the Availability Digest

www.availabilitydigest.com

Islamic Hacktivists Attack U.S. Banks

October 2012

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 of 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.

Izz ad-Din al-Qassam Cyber Warriors

The group that claims responsibility for the attacks calls itself the Izz ad-Din al-Qassam Cyber Warriors. It is believed to be an arm of Hamas, the political party that governs the Gaza Strip in Palestine.

The group takes its name from the Muslim preacher Izz ad-Din Abd al-Qadar ibn Mustapha ibn Yusuf ibn Muhammad al-Qassam, who was a leader in the fight against British, French, and Zionist organizations in the Levant (an area encompassing roughly the western regions of the Muslim world) in the 1920s and 1930s.

The group makes its plans well known in advance via posting on certain web sites – notably www.pastebin.com. On September 18, 2012, it posted its initial warning:

> "Dear Muslim youths, Muslims Nations and are noblemen
>
> "When Arab nations rose against their corrupt regimes (those who support Zionist regime) at the other hand when, Crucify infidels are terrified and they are no more supporting human rights. United States of America with the help of Zionist Regime made a Sacrilegious movie insulting all the religions not only Islam.
>
> "All the Muslims worldwide must unify and Stand against the action, Muslims must do whatever is necessary to stop spreading this movie. We will attack them for this insult with all we have.
>
> "All the Muslim youths who are active in the Cyber world will attack to American and Zionist Web bases as much as needed such that they say that they are sorry about that insult.
>
> "We, Cyber fighters of Izz ad-din Al qassam will attack the Bank of America and New York Stock Exchange for the first step. These Targets are properties of American-Zionist Capitalists. This attack will be started today at 2 pm. GMT. This attack will continue till the Erasing of that nasty movie.
>
> "Beware this attack can vary in type.
>
> "Down with modern infidels."

The next day, the group posted the following warning:

> "In the second step we attacked the largest bank of the united states, the "chase" bank. These series of attacks will continue untill the Erasing of that nasty movie from the Internet.
>
> "The site "www.chase.com" is down and also Online banking at "chaseonline.chase.com" is being decided to be Offline !
>
> "Down with modern infidels.
>
> "### Cyber fighters of Izz ad-din Al qassam ###"

The Banking Victims

Sure enough, on Tuesday, September 18th, the Bank of America was attacked, followed, as promised, by an attack the next day on JPMorgan Chase. The attacks were massive DDoS attacks that prevented customers from accessing the banks' web sites and online banking services for most of the day.

Following the BofA attack, the Financial Services Information Sharing and Analysis Center (FS-ISAC), which is owned by dozens of large financial firms, including BofA and JPMorgan Chase, raised its cyber threat level from "elevated" to "high."

The group next announced pending attacks on Wells Fargo, U.S. Bank, and PNC. It said that these would commence at 2:30 PM GMT (10:30 AM EDT, 7:30 AM PST) and last for eight hours.

Sure enough, Wells Fargo was attacked on Tuesday, September 25th. U.S. Bank was attacked on September 26th, and PNC on September 27th. In each case, the attack lasted most of the day. (We at the *Availability Digest* can confirm the PNC attack as that is our bank. We could not access the PNC web site for most of the day into early evening.)

These attacks were followed the next week by preannounced attacks on Capital One, SunTrust Banks, and Regions Financial.

Interestingly, the New York Stock Exchange did not seem to be attacked as threatened. Perhaps it was spared since it does not depend upon a public portal such as the online banking service web sites.

A Volunteer DDoS Attack

The Izz ad-Din al-Qassam Cyber Warriors evidently used a different and very effective strategy for their DDoS attacks. The standard DDoS attack uses a botnet set up by the hacker. After infecting hundreds or thousands of computers around the world, the hacker sends a command to the computers to start generating requests to the target site to overwhelm the site and make it virtually inaccessible to legitimate users.

This group used a volunteer-powered DDoS strategy. It enlisted the cooperation of perhaps hundreds of thousands of volunteers around the world who downloaded a program from a file-sharing site that would send continuous request messages on command to a target. At the assigned time, the volunteers launched their programs, and the target was overwhelmed with request messages. The attacks were launched under the name "Operation Ababil," meaning "swarm."

This strategy had two consequences. One is that the typical DDoS mitigation strategy of filtering out attack messages based on IP addresses was made very difficult because of the number of attack sources. The other is that the targets were bombarded by an estimated 100 gigabits/second of traffic rather than the five to ten gigabits/second that is more typical for a DDoS attack.

Only an attack triggered by a massive outpouring of anger could achieve this result.

DDoS Defense

Little can be done by law enforcement to curtail DDoS attacks. They are typically carried out in countries where there are no laws governing such attacks or where law enforcement is lax.

Firms need to implement mitigating controls and a formal incident response plan before an attack occurs. Some mitigating strategies include:

- purchasing more bandwidth for critical web sites and the networks that feed them.
- redirecting traffic to a cloud-based alternative to obtain additional bandwidth on demand.
- using alternate routing tools to redirect traffic to other locations to balance the load.
- using appliances that do packet analysis to separate good traffic from bad traffic, sending the later to an unused IP address.

A useful discussion of these and other techniques can be found on the DDoS Defense web site (http://www.ddosdefense.net/). See especially the article entitled, "How To Select A Distributed Denial of Service 'DDoS' Mitigation Service.

Still, the best defenses may not protect even the best-prepared firms from a concerted attack such as those described above. All firms should have a formal incident response plan that specifies how the firm will continue to provide services and products during such a successful attack. This plan should be included in the firm's Business Continuity Plan.

Summary

The demand of the Izz ad-Din al-Qassam Cyber Warriors to "erase the nasty movie" has not been met. Secretary of State Hillary Clinton has made the disgust of the U.S. government with the movie patently clear. However, Google, the owner of YouTube, has removed the movie only in countries that have laws against such blasphemy. Where freedom of speech is guaranteed, such as in the U.S., the movie is still available online. However, other countries have blocked YouTube until the video is removed.

On September 27, 2012, U.S. federal authorities arrested Nakoula Basseley Nakouia, who created the movie under the alias "Sam Bacile." He was charged with the violations of his parole including his role in the film making and his use of the alias. He is being held without bail. A Pakistani minister has offered a bounty for the death of Nakoula.

The video has sparked debates about the freedom of speech and Internet censorship. The First Amendment to the U.S. Constitution protects freedom of speech in the United States. The U.S. Supreme Court has interpreted this amendment in 1952 as invalidating government restrictions on blasphemy and, in the mid-1970s, on hate speech. In March, 2011, the Court reiterated its position by an 8:1 majority. Their position is that even hurtful speech should be protected to ensure that public debate is not stifled.

Acknowledgements

Material for this article was taken from the following sources:

Arab hackers attack Western websites over film, *CSOonline*; September 25, 2012.
Theories mount on bank attacks, but experts stress defense, *CSOonline*; September 25, 2012.
Banks can only hope for best with DDoS attacks, *CSOonline*; September 26, 2012.
Islamic hacktivists' bank attack claims gain credibility, *CSOonline*; September 26, 2012.
Wells Fargo recovers after site outage, *CSOonline*; September 26, 2012.
Hacktivists strike U.S. Bank with volunteer-powered DDoS, *CSOonline*; September 26, 2012.

Wells, U.S. Bank, PNC Among Institutions Linked to Attacks, *BankInfoSecurity*; September 26, 2012.
IZZ ad-Din al-Qassam hackers launch cyber attack on US Bank Wells Fargo, *Computer Weekly*; September 27, 2012.
PNC Financial: After the Website Outage, next steps, *Dotcom Monitor*; September 27, 2012.
Izz ad-Din al-Qassam, *Wikipedia*.