radware
Smart Network. Smart Business.

ERT Attack Report

Attacks on Large US Bank During Operation Ababil

March 2013

Table of Contents

Executive Summary

Along with several major banks in the U.S., one large US Bank has been under attack since October 2012 as part of the infamous "Operation Ababil". The bank has been unable to mitigate the attacks for more than 5 months and has suffered from continual service interruptions on the banks online services.

On March 12th another massive attack period started, but this time Radware DefensePro was already deployed onsite and Radware's Emergency Response Team (ERT) was invoked. During the next few weeks the ERT worked closely with the bank to modify its system infrastructure and deploy Radware's AMS until it achieved a successful mitigation for all attacks.

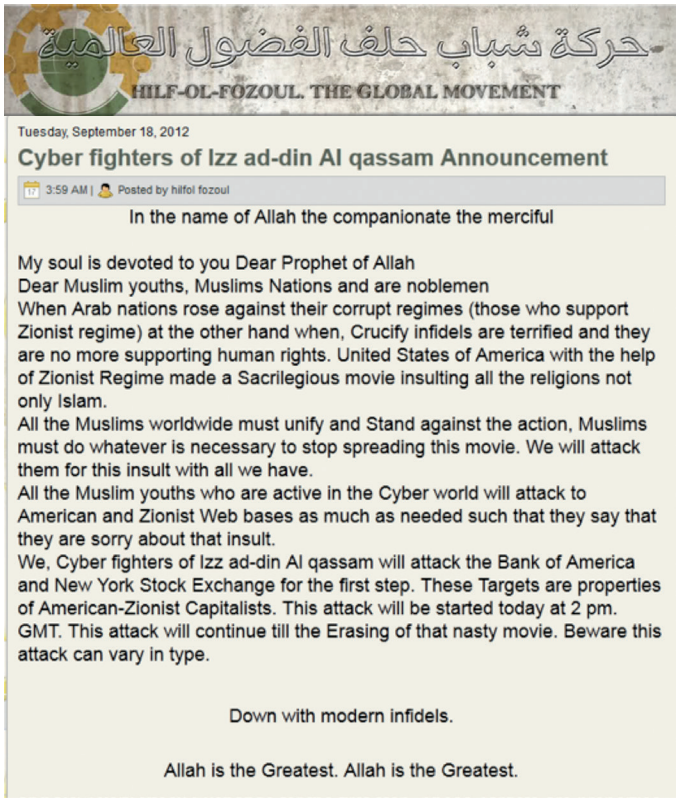
The main attacks seen at the bank were volumetric UDP/ICMP floods coupled with HTTP/S application floods. The volumetric floods reached a peak of 16Gbps and were mitigated upstream by the ISP. However, the ISP was not able to mitigate the application level attacks and these were the attacks which took down the bank each time. Some of the Bots that participated in the attack were more advanced than we have previously seen and were able to follow 302 redirects and cookies. At some point, one Bot was even able to successfully pass the Java script challenge for the first time ever. This required the ERT and Radware R&D to come up with a very quick resolution for the advanced Bot.

Background: Operation Ababil

On early September 2012, videos, about 14 minutes in length, that claimed to be "trailers" of a longer named **"Innocence of Muslims"** film were uploaded to YouTube. The film that claimed to contain offending content to the Muslim community has invoked demonstrations and violent protests in many Muslim countries which included among others an attack on U.S consulates and embassies.

On September 18th, 2012 a group called "Cyber fighters of Izz ad-din Al qassam" announced an upcoming cyber attack campaign and called for an attack on what they claim 'American and Zionist' targeted. The attack campaign was named "Operation Ababil" which was also the name of a failed Pakistani military operation that occurred in April, 1984.

The prolong ongoing attack campaign has set a goal to take down US based financial institutions web sites and online services.


حركة شباب حلف الفضول العالمية

HILF-OL-FOZOUL. THE GLOBAL MOVEMENT

Tuesday, September 18, 2012

Cyber fighters of Izz ad-din Al qassam Announcement

3:59 AM | Posted by hilfol fozoul

In the name of Allah the companionate the merciful

My soul is devoted to you Dear Prophet of Allah
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.

Allah is the Greatest. Allah is the Greatest.

Figure 1- Original Attack Campaign Announcement

Servers Enlisted to Launch the Attack

In recent months, Radware's ERT has witnessed what may be a new dramatic change in the DDoS landscape - the appearance of server-based botnets. Unlike the early days of single-server attacks, the new DDoS attacks employ multiple server machines, spread out geographically and organized in a powerful botnet. This new type of server-based DDoS architecture can be much more threatening than the common botnet attacks for several reasons:

- **Firepower** – servers have a much larger upload bandwidth, which enables fewer machines to produce the same impact as many client Botnets. Consider that the average US home computer has 600 Kbps upload speed, whereas a typical hosted server has an upload speed of 1Mbps-100Mbps – up to X150 times the bandwidth speed.
- **Reliability** – servers provide a far more reliable environment compared to home PCs. Home PCs are frequently shut down or taken offline, so that attackers must enlist a much larger number of computers than those that will actually be used in the attack. Servers, on the other hand, are always online and available for an attack.
- **Command and Control** – controlling a small number of highly available servers eliminates many of the challenges related to orchestrating thousands of unreliable botnet computers.

The attack on the bank continued the trend of attacks by servers and the attackers used the infamous Bot named 'itsoknoproblembro' aka `BroBot`. 'itsoknoproblembro' is a general purpose PHP script injected into the victim machine allowing the attacker to upload and execute arbitrary Perl scripts.

The 'itsoknoproblembro' script injects an encrypted payload, in order to bypass IPS and Malware gateways, into the index.php, allowing the attacker to upload new Perl scripts at any time. Initial server infection is usually done by using the well known RFI/LFI techniques.

By uploading Perl scripts that run different DoS flood vectors, the server might act as a Bot in a DDoS Botnet army. Although originally designed for general purpose, some variants of this tool were found in the wild, customized to act as a proprietary DDoS tool, implementing the flood vector logics inside.

This attack tool is hard to detect as the Bot dynamically updates its attacking nodes and characteristics. Each compromised server can produce high bandwidth and high rate of traffic utilizing multiple attack vectors in parallel.

Attack Vectors

The main attacks seen at the bank were volumetric UDP/ICMP floods coupled with HTTP/S flood. The volumetric floods were mitigated upstream by the ISP's and reached levels greater than 16Gbps. The ISP's however could not mitigate application level floods and these were the attacks which took down the bank each time.

ERT observed the following types of attacks at the bank:

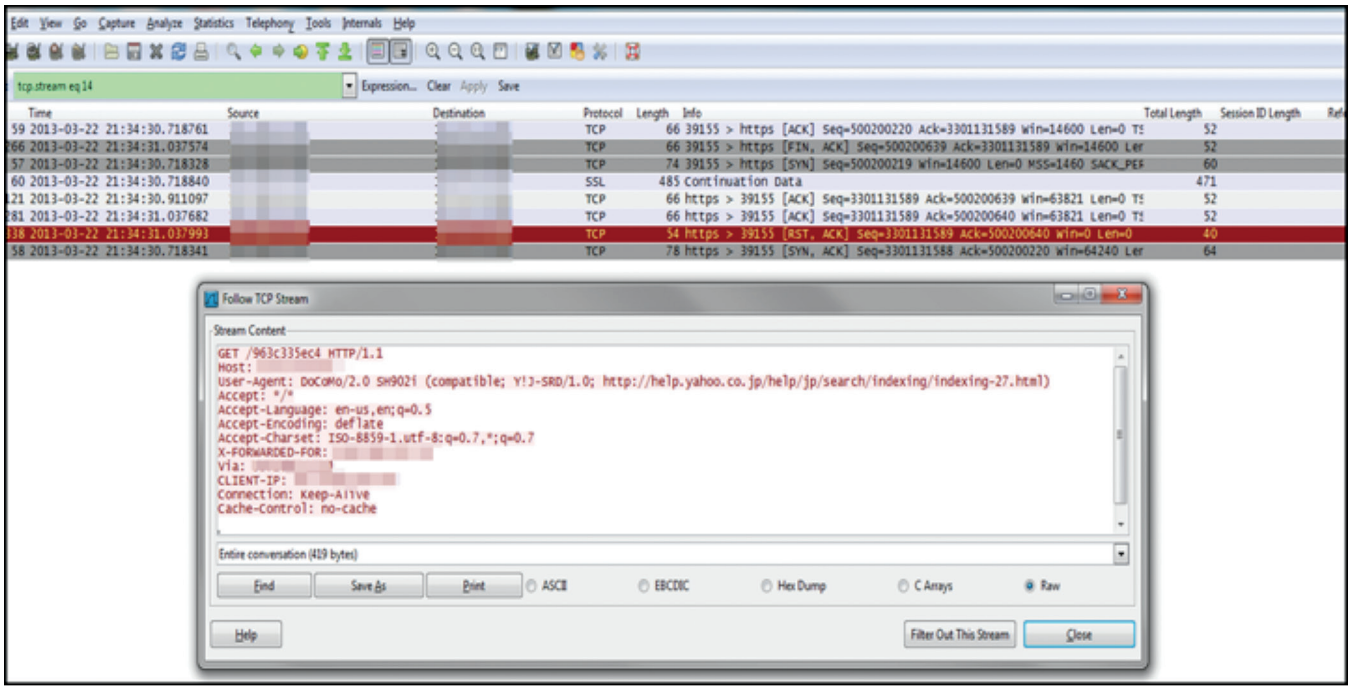
1. HTTP/S floods
2. TLS/SSL negotiation attacks
3. Server cracking attempts
4. Volumetric floods

Variations of HTTP/s Floods

Multiple vectors of HTTP and HTTP's floods were observed. They were designed with saturating connection tables, HTTP's daemons, bypassing CDN's, bypassing a fixed signature by changing payloads, impact backend CPU and SSL/HTTP daemon resources, exhaust backend DB systems. Below are some of the attack types we have seen.

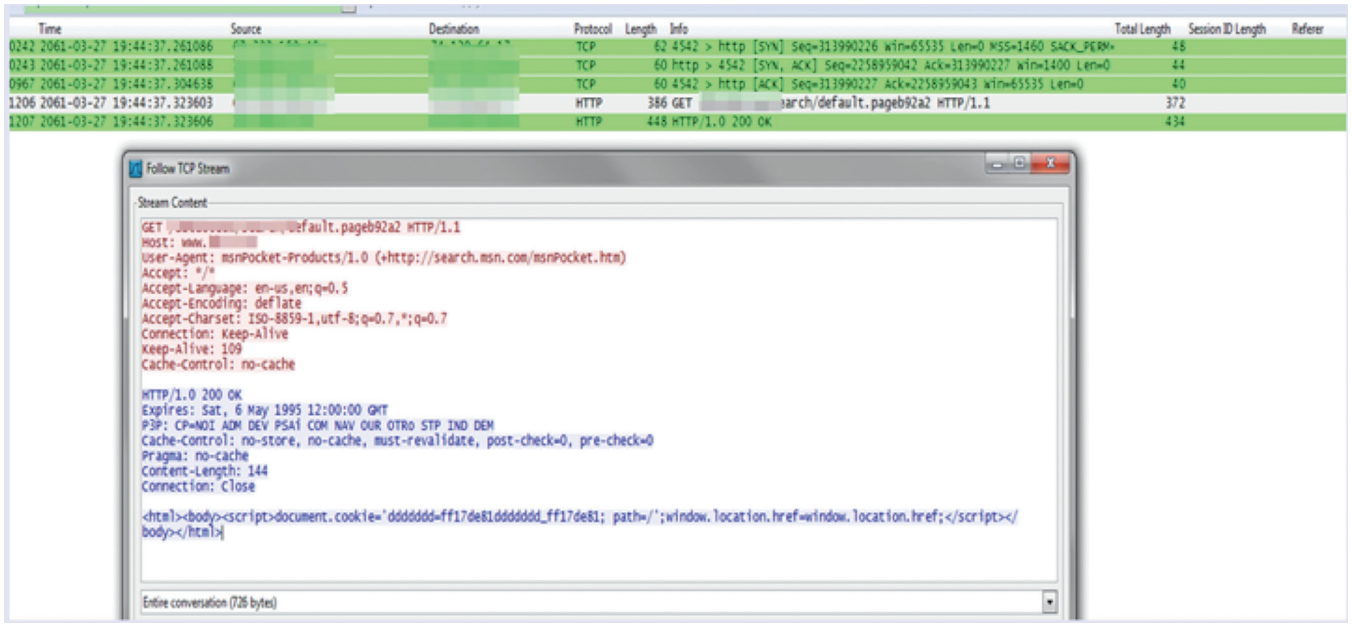
Clear Text HTTP's Flood

This flood was designed to saturate connection tables to port 443 and exploit any exception handling on the backend system. Essentially this flood sends clear text HTTP commands and headers to port 443. It is identifiable in the fact that it is sending HTTP clear text to HTTPs port, which is not supported in this particular environment or in most environments. Also the URL is dynamic so it would bypass CDN caching.



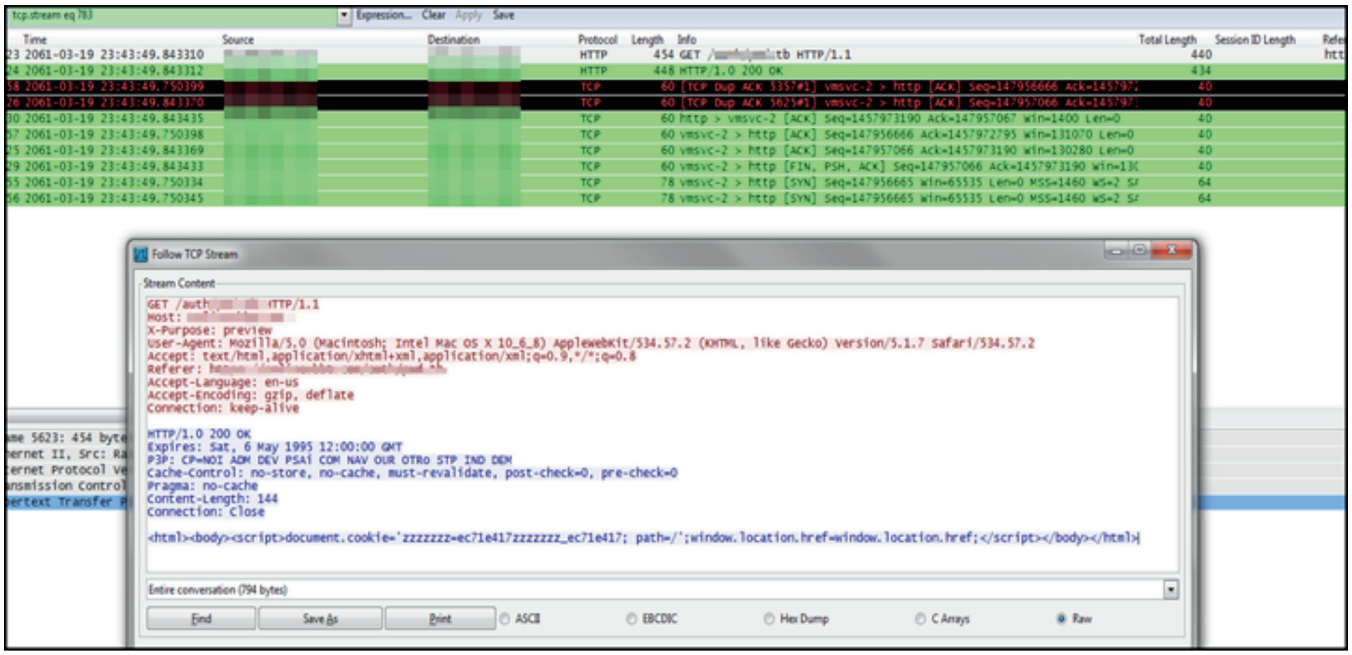
Search Page Request HTTP Attack

This HTTP flood was directed to port 80 and is accessible to public web clients, i.e. you do not need to be authenticated to run this search query. The attack was designed to bypass CDN, exhaust web daemon's connection tables as well as the backend system by querying the DB for each search query run. The search query is dynamic and therefore cannot be cached either by the default web cache or CDN services.



Authentication Engine Flood

Authentication retries were a common attack vector seen. This authentication attempt is an HTTP request to the authentication engine. The idea here was to exhaust resources to the web server in terms of the authentication engine itself and the connection table. The engine itself wasn't really affected but the connection limit capacity of the HTTP daemon is. This URL is also not cached by any CDN service so the request goes through directly to the servers.



Additional Notes on the HTTP/S Floods

The floods targeting the bank were not a high rate in terms of bandwidth but caused significant damage to the backed and impacted service availability. The floods were mixed and there was never just a single HTTP/s flood happening at one time. All header values were dynamic and were constantly changed during the course of the attack.

Summary

During the entire Operation Ababil attack campaign, the attackers demonstrated a high level of sophistication and skills that took down the online services of some of the world's largest banks. The attack on this bank also revealed the dynamic of the attackers and their ability to change their attack tools and patterns during the attack campaign. The attackers even managed to modify their Brobot to successfully respond to a java script challenge, and to appear as a legitimate user at some point during the campaign. The fact that the bank uses CDN services made the detection and attack mitigation even more complex as the CDN masks a lot of the required information, which results in longer response time and adds more complexity.

As demonstrated in this attack case, organizations should deploy a DDoS mitigation solution on premise and combine with 24x7 support of security experts to successfully fight today's cyber security threats.

SVC-ERT-US-Bank-Attack-Report-DS-01-2013/05