Distributed Denial of Service Attacks (DDOS):

Fighting to Protect our use of the Internet

May First/People Link

November 11, 2016

Political Context

Two kinds of attacks:

- *Compromise*: When an attacker gains access to your site or database and can see files or data that should not be available to them.
- *Denial of service:* When an attacker floods your site with traffic so that nobody else can access the site.

How does it work?

A “distributed” denial of service attacker

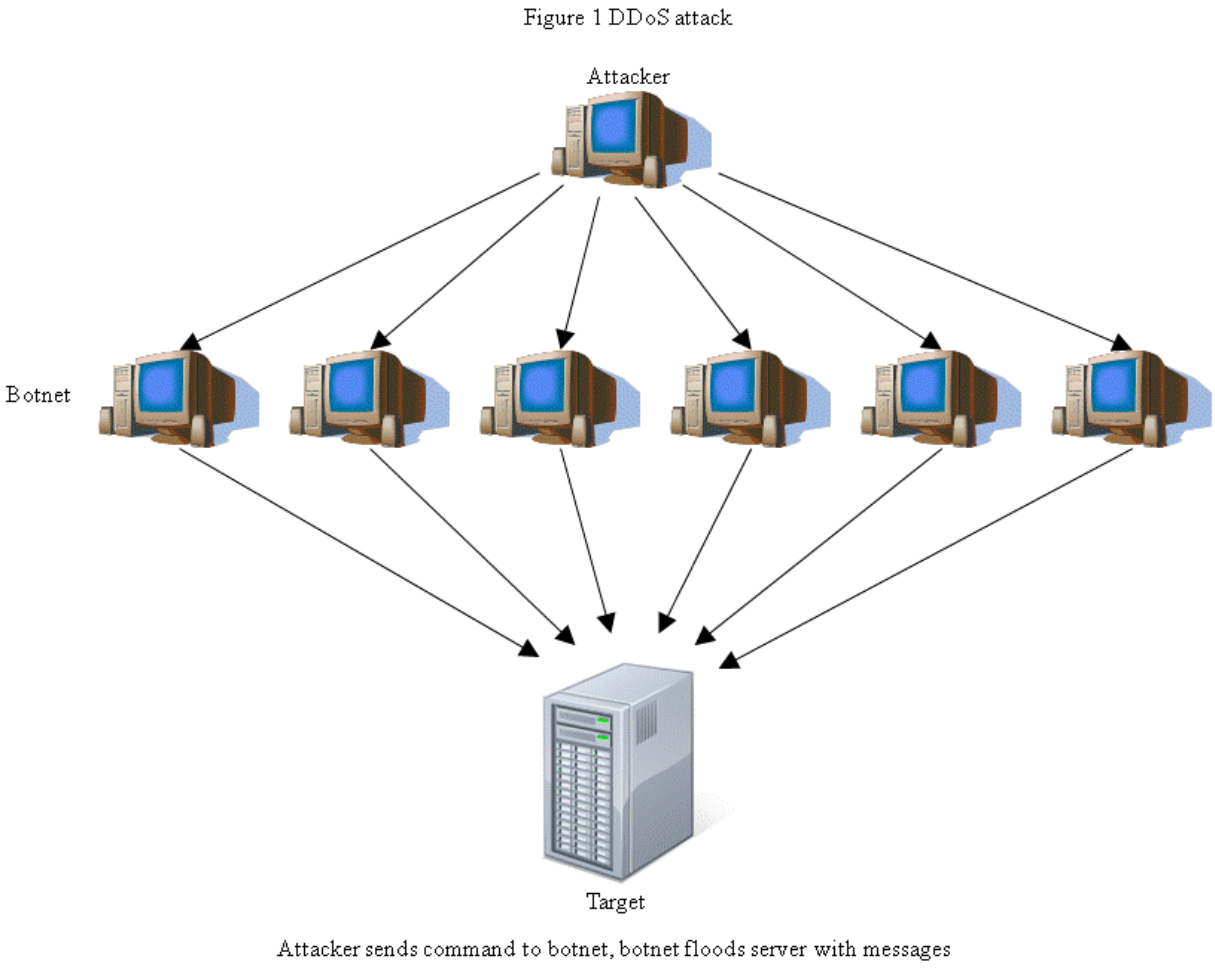
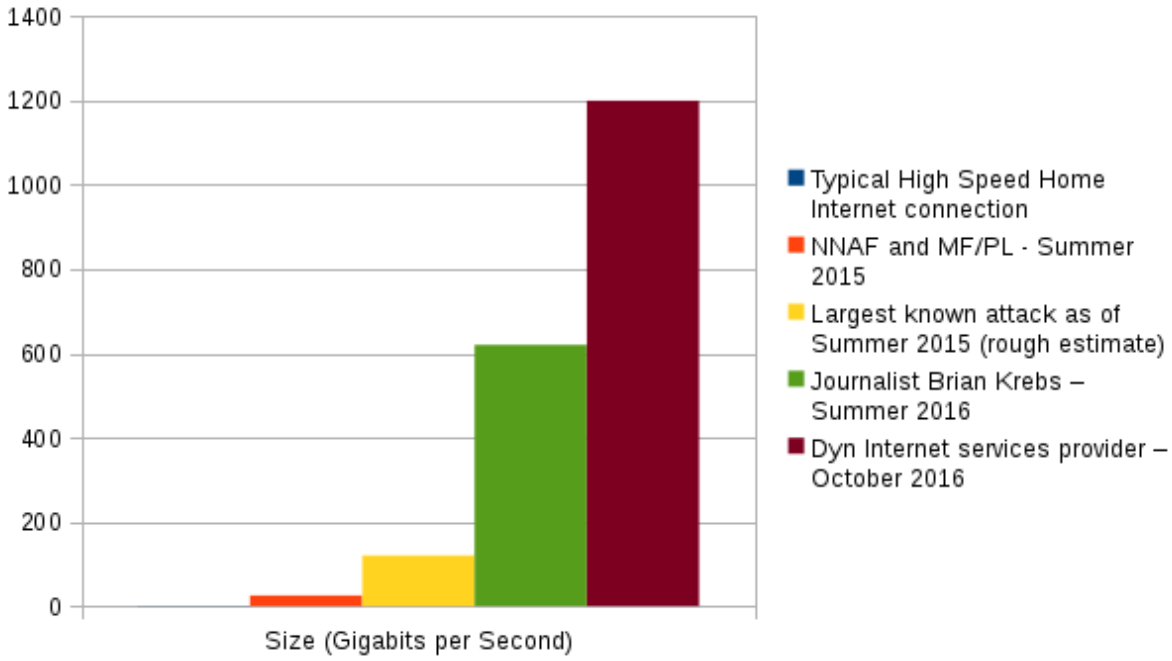


Image credit: http://www.cs.wustl.edu/~jain/cse571-11/ftp/cyberwar/

How bad is this?



How are bot networks built?

Mirai software, game changer? Or just 62 really dumb default passwords...

```
    // Set up passwords
    add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);  // root     xc3511
    add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);       // root     vizxv
    add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);       // root     admin
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);   // admin    admin
    add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);   // root     888888
    add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);   // root     123456
    add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);       // root     54321
    add_auth_entry("\x50\x4D\x4D\x56", "", 4);                           // root     (none)
    add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);           // root     root
    add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);       // root     12345
    add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);           // user     user
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                       // admin    (none)
    add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);           // root     pass
    add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16", 2);           // root     1234
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x10\x11\x16", 1);       // admin    1234
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x10\x11\x16\x17", 1);   // admin    12345
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x17\x16\x11\x10\x13", 1);   // admin    54321
    add_auth_entry("\x4F\x4D\x56\x4A\x47\x50", "\x44\x57\x41\x49\x47\x50", 1);   // mother   fucker
```

How is this possible?

- Some network still allow spoofed addresses (BCP38). Full implementation of BCP38 would stop “amplification attacks”
- Failure of capitalism: rush to profit means selling devices that have known flaws. Must recall all devices with known problem and impose fines (like car manufacturers who are caught selling known unsafe cars)
- Providers don’t care – you get billed for your Internet usage. Must detect and stop attacks (like the way you get a notice if you are downloading copyright material)
- Centralization
    - By investing in Facebook, Google and Twitter, we create a massive chasm between the capacity of a few companies and the rest of us. They will use this divide to their advantage. Will we live in a world where only two or three corporations can with stand a denial of service attack and the rest of us can’t?
    - Not even the big corporations are safe – we must build de-centralized services, that are designed to put information on multiple networks.

Stopping a Denial of Service Attack

Using a “reverse proxy” cache

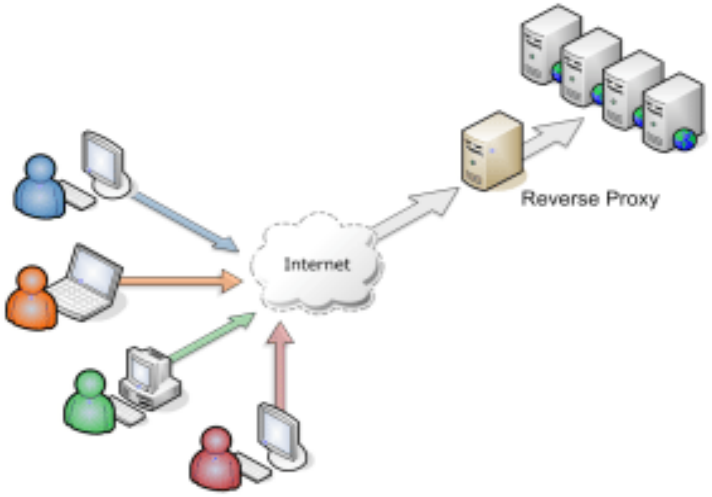
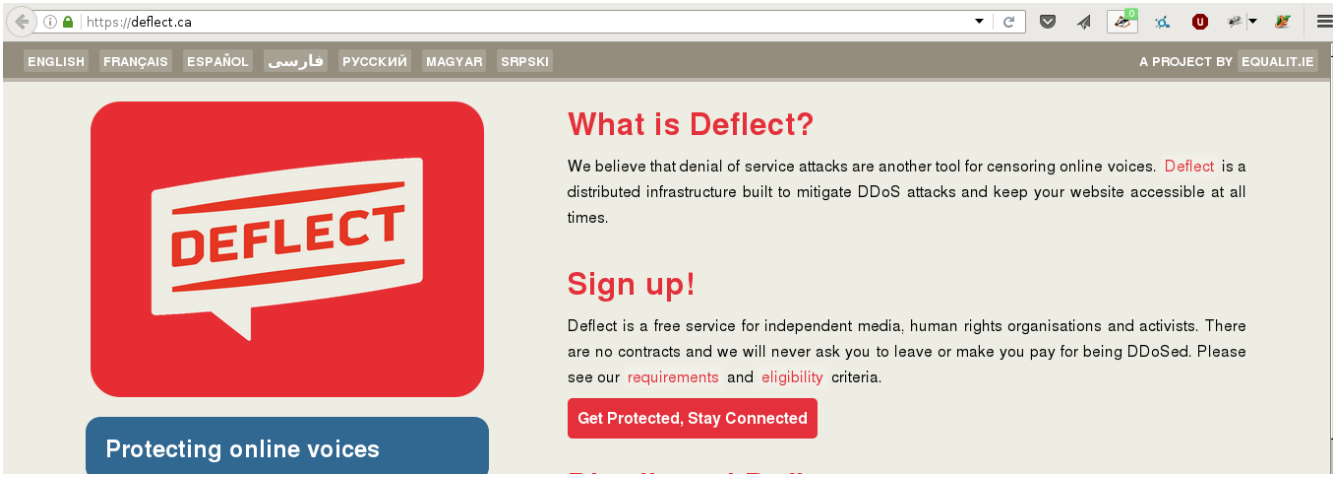


Image Credit: http://blog.caelum.com.br/melhorando-o-guj-jetty-nio-e-load-balancing/

Stopping a Denial of Service Attack

Signing up with Deflect



How does our network protect us?