radware

Smart Network. Smart Business.

ERT Threat Alert

#OpAbabil Phase 4

Emergency Response Team

7/26/2013

Threat Overview: #OpAbabil Phase 4

The week of July 22nd has started the fourth wave of DDoS attacks against U.S. banks and financial institutions. Cyber Fighters of Izz ad-Din al-Qassam, the group behind the previous three waves of OpAbabil attack against U.S. banks, has announced its fourth phase. This is the continuum of its fight against what it refers to as – "the widespread and organized offends to Islamic spirituals and holy issues, especially the great prophet of Islam and the offending film on the Internet."

The targets of this attack remain leading U.S. banks including Bank of America, Chase Bank, PNC, Union Bank, BB&T, US Bank, Fifth Third Bank, Citibank and others.

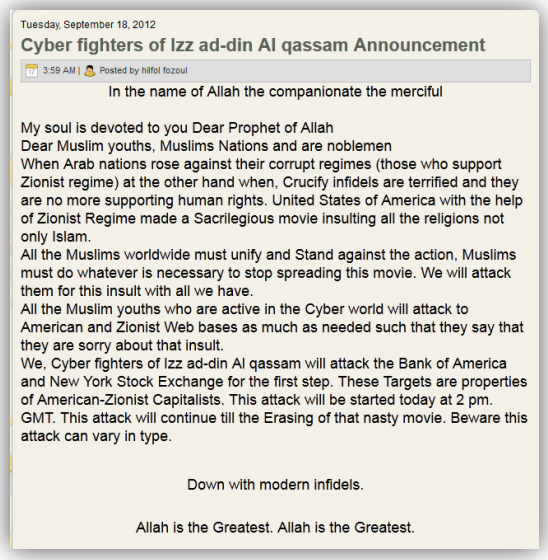
On their Pastebin post the group threatens to continue the attacks until the film *"Innocence of Muslims"* is completely removed from the Internet. Cyber Fighters of Izz ad-Din al-Qassam announced "the new phase will be a bit different and you'll feel this in the coming days."

Radware's Emergency Response Team (ERT) has witnessed high volume TCP and UDP flood attacks, DNS implication attacks and SSL based attacks. The group has published a formula to justify the fact the U.S. must pay in money for the insult.

Background

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

On September 18 2012, a group called "Cyber Fighters of Izz ad-Din al Qassam"announced a cyberattack campaign and called for an attack on its '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. The goal of this ongoing attack campaign is to down U.S.-based financial institutions' web sites and online services.



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 Operation Abibail Attack Campaign Announcement

Attack Vectors

Radware's ERT is actively involved in fighting and mitigating these attacks and found these attacks to be both sophisticated and containing multiple complicated attack vectors. While there is no attack tools published, the ERT sees evidence of several types of DoS attacks:

- **Massive TCP and UDP flood attacks—**targeting both Web servers and DNS servers. Radware's ERT has tracked and mitigated up to 25Gbps of attack traffic against one of its customers. We expect more of the same in the coming attack phase

- **DNS amplification attacks**—the attacker finds an internet domain that is registered with many DNS records. During the attack, the attacker sends DNS queries that request the entire list of DNS records for that domain. This results in large replies from the DNS servers, usually so big that they need to be split over several packets
- **HTTP flood attacks**— cause web server resource starvation due to overwhelming number of page downloads
- **Encrypted attacks based on SSL protocol running HTTPS GET requests—**SSL attacks not only generate load on the HTTP server, but also consume 15x more CPU resources which are involved in processing the SSL traffic

Such large volumetric attacks possibly come from server bots a.k.a Brobot. The ERT has recently witnessed a significant increase in the Brobot and DDoS-for-hire market.

Traffic diversion using BGP routes, may be the "ace up the sleeve" to which the attacking group was referring.. It seems that the attacker is publishing BGP routes in order to reroute traffic out of the target address space. This may lead to denial of service or "man in the middle" attacks.

Radware ERT Recommendations

- Deploy a DDoS mitigation solution on-premise. This can mitigate application attacks as well as SSL based attacks

- Deploy in-thecloud DDoS scrubbing. This can mitigate volumetric TCP and UDP flood attacks that may cause internet link saturation