Executive Summary

In early September of 2012, short videos claiming to be “trailers” of a longer film entitled “Innocence of Muslims” was uploaded to YouTube.

The film, which claimed to contain offending content to the Muslim community, has invoked demonstrations and violent protests in many Muslim countries which included 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 claimed to be ‘American and Zionist’ targets.

The attack campaign was named “Operation Ababil” which was also the name of a failed Pakistani military operation that occurred in April, 1984.

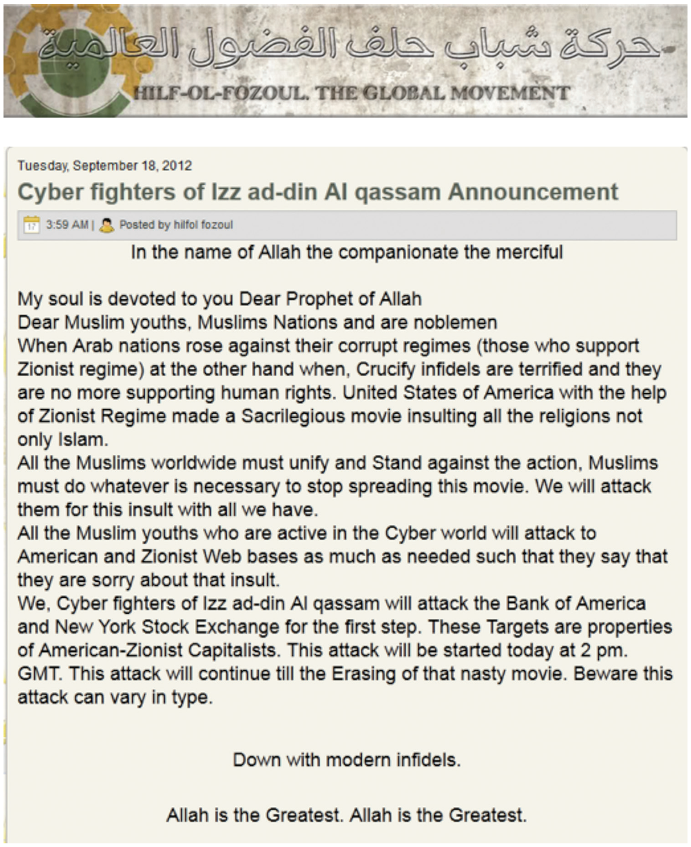
As mentioned in the public announcements by the `Cyber fighters of Izz ad-din Al qassam’, the attack was split into two major stages. The first stage of the attacks targeted Bank of America and the New York Stock Exchange, while the second stage of the attack targeted J.P. Morgan Chase Bank.

The entire attack campaign began on September 18th, 2012 and lasted for four days in which all the proclaimed targets were attacked.

On December 29th, 2012, another attack was launched against BOA and Citi Group. This attack was launched from compromised computers that were hosted on big hosting service servers.

The attack caused high outbound for web hosting companies. Recently, we received additional information from one of our clients naming two IPs belonging to a web hosting company sending malicious traffic. They also suggested that the attack was done by the malware ‘brobot’ which provided URLs that turned out to be HTTPS.

On January 9th, 2013, U.S. officials blamed Iran as the one standing behind this attack.


حركة شباب حلف الفضول العالمية
HILF-OL-FOZOUL. THE GLOBAL MOVEMENT
3:59 AM | Posted by hilfol fozoul

Tuesday, September 18, 2012

Cyber fighters of Izz ad-din Al qassam Announcement

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

Attacks and Outcomes

Bank of America
According to the media coverage, the Bank of America's public web site did not respond for a short period of time during September 18th and was later reported to have experienced "occasional slowness" issues.

J.P. Morgan Chase Bank
According to media coverage, an attack was initiated on J.P Morgan Chase Bank on September 20th which lasted a few hours.

The reports have indicated the Chase bank main web site (www.chase.com) was unavailable for at least some customers for a short period of time. JPMorgan Chase spokesman Patrick Linehan stated that, "We're experiencing intermittent issues with Chase.com. We apologize for any inconvenience and are working to restore full connectivity."

Attack Details

These recent attacks were investigated and analyzed by Radware`s ERT.

The following section provides a deep insight into the technical aspects of the attack tools and various techniques used in the recent campaigns as well as the mitigation strategies used.

Attack Techniques

Attack Vector I – UDP Garbage Flood

The main attack technique observed in the recent attacks was UDP Garbage Floods that target the organizations internal DNS servers.

The main motivation behind this attack vector is to generate huge traffic volumes in order to saturate the Internet pipes and consume all available bandwidth for the network, thus denying services for any legitimate traffic to the network.

Furthermore, this attack technique could possibly tie up web servers processing resources for replying with ICMP Destination unreachable packets and could also cause other statefull devices to crash.
The attack rates observed by the ERT team during the attacks were as high as 1Gbps, although the actual attack rates were possibly even higher. Our visibility was limited by the organizations physical inbound throughput.

All UDP packets sent during the attacks were identical in content and size which suggest that they were originated by the same attack tool.

Below are the specific characteristics of the UDP packets contained in the attack:

Characteristic	Description
Target Protocol\Port\Service	The main target port of the attack was UDP port 53 – targeting the internal (internet facing) DNS servers. We have also received data of a UDP port 80 attack.
Packet Size	1358 Bytes
Layer 4 Data	L4 Data section in all UDP packets was composed strictly of 'A' (0x41) characters throughout the entire payload.

The sources of the attack that were observed by Radware's ERT team seemed to originate from several specific IP address, although the IP addresses might have been spoofed.

Below is a list of source IP addresses we have identified from one of the traffic captures:

IP Address	Details
210.51.4.137	What seems to be a legitimate Beijing, China based web server.
67.19.27.250	Seems to be a non-operational web server, hosted by ThePlanet.com – A Houston, Texas based hosting company.

Contrary to several media coverage reports that claimed the attack was a "reflected DNS" type attack, we did not see any evidence to support this claim since the packets were malformed DNS requests (not fragmented).

This malformed DNS traffic may not have originated from any legitimate DNS server which is a mandatory component for launching an attack of this type.

Mitigation Strategy

UDP flood such as the one described above may be effectively detected and blocked by the signature protection module of DefensePro.

Even though the DefensePro mitigation was successful, networks with lower incoming bandwidth than the overall attack rate have suffered from bandwidth saturation issues due to the high attack rates and therefore were still denied any legitimate traffic to the attacked services.

In order to successfully mitigate this attack technique in the "Insufficient Bandwidth" networks, it is recommended to implement additional DoS defense mechanisms at the ISP level which will be able to sustain these high network traffic volumes.

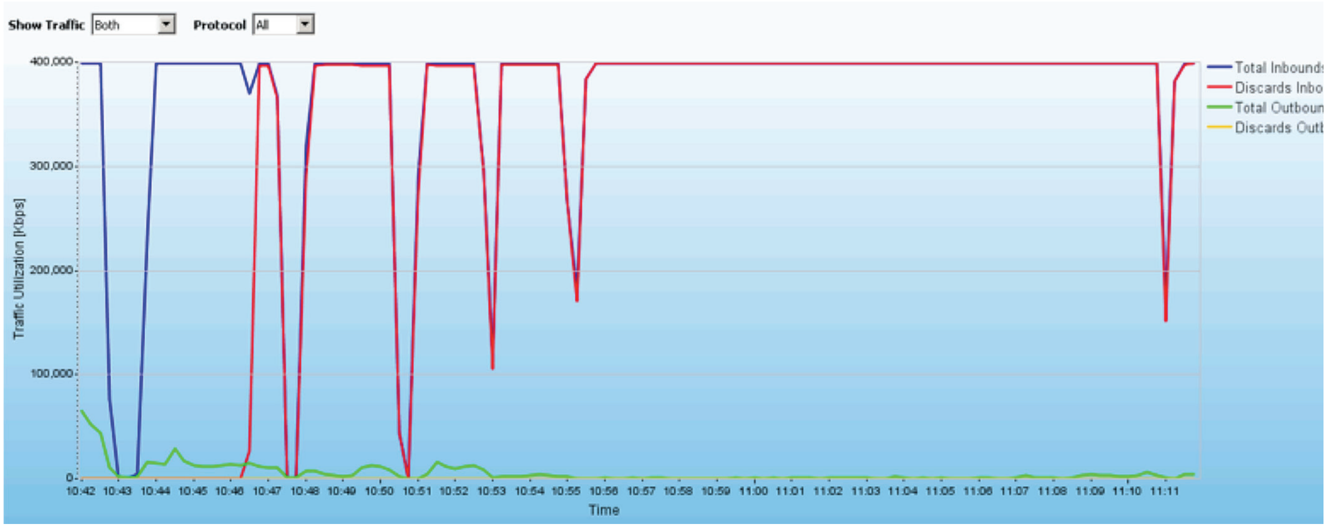


Figure 3 - UDP Garbage Flood Mitigation Graph

Attack Vector II – TCP SYN Flood

The TCP SYN flood attack technique was identified during the attack on several targets.

No additional packet captures or forensics data were provided regarding this attack technique.

This attack technique is a commonly known and widely used technique. The main motivation for this attack technique is exhausting resources of Firewall\IPS\other network equipment and exhausting web server resources thus causing a denial of service condition on the attacked network\server.

Since these attacks are very common, it is our belief that it would not played a major role in the overall attack and was most likely used to divert attention from the main attack techniques or to be used by lower resource attackers who wished to join the attack campaign.

Mitigation Strategy

DefensePro is able to mitigate a SYN flood attack by using the SYN protection and/or the BDOS module. The client policy configuration included the following:

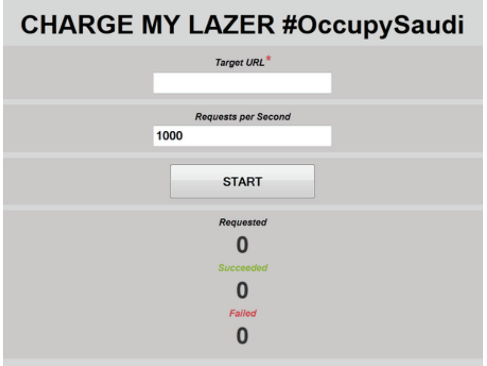
SYN Protection – this protection module enabled the DefensePro to detect large rate variations in TCP traffic and TCP flag distributions which is a common network behavior caused by such attacks. Upon successful attack detection, the SYN Protection module is able to initiate web challenges, TCP challenges and act as a transparent proxy is order to mitigate the attack.

BDOS – although not activated as the first line of defense, it served as a second line of defense and was configured to detect TCP protocol anomalies, with effective signatures.

Based on the vast experience with mitigating attacks of this nature, we assume that DefensePro successfully mitigated this attack, although we have not received any relevant packet capture or forensic data regarding this attack.

Attack Vector III – Mobile LOIC (Apache Killer Version)

Another reported attack technique that was allegedly used during this campaign is a custom version of the Mobile LOIC tool (aka Mobile LOIC - Apache Killer) which is designed to exploit a known vulnerability in Apache servers – corresponding to CVE-2011-3192.


CHARGE MY LAZER #OccupySaudi

Target URL*

Requests per Second: 1000

Requested: 0
Succeeded: 0
Failed: 0

Figure 4 - LOIC Apache Killer

This attack tool targets Apache servers using Apache HTTP server versions 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19.

Although this attack technique has proved to be quite effective against vulnerable servers, it is quite ineffective against up to date versions of the apache HTTP servers and most Intrusion Prevention systems that contain a relevant signature and are able to easily block this tool`s traffic.

Since customer servers seem to be running an up to date version of the apache HTTP server, and based on the data we have analyzed from the previous attack campaign, it is our belief that this attack technique did not cause any actual damage to their networks.

Mitigation Strategy

DefensePro is able to successfully detect and stop this attack technique by using the signature protection module which contains a specific signature that matches this tool network behavior and blocks all traffic associated with it.

Attack Vector IV – HTTP Request Flood

During the second attack wave on one of the customers, the main attack technique observed was an HTTP Request Flood targeting the main web site.

The main motivation for this attack technique is exhausting resources of the web server by generating a huge number of HTTP requests - preferably for “heavy” pages - thus causing a denial of service condition on the attacked web server.

The attack rates observed by the ERT team during the attack were as high as 80K – 100K TPS (transactions per second).

Below, are the specific characteristics of the HTTP packets contained in the attack:

Characteristic	Description
Target Protocol\Port\Service	Port 80\TCP – HTTP service
URL	Consistent pattern
User Agent	Seems to be dynamically chosen from predefined set of user agents. (see below)
HTTP Flags	All other HTTP header data seems to be randomized

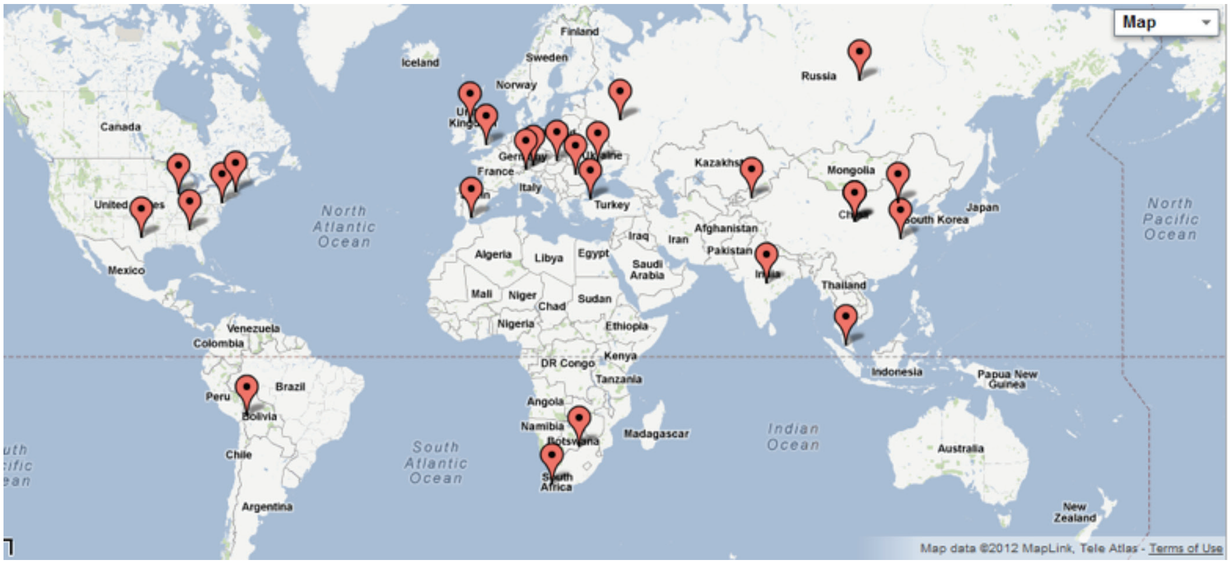


Figure 5- HTTP Flood Sources Geographical Locations

The HTTP requests used in this attack followed a specific pattern. The pattern included a simple GET request to several (legitimate) locations within the site and a randomized input parameter.

The randomized input parameter and HTTP header data was probably used in order to bypass standard detection and caching mechanisms.

HTTP Request Samples
GET /customer-base-uri/etvs?2408b
GET / customer-base-uri /bonds?4d094
GET / customer-base-uri?aad95
GET /

The HTTP user agent value used during this attack seemed to be repeatedly changing by all of the attacking clients. This is consistent with standard User Agents randomization mechanisms where a predefined list of legitimate user agents is used either manually or integrated into the attack tool.

In addition, most of the User Agent values used were of known crawlers and most likely used in order to bypass standard bandwidth based protections.

Below is a list of User Agents used in this attack:

HTTP Request Samples
DoCoMo/2.0 SH902i (compatible; Y!J-SRD/1.0; http://help.yahoo.co.jp/help/jp/search/indexing/indexing-27.html)
Googlebot/2.1 (http://www.googlebot.com/bot.html)
IE/5.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 1.1.4322;)
Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.4b) Gecko/20030505 Mozilla Firebird/0.6
Opera/9.00 (Windows NT 5.1; U; en)
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;)
msnbot-Products/1.0 (+http://search.msn.com/msnbot.htm)

Mitigation Strategy

DefensePro is able to mitigate HTTP floods by using an HTTP challenge (either on the SYN protection modules or on the HTTP mitigator module).

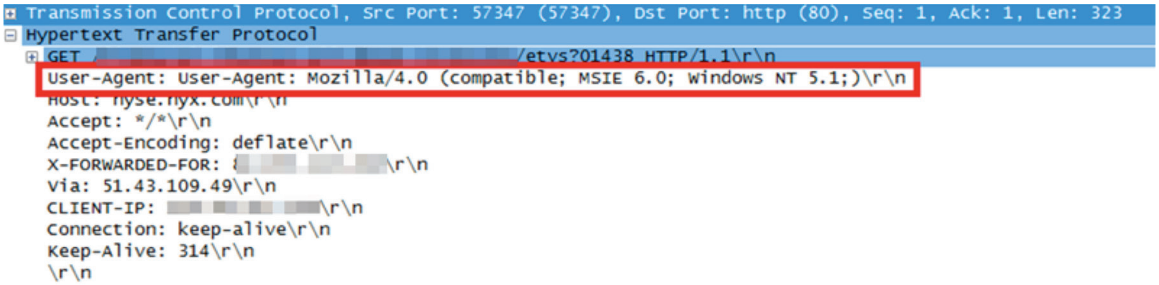
This defense technique is intended to present a challenge to the traffic initiator in such a way that only legitimate sources could be able to successfully respond, thus dropping the attacking sources before they can reach the actual web server.

By analyzing the HTTP request URL's distribution, we have noticed that a high rate of the incoming traffic was targeting URL`s at a specific location.

Therefore, as a second line of defense, a new signature protection was constructed that was designed to block every source initiating a high rate of requests to the following URL.

The signature was implemented and successfully identified and blocked the attacking sources.

After a second look at the User Agent list, one value has caught our attention:
"User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;)"



```
⊞ Transmission Control Protocol, Src Port: 57347 (57347), Dst Port: http (80), Seq: 1, Ack: 1, Len: 323
⊟ Hypertext Transfer Protocol
  ⊞ GET /[redacted]/etys?01438 HTTP/1.1\r\n
    User-Agent: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;)\r\n
    Host: nyse.nyx.com\r\n
    Accept: */*\r\n
    Accept-Encoding: deflate\r\n
    X-FORWARDED-FOR: [redacted]\r\n
    Via: 51.43.109.49\r\n
    CLIENT-IP: [redacted]\r\n
    Connection: keep-alive\r\n
    Keep-Alive: 314\r\n
    \r\n
```

Figure 6- "Mistyped" User-Agent Field

This value is unique since it seems to contain a typo which is caused by placing the "User Agent:" string inside the user agent value itself.

By crossing this data with the highest traffic generators, we have confirmed that each attack source has used this "mistyped" user agent at least once during the attack.

This valuable data has allowed us to create an even more specific signature that will block and suspend every attacking source.

Appendix I – Media Coverage

http://www.foxbusiness.com/industries/2012/09/19/chase-website-experiences-intermittent-troubles/

http://in.reuters.com/article/2012/09/20/jpmorganchase-website-idINL1E8KJAZS20120920

http://money.cnn.com/2012/09/19/technology/chase-site-slow

http://www.bdlive.co.za/businesstimes/2012/09/23/cyber-threat-high-for-banks

http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0

http://video.foxbusiness.com/v/2083330491001/iran-behind-bank-attacks/?intcmp=obinsite

http://www.cnn.com/video/#/video/bestoftv/2013/01/09/exp-tsr-todd-us-banks-hacked-iran.cnn

http://news.yahoo.com/bank-hacks-were-iranians-officials-025838225.html

http://www.itworld.com/networking/335030/botnets-hire-likely-used-attacks-against-us-banks-security-firm-says?page=0,2

http://www.cio.com/article/726090/Botnets_for_Hire_Likely_Used_in_Attacks_Against_US_Banks_Security_Firm_Says

http://www.pcworld.idg.com.au/article/446049/botnets_hire_likely_used_attacks_against_us_banks_security_firm_says/

http://www.cso.com.au/article/446049/botnets_hire_likely_used_attacks_against_us_banks_security_firm_says/

http://www.theregister.co.uk/2013/01/09/us_banks_ddos_blamed_on_iran/

http://www.dailytech.com/US+Officials+Point+Finger+at+Iran+in+Bank+Hack/article29610c.htm

http://www.slashgear.com/iran-cyberattacked-us-banks-according-to-government-officials-09264437/

http://www.theverge.com/2013/1/9/3854146/us-government-may-think-iran-behind-bank-ddos-attacks