate security controls. In one such case, the administrative user name and password were “admin,” “admin.” The administrator had not been concerned about security because “there was nothing on his web site worth stealing!”

The attackers hijacking web servers use a backdoor to leverage the server’s PHP environment to inject dynamic attack code that allows the attacker to quickly adapt to any changes in the web site’s security facilities. Using servers instead of PCs, the attacks are far more sophisticated. They attack a victim’s web server at several levels:

- Network level: The network is bombarded with traffic, consuming all the bandwidth needed by legitimate incoming requests. Such an attack can be as simple as sending massive numbers of pings to the web site or as sophisticated as an amplified DNS attack, in which UDP queries requiring large responses are sent to the web site’s DNS server. In these cases, the source IP address can be spoofed; so there is no indication of the source of the requests.

- Infrastructure level: Network devices such as firewalls, routers, and switches are usually stateful. They maintain state in internal tables. If their state tables fill, they can handle no further traffic. DDoS attacks at the infrastructure level attempt to fill the state tables of network devices so that they are bogged down and cannot handle any more legitimate traffic.

- Application level: The web server applications are targeted. A simple example of this a mass of login requests. The requests do not have to be successful – they just have to consume server resources as the login is processed and rejected. If an attacker has managed to obtain legitimate login names and passwords, it can do even more damage by invoking application functions such as searches that require a great deal of processing capacity.

One concern for the future is hacked clouds. If an attacker can create a malicious virtual machine in a cloud, the virtual machine can replicate itself across the cloud, creating a distributed bot that can generate massive malicious traffic. In the extreme, the malicious virtual machine can commandeer all of the remaining resources in the cloud, effectively taking the cloud down for legitimate users.

What to Do?

Banking web sites are more susceptible to DDoS attacks than non-banking e-commerce sites because their additional levels of security for authentication, transaction verification, and device identification require more bandwidth. According to security experts, banks need to address three key areas:

- Layered use of authentication at login, which consumes bandwidth.

© 2013 Sombers Associates, Inc., and W. H. Highleyman

- Reliance on Internet service providers not equipped to handle extreme bandwidth demands.
- Internal management of web servers to allow a bank to hand off traffic overflow when volumes are excessive.

These experts note that defenses include:

- using appropriate technology, including cloud-based services, to handle overflow when high volumes of web traffic strike.
- assessing their exposure to DDoS attacks by testing their systems with traffic volumes that mimic real-world attacks.
- implementing online outage mitigation and response strategies before an attack hits.
- training staff to recognize the signs of a DDoS attack so that mitigation strategies can be invoked as soon as possible.
- coordinating with ISPs and other service providers to implement traffic controls such as scrubbing, rate-limiting, and source-blocking.

A cautionary note: DDoS attacks are frequently used as tools of distraction to mask fraud attempts in the background. If a DDoS attack occurs, the awareness of malicious intrusion attempts should be heightened.

The bottom line is that disruptive DDoS attacks will persist. A bank's business-continuity plan must take this into account and define how online customer services will continue in the event that the bank's online banking services are seriously degraded or interrupted by such an attack.

An important aspect of the plan is communication with the bank's customers to let them know that a suspected attack is underway and what to do in the interim. Initially, some banks posted information about an attack on social media. Other banks denied that an attack was in progress or said only that their sites were experiencing intermittent outages. Banks are now realizing that although customers must know what is going on and what they should do, exposing this information to the general public only encourages the attackers by letting them know of their successes. Banks now have taken to targeted emailing to their customers for this purpose.

Summary

Based on current experience, there is no absolute defense against DDoS attacks. Attackers seem to be growing sophisticated more quickly than new, effective defenses can be deployed. Any online server, regardless of its sophistication, can be overwhelmed with enough traffic; and a dedicated attacker can generate whatever amount of malicious traffic is required to achieve its goals.

The good news is that mitigation efforts are indicating some results. Banks, ISPs, cloud-based prevention providers, and security vendors have all increased their efforts. The result is that the number of DDoS attacks against banks has become less frequent. Attacks are lasting for a shorter period of time and are causing less damage.

In addition, the U.S. National Security Agency is now cooperating with the financial services industry to help mitigate the impact of DDoS attacks. This effort underscores the government's concern about these unprecedented assaults.

© 2013 Sombers Associates, Inc., and W. H. Highleyman

Acknowledgements

The material for this article was taken from the following sources:

Recent Bank Cyber Attacks Originated From Hacked Data Centers, Not Large Botnet, *Security Week*; October 5, 2012.
Deep Inside a DNS Amplification DDoS Attack, *CloudFare blog*; October 30, 2012.
What to Do About DDoS Attacks, *Bank Info Security*; November 8, 2012.
5 Banks Targeted for New DDoS Attacks, *Bank Info Security*; December 11, 2012.
DDoS Attacks: PNC Struck Again, *Bank Info Security*; December 14, 2012.
Bank DDoS Attacks Employ Web Servers As Weapons, *Dark Reading*; January 9, 2013.
Iran Tied to DDoS Attacks Against U.S. Banks, Report, *Security Week*; January 9, 2013.
Iran Denies Cyber Attacks on US Banks, *ABC News*; January 11, 2013.
Banks seek NSA help amid attacks on their computer systems, *Washington Post*; January 11, 2013.
DDoS: Lessons from Phase 2 Attacks, *Bank Info Security*; January 14, 2013

© 2013 Sombers Associates, Inc., and W. H. Highleyman