True DDoS Stories: The Cyber Fighters

David Holmes, 2013-14-01

The Cyber Fighters are using a formula based on YouTube Likes, Dislikes, and the cost of anti-DDoS services to project how long they will continue their attack: 56 weeks.

I couldn't make this stuff up if I tried. Some crazy guy hires some actors, makes a truly horrible movie, adds anti-Islam content (post-production, say the innocent actors), and now there's a Cyber-jihadist group attacking the US financial sector until the video is taken down. Note that the US firms are basically the same type of victims from the WikiLeaks saga, but this time, instead of being targeted in the name of information freedom, they are being targeted in the name of censorship.

There is conjecture that the Cyber Fighters are unofficially sponsored by Iran, as payback for Stuxnet, but after reading the latest Cyber Fighters pastebin post, I'm inclined to believe that these guys really are just "protesting" the video. Read on and see if you disagree with me.

Backing up to the September Attacks

Because of the sheer volume of the September attacks, every target was forced to call an external anti-DDoS provider – either Prolexic or their own service provider (which is typically just a rack of Arbor boxes). Akamai has provided some defense as well, due to its distributed nature. The Cyber Fighters mixed a broad range of attacks, from simple UDP floods targeting DNS to SSL floods that got all the way through into the origin data center (since most financials don't share their SSL keys with their service providers).

As a result of the malicious SSL traffic, even with the anti-DDoS providers rate-limiting 90% of the traffic away from the origin data centers, the application tiers of many of the service providers stayed down, and on-premise defenses (such as, ahem, F5 gear) were enlisted to scrub that traffic.

For the September attacks, the Cyber Fighters used an interesting twist. A vulnerability in old versions of WordPress was exploited, where they dropped in the **itsoknoproblembro** DDoS toolkit and then launched kamikaze GETs and POSTs using these high-speed servers. They had enough of these to overwhelm blacklists for a while, but it sounds like Prolexic and the other DDoS providers are getting these IPs figured out and are blocking traffic from them.

End of story, right? Not really.

56 more weeks, unless you Dislike!

The Cyber Fighters, like all hacking groups, know all about Prolexic and the other anti-DDoS services. In fact, their attacks this week **rely** on the fact that some of these services charge by the megabyte or by the hour, not by the engagement. In last week's post to Pastebin, the Cyber Fighters show they are using a formula to calculate how long they should keep on attacking.

> Cyber Fighter "Insult Metric to Attack Time" Formula

```
/* Based on popularity of "Innocence of Muslims" video */
```

```
T = 26546482 /* total views */
L = 73721    /* total likes */
D = 194906   /* total dislikes */
DF = 10      /* coefficient dislike factor */
CF = 100$    /* ransom per each view/like */
C = 30000$   /* Approximate Cost on US banks per each DDoS minute */

TC = (T+L-F*D) * CF = 2,467,114,300$
TM = TC/C = 82237 minutes
S = 420 minutes

===> TD = TM/S = 196 days

PD = (6-1+4)*3 = 27 days
REM = TD-PD = 169 days ( about 56 weeks or 14 months )
```

Basically, they perceive any “view” or “like” of the offending video to be an insult, and to that they add some time to their attack. They will subtract ten times that amount for every dislike. Ultimately, they multiply all this time by what they consider the “cost of the anti-DDoS services”, which they estimate at the crazy number of $30,000 per minute (the services are expensive, but I don’t think they’re *that* expensive).

With all their calculation, they project the duration of the attack, based on these “insult metrics,” to be **56 more weeks**. 56 weeks from now is well into 2014.

This is an interesting example of what Mike Rothman at Securosis [PDF] calls “**eDoS**” – purposefully attacking someone to cause “economic Denial of Service”. The CyberFighters’ aim is to produce $2.5 billion dollars in eDoS damages.

So you tell me... State-sponsored or not?

I’ve never seen anything like this before. If they are taken at their word, the Cyber Fighters are a different breed, to be sure; they even claimed to have suspend their attacks periodically to give the oppressed IT workers defending the banks time to rest.

It is one thing to claim lofty ideals about hacktivism, but it’s another to go all left-brain quantitative about it, complete with if () statements and old C-style comments. There's a weird, authentically geeky mind behind this. Whether or not that kind of mind can be bought off by a state is the real question. The personality that writes like this, that makes a show of defiance, is typically operating under from their own (non-commercial) motives. See: The Jester, AnonymouSabu, and others. Of course, this doesn’t prove that the Cyber Fighters *aren’t* sponsored by Iran or some other agency or state, but it's a data point.

So if the Cyber Fighters are another **True DDoS Story**, all I can say is that I couldn’t make this up if I tried.

Related blogs & articles:

True DDoS Stories: SSL Connection Flood

The Spectacular Rise and Fall of LulzSec

Defending Against Denial of Service Attacks [Securosis PDF]

Mitigating Nuclear DDoSer, R-U-Dead-Yet, Dirt Jumper, Keep-Dead, and Tor Hammer with F5

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com