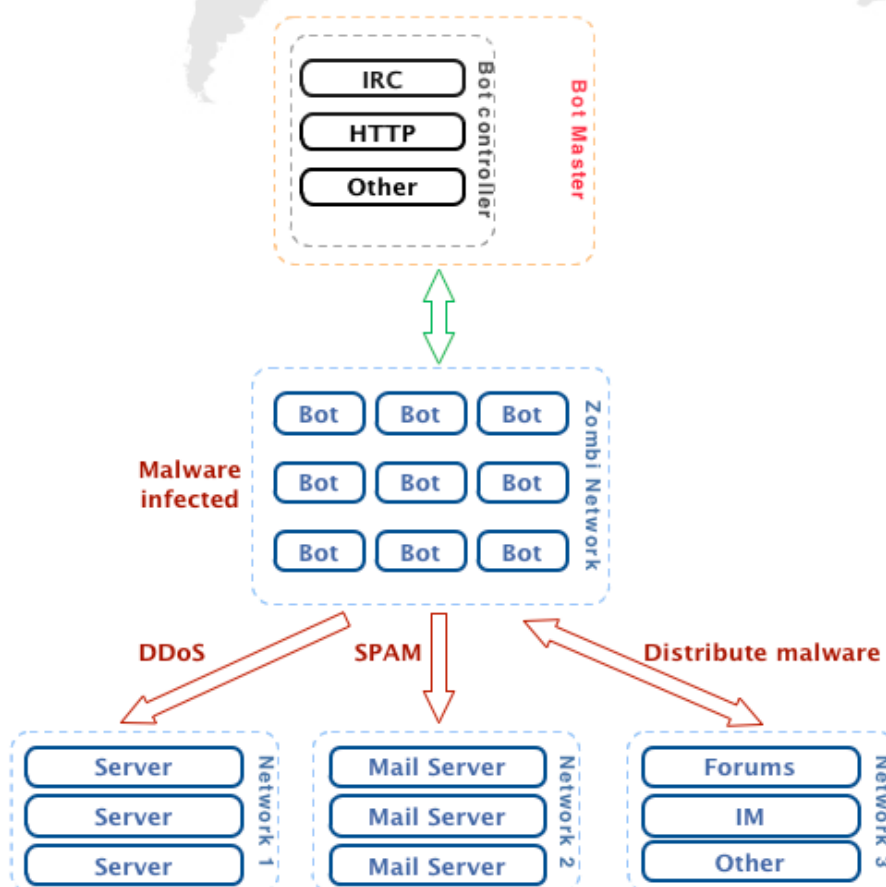


<http://en.wikipedia.org/wiki/Botnet>

Botnet is a jargon term for a collection of software agents, or robots, that run autonomously and automatically. The term is most commonly associated with malicious software, but it can also refer to a network of computers using distributed computing software. While botnets are often named after their malicious software name, there are typically multiple botnets in operation using the same malicious software families, but operated by different criminal entities.

From this common definition we can deduce the basic behaviour of a botnet and then start to develop a more complex vision of the problem.

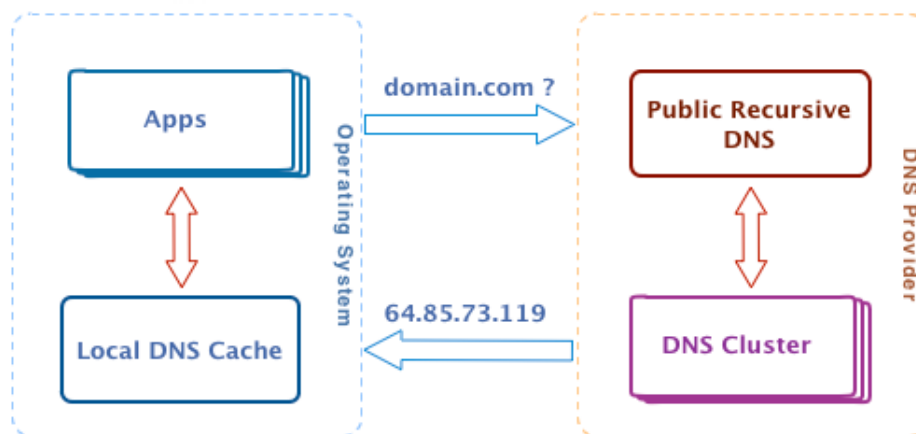


These machines were first developed in the 90's. However they were not used for economical benefits but instead to distribute attacks and bouncers for new attacks, etc. It was then the cybernetics mafia began using them in a new business model and to this day they are the most frequently employed for illegal acts on the Internet.

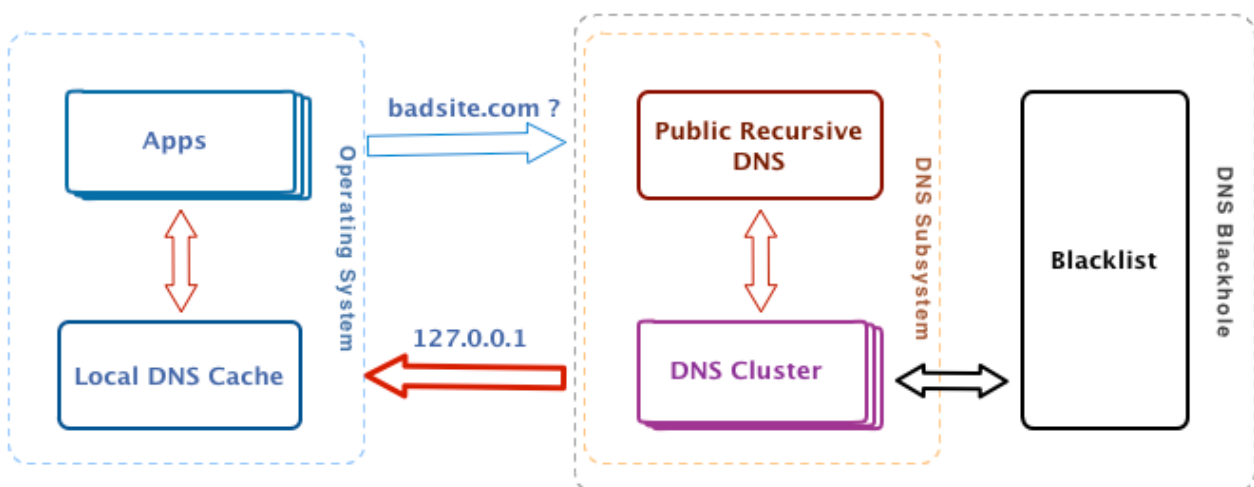
For this purpose they developed a new methodology based on the Malware infection so as to infect the resources of computers. In the beginning the most common way to control these infected computers was to use a IRC (*Internet Relay Chat*) channel. Now a new mechanism for controlling has been developed that is becoming increasingly more common, which is based in HTTP (*Hypertext Transfer Protocol*) This for instance being used for Twitter.:<http://asert.arbornetworks.com/2009/08/twitter-based-botnet-command-channel/>.

Once the computer is infected with Malware and they start to access the channel control, the computers are in a "zombie-state" waiting for new orders from the Bot's Master side, who is the one frequently responsible for financing the creation of the botnet. The common objective of this payment is to be able to have access to this botnet in order to carry out malicious attacks, such as **DDoS** (*distributed denial-of-service attack*), **SPAM** (*junk-email*) or even to distribute more malware with other different objectives as **Phising**.

As a solution, some companies offer a new internal security service whose objective is to prevent user access by deploying one of the oldest network protocols of the Internet, the **DNS** (*Dynamic Name Server RFC 1034/1035 de 1987*) protocol.



Clients request a name resolution for the domain.com through a public DNS server and this returns the result to the client 64.85.73.119. To add a new layer of security, companies make a **public DNS server**, available to the client, that works in the same way as the standard protocol.



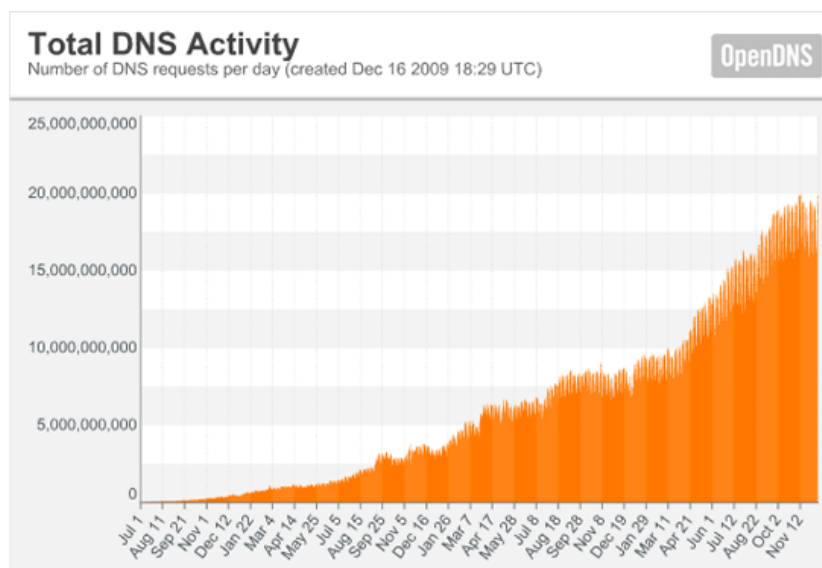
This server will compare *using a blacklist* whether or not the domain that is trying to be resolved, badsite.com, is available within their database of Malware domains. It will then process this information in order to disguise the name's resolution to a different IP, in this case 127.0.0.1. This kind of modification is known as DNS Hijacking. In this way we will be sure that our client is not caching the destiny.

By employing these services we will achieve the following:

1. **DNS cache and less latency** : the Web browsing experience will be faster due to the server having most of the cases requested by other users. Most of them have a cluster Geolocated, improving the response time in every request.
2. **Content parental control** : blacklist can have sites with pornographic content, violent, etc.
3. **Anti-SPAM Filter**: is not necessary an external filter to know the origin of an active spam source. It was the case most frequently to use RBL (*Real-time Blackhole List*), DNSBL (*DNS Blacklists*), DRBL (*Distributed Realtime Block List*), DNSWL (*DNS Whitelist*), RHSBL (*Right Hand Side Blacklist*) o URIBL (*Uniform Resource Identifier Blacklist*). Frequently used from SPAMHAUS (<http://www.spamhaus.org>) , SpamCop (<http://www.spamcop.net>).
4. **Adsense filter** : apart of the Anti-SPAM filter, this can be exported to other protocols such as to HTTP. in which the filtering of the marketing content is even easier than putting a HTTP proxy with a blacklist.
5. To have a **DNS address available and quite easy to remember**.
6. **Orthographical correction and autocompletion** : if a domain resolution fails, it can try to find out if there is some typographical error, returning the domain information in a good state.

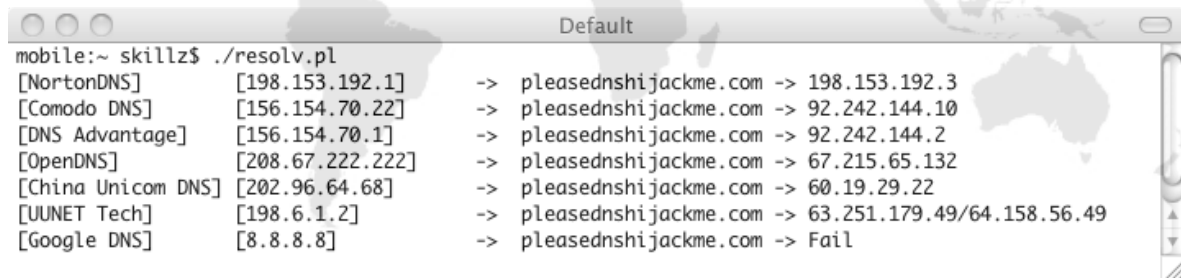
We should remember that the purpose of Internet is to create a decentralized and independent network, or at least in definition it should be. But, what has happened with the bigger services operators that are providing public DNS services with the above characterises mentioned?, we can take the example from **OpenDNS**.

Latest statistics of use that are being published in various blogs (<http://blog.opendns.com>) : are shedding light on some interesting data to consider:



As we see from the chart, resolving 20 millions of DNS petitions in 24h, has doubled the final figure (10 millions), in April of the same year. More than 25.000 schools in the USA are using **OpenDNS**, and several companies are migrating to their services.

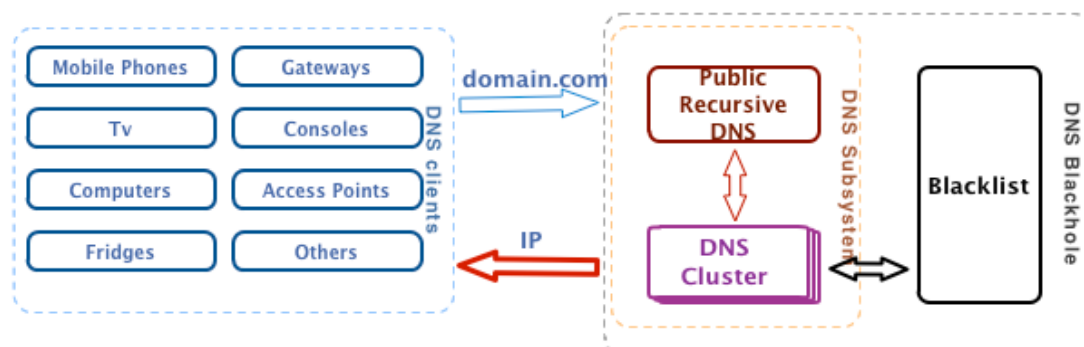
In the following picture we can see the DNS petition within the public servers (mentioned above) that are being offered.



```

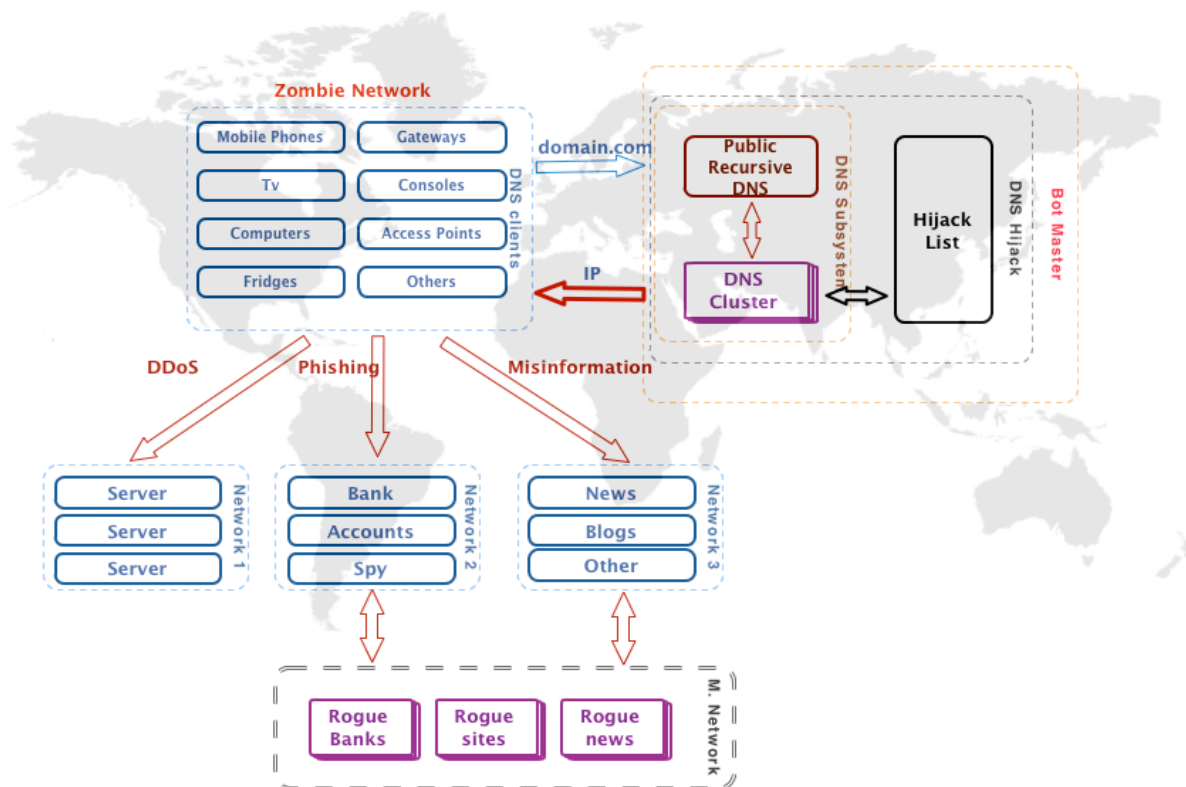
mobile:~ skillz$ ./resolv.pl
[NortonDNS]      [198.153.192.1]  -> pleasednshjackme.com -> 198.153.192.3
[Comodo DNS]    [156.154.70.22] -> pleasednshjackme.com -> 92.242.144.10
[DNS Advantage] [156.154.70.1]  -> pleasednshjackme.com -> 92.242.144.2
[OpenDNS]       [208.67.222.222] -> pleasednshjackme.com -> 67.215.65.132
[China Unicom DNS] [202.96.64.68] -> pleasednshjackme.com -> 60.19.29.22
[UUNET Tech]    [198.6.1.2]     -> pleasednshjackme.com -> 63.251.179.49/64.158.56.49
[Google DNS]   [8.8.8.8]       -> pleasednshjackme.com -> Fail
  
```

Maybe it is the moment to consider whether this is a good idea or not, or even if would be necessary to stop it. We are allowing far too much control of the Internet, to multinational companies with their private interests and own servers. It has been proved that several of them are conducting DNS hijacking to return fake results and in order to redirect users to sites under their control, so as to demonstrate custom publicity through the domain showed, in order to generate stats to sell, etc. At the moment most of them are offering this service without personal benefit as a public service, but do we believe this?. Remember the latest chart applied to any device to connect to Internet:



Consider again the control features of this that these companies can utilise in their clients name. And also ***how the biggest botnet was developed that has extremely intelligent logic.***

- **Is not necessary to find vulnerabilities to create bots:** it is frequently seen that bots are launched through infections.
- **Is not necessary to develop Malware/Software for management or for updating:** everything is continually being developed. The only necessary thing to do is to take in advance the protocol that will manage the bot. Is not necessary updated, due to the resolutions are dynamic and a DNS server change is immediately.
- **DNS resolution supports all the operating systems :** GNU/Linux, MS Windows, Mac OSX, Android, iOS, Bada, *Nix, VxWorks, etc.
- **Any device can be a Bot:** a mobile phone with Internet connection, game console, etc.
- **It is possible to do these same attacks.***
- **Less evidence in a forensic analysis :** this should be available in traffic captures, is not Malware working on the system and the DNS changes are dynamic (but they are not registered). Only the local cache could give a proof but normally it expires in periods too short.
- **The “infection” is based in social engineering:** offering a DNS service
- black hole, cache and an easy DNS address to remember.
- **The vast majority of firewalls allow DNS traffic :** In almost organization external traffic is allowed for name resolution.
- **Capacity to attack based in Geolocation services:** knowing the origin of the IP you can then figure out the destination of a specific attack. Custom Phising, DDoS with less latencies in the same country, etc.



*Example of attacks :

1. **DDoS** : it is possible to pose as the client in order to forward all the traffic generated to IP victim directions. What will happen if we switch the register of *.google.com to critical a IP address?
2. **Phishing** : the same as poisoning cache attack. This is not necessary due to the client trusting the DNS server. Accounts will be captured, as well as credit cards numbers, users and passwords for critical sites.
3. **Misinformation** : fake resources will be available, causing confusion to the user or population.
4. **Spying** : it will be present in emails, instant conversation or VoIP.

Several references are available indicating the presence of patriotic botnets that governments are developing with botnets containing their own weapons for future cyberwar. Proof of these are found in the following links:

<http://seclists.org/fulldisclosure/2010/Jun/346>.

<http://translate.google.es/translate?js=y&prev=t&hl=es&ie=UTF-8&layout=1&eof=1&u=http%3A%2F%2Fwww.publico.es%2F323921%2Fataque&sl=es&tl=en>

It is evident to see that these companies are present in different locations within the most important countries of the World, and also that these resources are available for countries in conflict. The interest of the country always overrides that of human logic, and all kind of weapons are used to neutralize the enemy. What will happen when the enemy begins to attack? Is it time for ,countries to create their own Golden shield project?, (http://en.wikipedia.org/wiki/Golden_Shield_Project).A project to have under control/censure, to be operated by the Ministry of Public Security (MSP), a division of China's government. The project began in 1998 and their operations in November 2003.

Maybe this "China Firewall" is merely a simple tool to control/censure all the citizens. To be more than a firewall, and who's real objective is to be ready for war.

Without legislation to control all of these mechanisms in a global and open way, within a country engaged in conflict who has the capability to create his own cyber-army, we will merely be pawns confused over the marketing.If we only give these controls under "trust" to big companies we will forgot the words of **G.Washington**:

"To be prepared for war is one of the most effectual means of preserving peace."

Reverse Skills.

<http://twitter.com/reverseskills>