Dissecting 'Operation Ababil' - an OSINT Analysis

ddanchev.blogspot.com.es/2012/09/dissecting-operation-ababil-osint.html

```
3. In the previous announcements we stated that we will not tolerate insulting exalted character of the prophet of
   mercy and kindness. Due to the insult, we planned and accomplished a series of cyber operations against the
   insulting country's credit and financial centers.
4.
5. Some U.S. officials tried to divert people's attention from the subject and claimed that the main aim of the
   operation was not deal to insults but it had other intentions. The officials claimed that certain countries have
   taken these measures to solve their internal problems.
6.
7. We strongly reject the American officials' insidious attempts to deceive public opinion. We declare that the
   kindness and love of Muslims and free-minded people of the world to the great prophet of Islam is much more than
   their violent anger be deflected and controlled by such deceptive tricks.
8.
9. Insult to a prophet is not acceptable especially when it is the Last prophet Muhammad (Peace Be upon Him). So as
   we promised before, the attack will be continued until the removal of that sacrilegious movie from the Internet.
10.
11. Therefore, we suggest a Timetable for this week attacks. Knowing which times the banks and other targets are out
    of service, the customers of targeted sites also can manage to do their jobs as well and have a rest while the
    specific organization is under attack.
12.
```

Provoked by a questionable online video posted on YouTube, Muslims from the around the world united in an apparent **opt-in botnet crowdsourcing campaign** aiming to launch a DDoS (denial of service attack) against YouTube for keeping the video online, and against several **major U.S banks and financial institutions**.

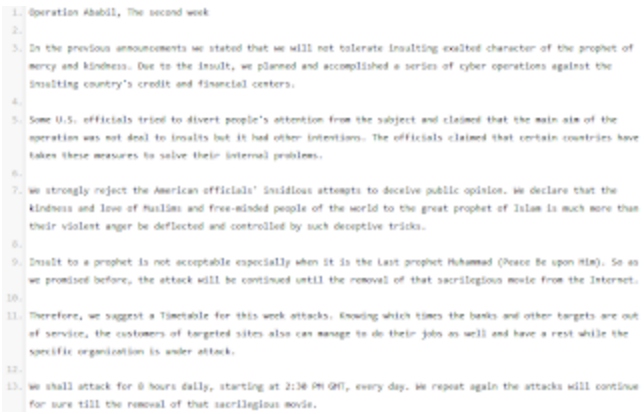
Dubbed "*Operation Ababil*", and operated by the Izz ad-Din al-Qassam a.k.a Qassam Cyber Fighters , the campaign appear to have had a limited, but highly visible impact on the targeted web sites. Just like in every other crowdsourced opt-in botnet campaign such as the "**Coordinated Russia vs Georgia cyber attack in progress**", the "**Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites**", the "**Electronic Jihad v3.0 - What Cyber Jihad Isn't**" campaign, and the "**The DDoS Attack Against CNN.com**" campaign, political sentiments over the attribution element seem to have orbited around the notion that it was **nation-sponsored by the Iranian government**.

What's so special about this attack? Did the individuals behind it poses sophisticated hacking or coding abilities? Was the work of hacktivists crowdsourcing bandwidth, or was it actually sponsored by the Iranian government? Can we even talk about attack attribution given that the group claiming responsibility for the attacks doesn't have a strong digital fingerprint?

In this post, I'll perform an OSINT (open source intelligence) analysis aiming to expose one of the individuals part of the group that organized the campaign, spread their propaganda message to as many Muslim Facebook groups as possible, and actually claim responsibility

for the attacks once they took place.

The campaign originally began with a message left on Pastebin.com by the Qassam Cyber Fighters group announcing "Operation Ababil":



Operation Ababil, The second week

In the previous announcements we stated that we will not tolerate insulting exalted character of the prophet of mercy and kindness. Due to the insult, we planned and accomplished a series of cyber operations against the insulting country's credit and financial centers.

Some U.S. officials tried to divert people's attention from the subject and claimed that the main aim of the operation was not deal to insults but it had other intentions. The officials claimed that certain countries have takes these measures to solve their internal problems.

We strongly reject the American officials' insidious attempts to deceive public opinion. We declare that the kindness and love of Muslims and free-minded people of the world to the great prophet of Islam is much more than their violent anger be deflected and controlled by such deceptive tricks.

Insult to a prophet is not acceptable especially when it is the Last prophet Muhammad (Peace Be upon Him). So as we promised before, the attack will be continued until the removal of that sacrilegious movie from the Internet.

Therefore, we suggest a Timetable for this week attacks. Knowing which times the banks and other targets are out of service, the customers of targeted sites also can manage to do their jobs as well and have a rest while the specific organization is under attack.

We shall attack for 8 hours daily, starting at 2:30 PM GMT, every day. We repeat again the attacks will continue for sure till the removal of that sacrilegious movie.

The original message left is as follows:
"*Operation Ababil, The second weekIn the previous announcements we stated that we will not tolerate insulting exalted character of the prophet of mercy and kindness. Due to the insult, we planned and accomplished a series of cyber operations against the insulting country's credit and financial centers.Some U.S. officials tried to divert people's attention from the subject and claimed that the main aim of the operation was not deal to insults but it had other intentions.*

The officials claimed that certain countries have taken these measures to solve their internal problems.We strongly reject the American officials' insidious attempts to deceive public opinion. We declare that the kindness and love of Muslims and free-minded people of the world to the great prophet of Islam is much more than their violent anger be deflected and controlled by such deceptive tricks.Insult to a prophet is not acceptable especially when it is the Last prophet Muhammad (Peace Be upon Him).

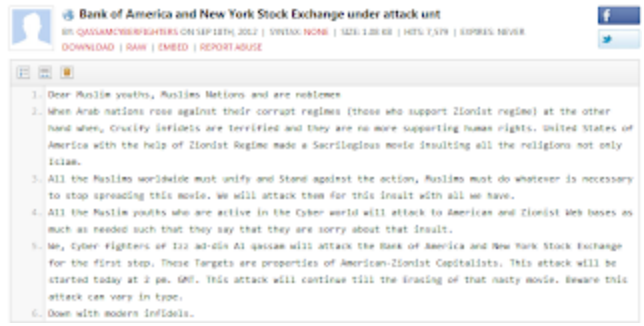
So as we promised before, the attack will be continued until the removal of that sacrilegious movie from the Internet.Therefore, we suggest a Timetable for this week attacks. Knowing which times the banks and other targets are out of service, the customers of targeted sites also can manage to do their jobs as well and have a rest while the specific organization is under attack.We shall attack for 8 hours daily, starting at 2:30 PM GMT, every day.

We repeat again the attacks will continue for sure till the removal of that sacrilegious movie.We invite all cyberspace workers to join us in this Proper Act. If America's arrogant government do not submit, the attack will be large and larger and will include other evil countries like Israel, French and U.Kingdom indeed.Tuesday 9/25/2012 : attack to Wells Fargo site, www.wellsfargo.comWednesday 9/26/2012 : attack to U.S. Bank site, www.usbank.comThursday 9/27/2012 : attack to PNC site, www.pnc.com Weekends: planning for the next week' attacks.Mrt. Izz ad-Din al-Qassam Cyber Fighters"

Periodically, the group also released update notes for the campaigns currently taking place:

The original message published is as follows:
"*Operation Ababil" started over BoA :http://pastebin.com/mCHia4W5 http://pastebin.com/wMma9zyGIn 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 ###*"

Second statement released by the group:



The original message published is as follows:
"*Dear Muslim youths, Muslims Nations and are noblemenWhen 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."

Clearly, the group behind the campaigns aimed to deliver concise propaganda to prospective Internet connected users who would later on be instructed on how to participate in the DDoS attacks. Let's assess the potential of the distributed DDoS tool that was used in the campaign.

Sample screenshot of the DDoS script in Arabic:

Inside the .html file, we can see that there are only three web addresses that will be targeted in their campaign:

```
</div>
<div>
      <dl>
                  <label id="statuss"></label>
            <dd style="opacity: 0.5;display:none;"  id="requestedCtr"></dd>
            <dt style="opacity: 0.5;display:none;" > </dt>
            <dd style="opacity: 0.5;display:none;" id="succeededCtr">0</dd>
            <dt style="opacity: 0.5;display:none;"> </dt>
            <dd style="opacity: 0.5;display:none;" id="failedCtr">0</dd>
      </dl>
</div>

<script>
var i=0;

var targets = new Array();
targets.push("http:// www.nyse.com/");
targets.push("http:// www.nasdaq.com/");
targets.push("http://www.bankofamerica.com/");

      (function () {
          var fireInterval;
          var isFiring = false;
          var requestedCtrNode = document.getElementById("requestedCtr"),
              succeededCtrNode = document.getElementById("succeededCtr"),
              failedCtrNode = document.getElementById("failedCtr"),
              targetURLNode = document.getElementById("targetURL"),
              fireButton = document.getElementById("fireButton"),
              messageNode = document.getElementById("message"),
              rpsNode = document.getElementById("rps"),
              timeoutNode = document.getElementById("timeout"),
                            statuss = document.getElementById("statuss");
          var targetURL = targetURLNode.value;
          targetURLNode.onchange = function () {
```

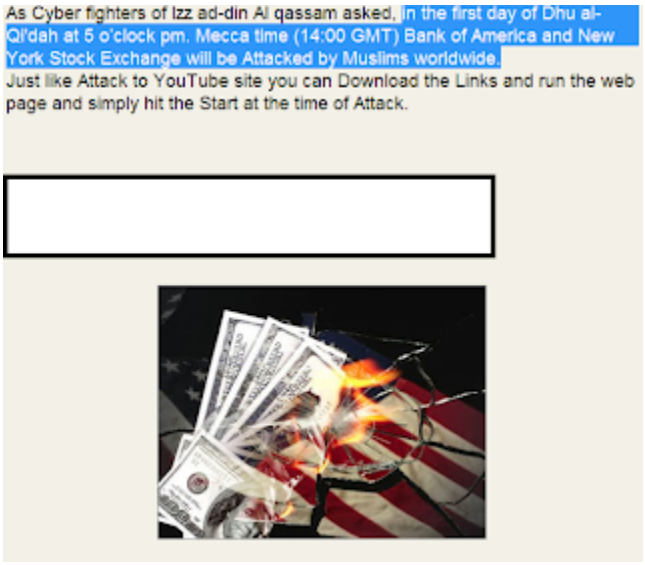
Detection rate for the DDoS script:
youtube.html - **MD5: c3fd7601b4aefe70e4a8f6d73bf5c997**
Detected by 6 out of 43 antivirus scanners as HTool-Loic; Hacktool.Generic; TROJ_GEN.F47V0924

Originally, the attack relied on a static recruitment message which included links to the DIY DDoS script located on **4shared.com** and **Mediafire.com**. What's particularly interesting is the fact that the files were uploaded by a user going under the handle of "*Marzi Mahdavi II*". It's important to point out that these static links were distributed as part of the recruitment campaign across multiple Muslim-friendly Facebook groups.
Thanks to this fact, we could easily identify the user's Facebook account, and actually spot the original message seeking participation in the upcoming attacks.

Marzi Mahdavi II's Facebook account:

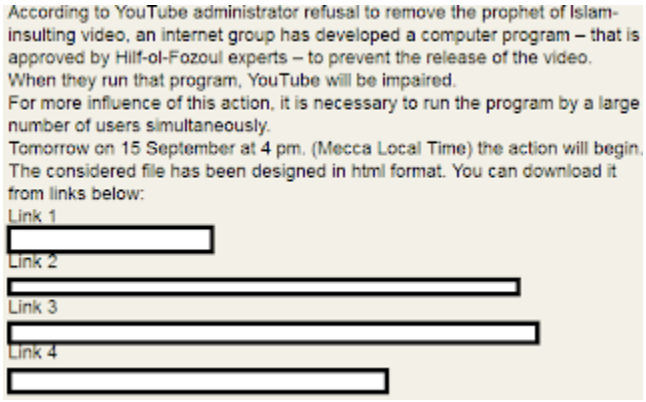
Sample shared Wall post seeking participation in the upcoming DDoS campaign:

Sample blog post enticing users to participate:



Marzi Mahdavi II has once referenced a link pointing to the same blog, clearly indicating that he's following the ongoing recruitment campaigns across multiple Web sites:

Second blog post enticing users to participate in the DDoS campaign:



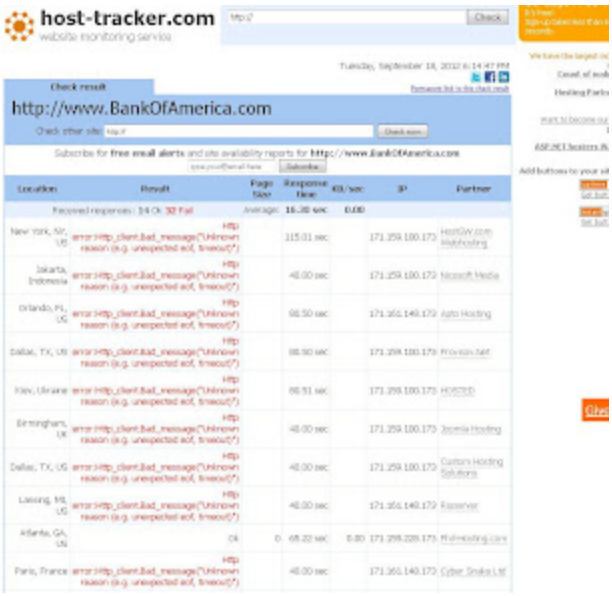
This very latest example of Iran's hacktivist community understanding of the cyber operations, once again lead me to the conclusion that what we've got here is either the fact that Iran's hacktivist community is lacking behind with years compared to sophisticated Eastern European hacking teams and cybercrime-friendly communities, or that Iran is on purposely demonstrating low cyber operation capabilities in an attempt to trick the Western world into thinking that it's still in a "catch up mode" with the rest of the world when it comes to offensive cyber operations.

Did these coordinated DDoS campaigns actually had any impact on the targered web sites? According to data from the Host-Tracker, they seem to have achieved limited, but visible results, a rather surprising fact given the low profile DDoS script released by the campaigners.

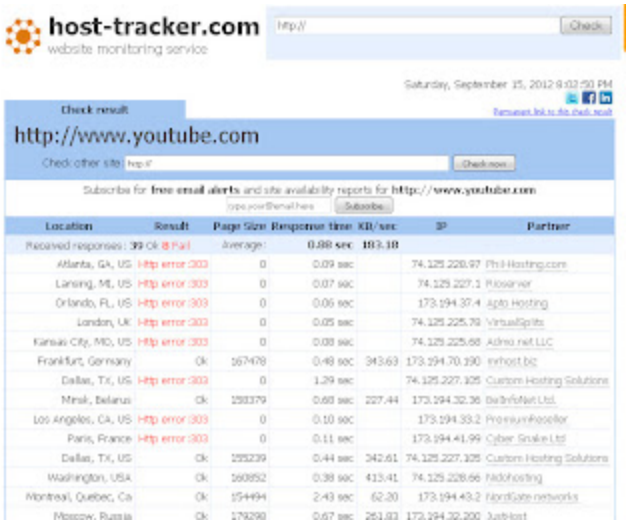
Sample Host-Tracker report for a targeted web site during the campaign:

Second Host-Tracker report for a targeted web site during the campaign:

Third Host-Tracker report for a targeted web site during the campaign:



Fourth Host-Tracker report for a targeted web site during the campaign:



Fifth Host-Tracker report for a targeted web site during the campaign:

Is the Iranian government really behind this campaign, or was it actually the work of amateurs with outdated and virtually irrelevant technical skills? Taking into consideration the previous **DDoS campaign launched by Iranian hacktivists in 2009**, in this very latest one we once again see a rather limited understanding of cyber operations taking into consideration the centralized nature of the chain of command in this group.

What's also worth pointing out is the fact that this is the first public appearance of the group that claims responsibility for these attacks. Considering this and the lack of a strong digital fingerprint for the group in question, virtually anyone on the Internet can **engineer cyber warfare tensions between Iran and the U.S**, by basically impersonating a what's believed to be an Iranian group.

This post has been reproduced from Dancho Danchev's blog. Follow him on Twitter.