Fast-flux Service Networks in botnet malware

ROGER LARSEN
Autumn Term Paper - IMT 4651 Applied Information Security
Gjøvik University College 2010,

Abstract
Botnets have for several years chocked security companies and researchers - with good reason. Botnets are a very complex and powerful kind of malware. Botnets in action controls computing power through the world similar to several supercomputers in the hands of cyber criminals. Large security companies predict that we have not seen the worst yet. A recent botnet in media, Zeus, was estimated to an attempted loss of $220 millions, but actual cost was *only* $70 millions. Trends show that industry will be the next victim for massive attacks from botnets. Fast-flux botnets uses weakness in DNS to hide their actually origin. Fast-flux is a technique many botnets use to hide their servers and/or origin site. They manipulate weaknesses in Domain Name System (DNS) to hide behind proxy agents that redirect sessions to their scam/fraud servers. In this paper I will describe malware and botnets in general and the DNS manipulation technique Fast-flux in more details.

Categories and Subject Descriptors: D.4.6 [**Security and Protection**]: Malware

General Terms: Computer Security, Malisious Software

Additional Key Words and Phrases: Botnets, Fast-Flux, FFSN

1. INTRODUCTION

Computer security is a crucial issue in every business and for many households as well. Every company/organization/public office have some knowledge in basic computer security. The computer department updates our computers, servers operating systems etc. to match the latest security threats. We rely on traditional security mechanisms like firewall and antivirus applications. We all have a good nights sleep and believe everything is all right... but is it really?
Probably not - antivirus and updated systems are a step behind evil malisious software (malware) every day. The process from a new malware is found until we are *"updated"* can take several days depending on the complexity of the virus, the antivirus supplier and Internet usage frequency of the actual computer. This makes every computer connected to the Internet exposed unprotected to new viruses all the time. The number of viruses are enormous. When the rate of new variants of malware are found to be can be as high as 60.000 in average every 24 hours[1] we really have a challenge (or cyber war in other word) [McAfee, Inc. 2010]. The developement in malware latest years have shocked even people working in computer security business. Botnets represents the most scary malware. In this matter we can say that there is a cyber war on Internet, especially against the botnet malware.

[1]McAfee revealed this number in their "McAfee Threats Report: Third Quarter 2010" October 16, 2010

Contents

1.1 This papers structure

This paper starts with some historical background regarding malware history and botnets more in general. Further i describes how Fast-flux technique works with an example from the real world. I finally list some predictions/trends for 2011. Enjoy reading!

2. MALWARE

2.1 Malware history

Malware have been defined since 1971. *The Creeper virus* is the first known malware. It was an experimental self-replicating program written by Bob Thomas at BBN Technologies. In the early 70's it was only the military and scientists that was able to use computers. This was the start of an complex history regarding computer malware. In the 80's Personal Computers (PC's) came more and more in housholds. There where eager young computer fanatics that lived for their hobby; computer programming. This made the malware evolution some steps further, but still malware where in general rather interresting in technical matter.

In 1988 malware started to get evil - harddisks got erased/formatted and programs and/or documents was deleted. In the 90's the Internet came to the households and computer industry was getting really big. With Internet we got malware infected from computers on the other side of the planet in minutes. Software companies began developing antivirus programs as a protection against more and more evil malware. Until no malware was primary created and used by private persons and/or small groups - now a much more powerfull group entered the scene; criminal organisations/mafia. Malware was now more business and money then ever before. They targeted personal and business computers with information gathering as their goals. Malware was getting more and more "intelligent" and collected bank account information and passwords - and sent this information to the creator(s) of the malware. This is today called phishing.

The number of malware passed 1.000.000 when entering 2008. The number of newly detected malware in 2007 was 2/3 of the total number in 2008. The graphs are likely to go logarithmic regarding number of malware. Today we have computers in almost every electric unit. Many people have so-called smartphones (small computers that you also can call with) and electronic book's (tablets) et.al. These mobile computerized units are all exposed for evil malware in different degrees.

Sources: [Information Please 2007] [Famento Inc. 2008] [Krebs 2003] [Panda Security,S.L. 2009] [Paquette 2001] [Symantec Corp. 2010]

Please see the appendix A and B for more details on definitions and historical malware timeline.

2.2 Malware today

Now in 2010 malware have entered a new stage; malware used in the national strategic toolbox. The most frightening malware in this category is the Stuxnet. It is a so-called botnet (a word derived from "software robot network" A). This kind of malware are commanded and controlled of its botmaster. Botnet malware are often a mix of several categories of malware, and can (by order or by threats)

change its pattern/behaviour (polymorphic). The Stuxnet malware attacks industrial equipment (PLC's) and can do a lot of damage to the industry directly - and indirectly people in general. Rumours point out U.S.A. or Israel's government as the source/creators of this malware [Fisher 2010]. This malware have recently hit Iran's atom industry quite heavily.

In November, 2010, we have recent heard that the controversial WikiLeaks website have been attacked by hackers. Today December 10, 2010 a counter attack from WikiLeaks supporters have been announced. You can enter a website and anonymously join in and be a part of an attack against big companies like punish Visa, Mastercard, Amazon and PayPal. See figure 1

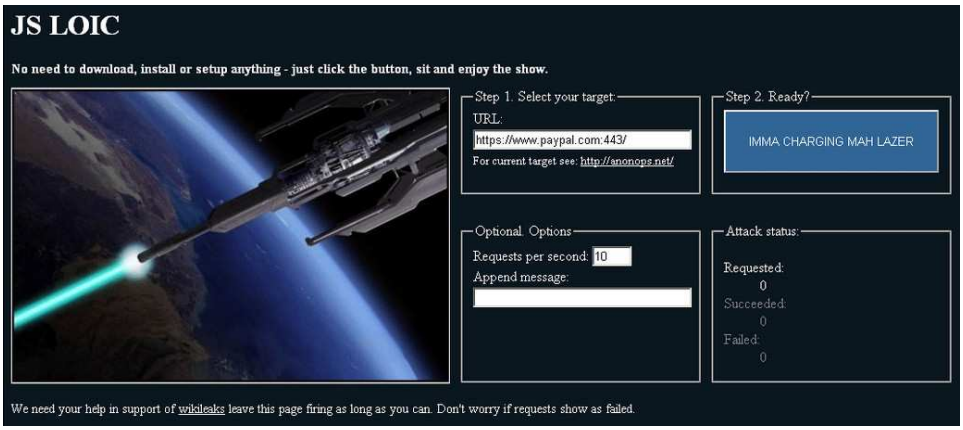

Fig. 1. GUI from web page to join-in against enemies of WikiLeaks.

Sources: [Symantec Corp. 2010], [Barford and Yegneswaran 2007], [Naraine 2010], [Telegraph Media Group Limited 2010], [Agence France-Presse 2010],[Poulsen 2010],[Single 2010].

2.3 What do malware cost the world?

The cost of malware regarding damage plus security and safety investments are enormous. The latest botnet in media; Zeus was estimated to attempted loss on $220 million, but actual cost was *only* $70 millions. Many security companies do not draw a nice picture regarding future situations with advanced malware running wild and/or malware in the hands of criminals
[Federal Bureau of Investigation, U.S. 2010].

3. BOTNETS

Bots differs from other malware by their communication with the botmaster and/or other bots. The botmaster is one or more cyber criminals that have access to control the actual bots. A botnets is a network of zombies (computers infected with malware, bots) that are controlled by one or more botmasters. The botmaster

can send command and control messages to the bot; that is - controlling the malware.Bots are simply a "puppet in a string" controlled by the botmaster. Bots are often a large and complex malware that are a mixture of many other kind of malware. They can often be polymorphic - that is; they can change/"morph" their behaviour and/or signature on order from bot master. Botnets have been observed to be very large. One large botnet was *Mariposa* [Thompson 2010]. The botnet *Mariposa* was estimated to be infected on 12+ millions computers [ZDNet 2010].

An other name for botmaster are botherder. The botmaster can be looked on as a herd that directs/controls his/hers flock of bots in his belonging botnets. The botmaster is normally only one piece of a network of cyber criminals that can span all over the world. The cyber criminals sells evil services to each other and are in many ways very powerful in their organisations similar to terrorist organisations. These cyber terrorists participants communicate with each other perhaps only by anonymous channels (anonymous for each other and everyone else). The way they are organized makes them more difficult to track down and perhaps shutdown their services. The latter is in many ways difficult because of many nations lack of laws regarding computer crime and weak worldwide agreement to exchange information fast enough.

Source: Microsoft Malware Protection Centre [Microsoft Corp. 2010].

3.1 Botnets in action

Botnets is involved in many hacker attacks all over the world. With a large amount of zombies the botmaster can do evil business against other system, send emails and/or just collect sensitive information. Here is a unranked list of some of the most common activities a bot participate in:

—Distributed Denial-of-Service Attacks (DDoS)

—Sending unsolicited emails (spam)

—Infect webpages with SPAM

—Sniffing traffic (for sensitive data it can send it's bot master)

—Keylogging (to collect passwords etc.)

—Spreading new malware (to increase the number of bots)

—Installing Advertisement Addons and Browser Helper Objects (BHOs) (to redirect web browser sessions)

—Google AdSense abuse (makes the "click on the ad" number grow artificial and earn extra money)

—Attacking IRC Chat Networks (performing DDoS similar attacks to IRC networks)

—Manipulating online polls/games (manipulating polls/games to please the bot master)

—Mass identity theft (capture authenticating data and bank accounts etc.)

—Attack industrial systems (bring down industrial computers (PLC's))

Sources: [Honeynet Project 2008b] [Schluting 2008].

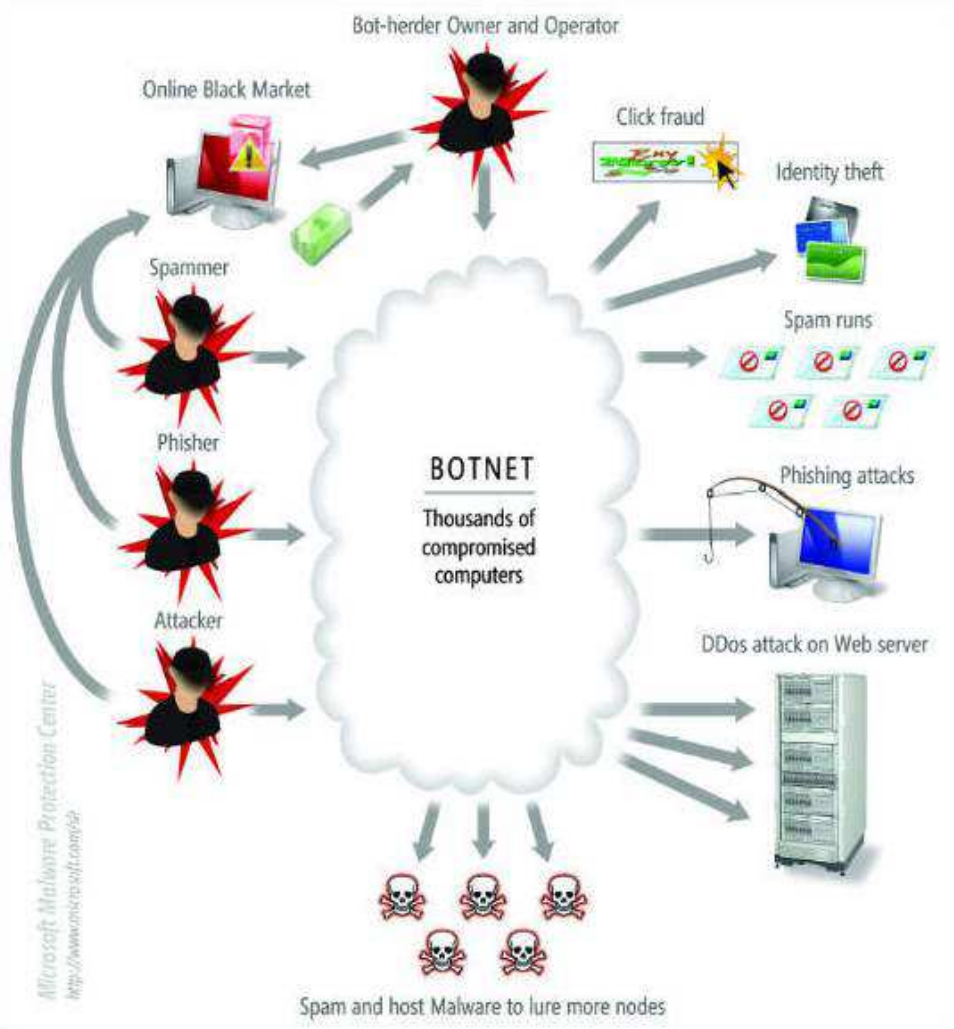

Fig. 2. Illustration of botnet activity.

3.2 Botnet Control and Command Mechanism (C&C)

The bots or zombies (computers infected with bot malware) differs from other malware in the way that they are controlled by a botmaster. Botnets can have rather complex command and control language (C&C) and protocols to communicate. The command and control mechanisms showed in table I are all related to IRC (Internet Relay Chat). This is findings done by Paul Barford and Vinod Yegneswaran in 2007 [Barford and Yegneswaran 2007]. It is findings from the complex botnet `Agebot`. This botnet was found in October, 2002. At the time it is very sophisticated and was said to be well-written in C/C++ programming language. It contained over 20.000 lines of code and had built-in high level of components/functions:

—A IRC based C&C function

—A large collection of known exploits
—The ability to launch different DoS attacks
—A shell with some polymorphic obfuscation functions
—Advanced functions in password detection, info. harvesting, packet sniffing, key logging and registry search
—Defend mechanism against typical antiviruses
—Test mechanisms for detecting debugging, process sniffers and reverse engineering tools signatures.

This is a very good example on how sophisticated and complex the bots really are. And now we face 8 years of development in malware after this first version of `Agobot`.

Command	**Description**
bot.about	Displays information (e.g., version) about the bot code
bot.die	Terminates the bot
bot.dns	Resolves IP/hostname via DNS
bot.execute	Makes the bot execute a specific .exe
bot.id	Displays the ID of the current bot code
bot.nick	Changes the nickname of the bot
bot.open	Opens a specified file
bot.remove	Removes the bot from the host
bot.removeallbut	Removes the bot if ID does not match
bot.rndnick	Makes the bot generate a new random nickname
bot.status	Echo bot status information
bot.sysinfo	Echo the bot's system information
bot.longuptime	If uptime >7 days then bot will respond
bot.highspeed	If speed >5000 then bot will respond
bot.quit	Quits the bot
bot.flushdns	Flushes the bot's DNS cache
bot.secure	Delete specified shares and disable DCOM
bot.unsecure	Enable specified shares and enables DCOM
bot.command	Executes a specified command with system()

Table I. Partial command language that the `Agobot` botnet uses.

Sources: [Barford and Yegneswaran 2007]

3.3 Bots survival mechanisms

Bots are complex malware that can hide quite well in their zombie (infected computer) with the use of built-in defence mechanisms. The smartest one trigges an action if they are threatened: They either go to sleep mode (hibernate), they terminate themself or finally, they attack the threat [Mukamurenzi 2008].

3.3.1 *Bots obfuscation mechanism.* Here are examples of mechanism that makes bots hard to detect/find:

—Polymorphism (bots can change their pattern/ID/signature)
—Authentication, authorization, encryption.
—Use common used communication channels (SSH, HTTP, HTTPS)

—Change/flux between commonly used protocols during control communication.
—IPv6 tunneling

3.3.2 *Bots deception and anti-forensics mechanism.* Bots are good in hiding itself by advanced stealth functions.

—Disable the antivirus and fake this itself
—Alter/poison the DNS cache so typical antivirus only update from `localhost`
—Test for VMware environment to hide its patterns/behaviour (if so - shot down)
—Test for debug/reverse engineering tools (if so - shot down)
—Inject itself into common used applications and change it's signature
—Slow down the activity
—Enter sleep mode /hibernate)
—Attack mechanism
—Stealth functions like hiding itself in unused partitions

Sources: [Barford and Yegneswaran 2007], [Mukamurenzi 2008], [Zhang et al. 2009].

3.4 Botnets - next generations

Trends shows that new generations of botnets will probably use more peer-to-peer communication. This smart mechanism minimise the need of a frequent dialogue between the botmaster and the bots. This new peer-to-peer botnets talk to each other and gives the botmasters recent order further to all next bots. In this way the botnet's botmaster/mothership is far more difficult to track down, and the botnets are even more reliable with high resilience.

4. FAST-FLUX

4.1 Background

4.1.1 *Round-Robin DNS.* Round-robin DNS (RRDNS) is a configuration in DNS that makes multiple servers answer one domain. This is a important functions on busy websites that makes typical management and load balancing possible with hopefully 100% uptime for online services. The demand of service from several customers need the redundancy and speed that several webservers can deliveres. In DNS this looks like table II, with a list of *A records* in DNS configuration.

In my example below i used a busy domain just for the illustration, and in the lack of fantacy I ended up using `ebay.com`. Figure II and figure III show the `ANSWER` part of the output using the DNS Lookup command *dig* (a part of the BIND software family from ICS [Internet Systems Consortium, Inc. 2010]).
A closer look on the two DNS Lookup results we see that the IP addresses most right i the tables changes its position the second time the command are executed. This is because of the Round-robin DNS function. It directs us to another server as intended the second time we ask for services. In the `ANSWER` section in figure II and III the second column shows the `TTL Record` (Time To Live) record. The value is in seconds, and typical value here are between 1800 to 3600 seconds. This is actual (what we now have guessed) the time the DNS information are set to "live" on a

client, that is; time to be valid.

```
;; ANSWER SECTION:
ebay.com.               3598    IN      A       66.135.205.13
ebay.com.               3598    IN      A       66.135.205.14
ebay.com.               3598    IN      A       66.211.160.87
ebay.com.               3598    IN      A       66.211.160.88
```

Table II. Output from `dig` command on `ebay.com`, first round.

```
;; ANSWER SECTION:
ebay.com.               3597    IN      A       66.211.160.88
ebay.com.               3597    IN      A       66.135.205.13
ebay.com.               3597    IN      A       66.135.205.14
ebay.com.               3597    IN      A       66.211.160.87
```

Table III. Output from `dig` command on `ebay.com`, second time.

4.1.2 *Content Distributing Network.* As RRDNS, Content Distributing Networks (CDNs) also uses DNS as an important mechanism in delivery of their services [Brussee et al. 2001]. The domain (typical newspapers webpage) of a CDN customers get content delivered from the CDNs site and then by the use of the CDNs nameservers (DNS). With sophisticated techniques the CDN computes the nearest (in terms of bandwidth and network topology) *edge servers* that can deliver fast and efficient with hopefully local content to the end user.

Figure IV shows the `ANSWER` section from the DNS Loockup tool `dig`
command on `images.apple.com`. The CNAME (*canonical name*) is an alias for the A record. We see that the domain `images.apple.com` use Akamai as their CDN. We see again multiple IP adresses regarding the `A record` which belongs to Akamai. Compared with the previously shown output of the `dig` command we here have significantly lower TTL. This low TTL makes Akamai (the CDN) the possibility to change the content for the clients very fast. This kind of tuning DNS is very much used on webpages all over the world. As long as there exists a commercial content blinking on the webpage we have a delivery of content within that domain name
[Holz et al. 2008].

```
;; ANSWER SECTION:
images.apple.com.       1859 IN CNAME  images.apple.com.edgesuite.net.images.
                                                          apple.com.edgesuite.net.
                       12004 IN CNAME  images.apple.com.edgesuite.net.
                                                           globalredir.akadns.net.
images.apple.com.edgesuite.net.globalredir.akadns.net.
                        1859 IN CNAME  a199.gi3.akamai.net.
a199.gi3.akamai.net.      20 IN A      195.18.221.171
a199.gi3.akamai.net.      20 IN A      195.18.221.185
```

Table IV. Output from `dig` command on `images.apple.com`.

4.2 Fast-Flux Service Networks

Round-robin DNS (RRDNS) and Content Distributing Network (CDN) are both part of the basic DNS mechanism that focus more on functions like flexibility, speed and redundancy/availability. In basic DNS's core derives from RFC's from 1982 (RFC-805) [ZoneEdit, LLC. 2010] [Stewart 2007]. By using their bots the cyber criminals redirect our HTTP session (typical) to their own evil webservers. The professional botmasters/botnets websites are often very close to legal/benign business in first look, and it is unfortunately easy to be a victim of a scam/fraud in this way.
This redirecting is done by so-called flux-agents. A flux-agent is a bot zombie (a compromised/malware infected computer) that works as a proxy in front of the botnets services. The flux-agent is controlled by the botmaster(s). When a client connects to a flux-agent, the session are redirected to the backend of the botmasters servers: the mothership and its web and DNS servers.
By using low `TTL counters` on DNS servers that hosts the domain used - the cyber criminals can change/flux their corresponding IP addresses continually. This technique is called Fast-flux, and when used in botnets we normally call it Fast-flux Service Network (FFSN).
Fast-flux is the name of the technique used to cycle the mappings of domain names to IP addresses of hosts participating in a botnet. The name Fast-flux derived from fast changing/fluxing) of IP addresses representing domain names. They use small times in the DNSs TTL parameter and fluxes the domain names vs. IP addresses fast. The bots simply redirect the clients connections to so-called flux-agents (or endpoints). These flux-agents then relay the connection to the botnets backend webservers (often called *mothership*). With fast changing IP addresses the bots process is much harder to stop/block. The facts that Fast-flux botnets may contain hundreds of thousands of flux-agents makes of course the hunting situation a nightmare. Large botnets using Fast-flux technique are often called Fast-flux Service Network (FFSN).
Sources: [Holz et al. 2008]

4.3 Fast-flux taxonomy

4.3.1 *Basic or Single Fast-flux.* The Fast-flux technique described in chapter 4.2 is normally called *Basic Fast-flux* or *Single Fast-flux*.

4.3.2 *Double Fast-flux.* A further development in Fast-flux are fluxing the DNS servers in addition to the fluxing of the IP-addresses to the flux-agents. This is called *Double Fast-flux*. See figure 3. See figure 3 for a better understanding of how the sessions/traffic flows. Source of figure: [Honeynet Project 2008a].

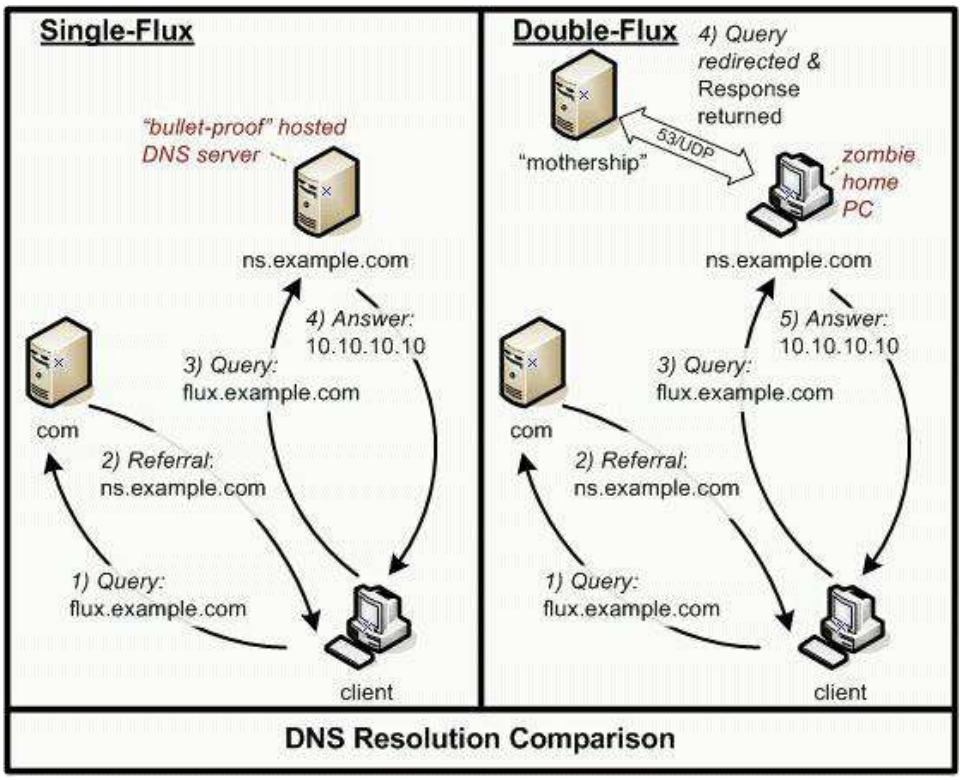

Fig. 3. Traffic flow on Single Fast-flux and Double Fast-flux

4.3.3 *Domain Fast-flux.* A further development of Fast-flux technique is fluxing the *Domain name*. This is called *Domain Fast-Flux*.

4.4 Fast-Fluxing Example

To help You understand how Fast-flux techniques works I have used an example found in the article *Detection and Mitigation of Fast-Flux Service Network* by Thorsten Holz et.al. [Holz et al. 2008].
The domain name `thearmynext.info` was found in several spam emails in July 2007. The DNS Loockup result using `dig` are shown in table V.

```
;; ANSWER SECTION:
thearmynext.info.       600     IN      A       69.183.26.53
thearmynext.info.       600     IN      A       76.205.234.131
thearmynext.info.       600     IN      A       85.177.96.105
thearmynext.info.       600     IN      A       217.129.178.138
thearmynext.info.       600     IN      A       24.98.252.230
```

Table V. Output from `dig` command on `thearmynext.info`, first round.

After the TTL timeout (given i the 2. column) we repeated the DNS Lookup tool `dig`. Table VI show the new results.

```
;; ANSWER SECTION:
thearmynext.info.       600     IN      A       213.47.148.82
thearmynext.info.       600     IN      A       213.91.251.16
thearmynext.info.       600     IN      A       69.183.207.99
thearmynext.info.       600     IN      A       91.148.168.92
thearmynext.info.       600     IN      A       195.38.60.79
```

Table VI. Output from `dig` command on `thearmynext.info`, second round.

Note that there are several *A records* similar to Round-robin DNS (RRDNS) described in section 4.1.1.
The observations are as follows:

—The TTL column are much lower then average (from 1800 to 3600(default)).

—The DNS servers gave us no repeating IP addresses that where answered the second time we executed DNS Lookup by using `dig`. This is a typical DNS answer for botnets using Fast-flux Service Networks.

—The IP addresses belongs to different networks ranges.

After using reverse DNS lookup [2] the results showed that the IP networks was used in the following countries: United States, Germany and Portugal. This should bring us on the alert! Further examination showed that the client with the actual IP addresses we got from DNS Lookup's `dig` was so-called flux-agents.

[2]Reverse DNS Lookup means using IP addresses in the `dig` command to show there exists a belonging domain name.

A flux-agent is a bot/zombie computer that works as a *"relay agent/proxy"* for the botmasters evil webservers. In figure 4 we have illustrated the normal HTTP session.

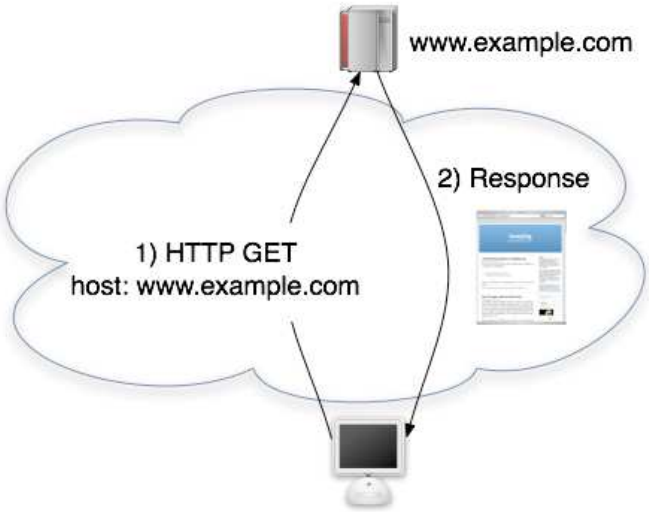

Fig. 4. Content retrieval process from good/benign HTTP site

The figure 5 shows how we are redirected by the flux-agent so we end up being scammed/fraud by the cyber criminals.

Please note that the DNS server should be in the figures 4 and 5. Initial in this scam/fraud we get answer from DNS servers controlled by the botmasters (or a corrupt/compromised DNS server).

4.5 Fast-flux resilience

Botnets have a weak point, an Achilles heel: The command and control communication channel. This is why botnets tend to use fast-fluxing as a baseline for the communication channel. They are dependent of having control of their their botnets. There are a lot of other cyber criminals that will take over the flock of bots if they are left alone for a while. This is why they build complex DNS systems to always have their communication channel ready. There are 3 main categories of Fast-flux models. See table VII.

Type	**Description**	**Resilience**
Basic fast-flux hosting	IP addresses of the botnets websites are fluxed	Low
Name Server (DNS) fluxing	IP addresses of the DNS servers are fluxed	Medium
Double fast-flux	Both IP addresses of the DNS servers and web sites are fluxed	High

Table VII. Fast-flux taxonomy

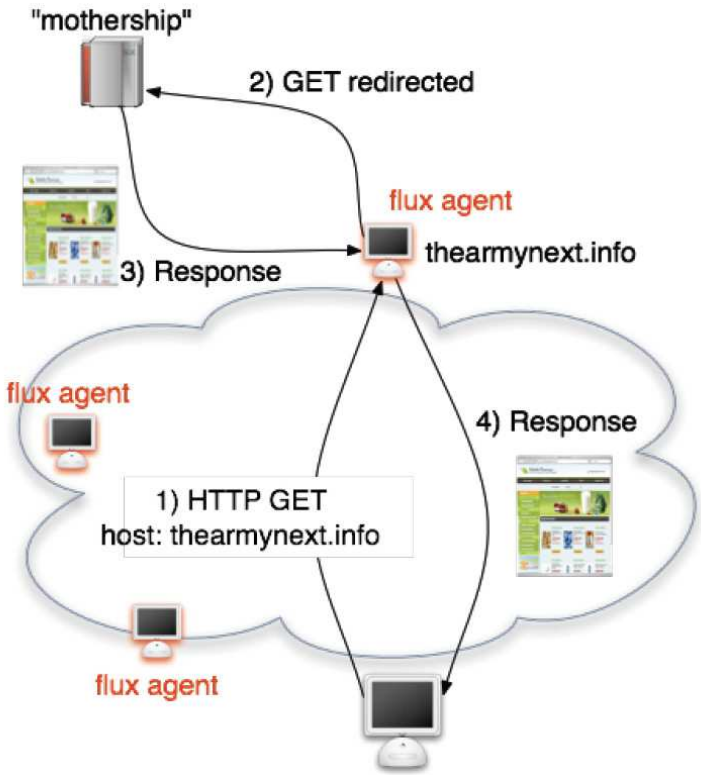

Fig. 5. Content retrieval process when flux-agents redirects You

Source: [Ollmann 2009] [Barford and Yegneswaran 2007]

4.6 Fsst-flux statistics

I found some real-time statistics regarding Fast-flux botnets on the *ATLAS Portal* [Arbor Networks, Inc. 2010]. The text below are quoted from their webpage:

> Currently monitoring 5 active fastflux domains. The average duration across the 66319 domains ever tracked is 1 week. The longest duration of any domain is 92 weeks.
> This information was obtained from Arbor Networks' ATLAS Initiative on (December 14, 2010) and permission to republish has been obtained. ATLAS initiative data is dynamic and therefore, the information may have changed since the date of publication of the data. ©Arbor Networks, Inc. ALL RIGHTS RESERVED. Atlas is a trademark of Arbor Networks, Inc

The figures 6 and 7 are showing "printscreen" of Fast-flux statistics from ATLAS captured 2010-12-14 ECT:16:29
[Arbor Networks, Inc. 2010]. An interesting point here are the large role U.S.A have regarding hosts, and that a botnet domain had survived 92 weeks.

NEWEST DOMAINS

Domain	Created
ashampoo-15.com	2010-12-13 11:59:40 EST
ashampoo-18.com	2010-12-13 11:59:39 EST
ashampoo-19.com	2010-12-13 02:59:12 EST
sgtewkhk.biz	2010-12-09 10:46:08 EST
jjwextxf.com	2010-12-08 09:43:33 EST
popgoestheweek.com	2010-11-29 16:06:13 EST
groovenotes.org	2010-11-29 16:06:11 EST
solobanjo.com	2010-11-29 16:06:09 EST
dwellingwithgod.com	2010-11-29 16:06:07 EST
bensimonds.com	2010-11-29 16:06:03 EST

LONGEST LIVED ACTIVE DOMAINS

Domain	Started	Duration
ashampoo-12.com	2010-10-15	8 weeks 2 days
jjwextxf.com	2010-12-08	< 1 minute
ashampoo-19.com	2010-12-13	< 1 minute
ashampoo-18.com	2010-12-13	< 1 minute
ashampoo-15.com	2010-12-13	< 1 minute

DISTINCT NETWORKS (past 24 hours)

Number of hosts	Domains
23	ashampoo-12.com, ashampoo-15.com, ashampoo-18.com, ashampoo-19.com

Fig. 6. ATLAS Fast-flux statistics - Domains

SERVERS (past 24 hours)
BY COUNTRY

Country	Number of hosts	Percentage
US (United States)	2320	55.9%
ES (Spain)	304	7.3%
FR (France)	269	6.5%
CA (Canada)	153	3.7%
IT (Italy)	135	3.3%
GB (Great Britain)	118	2.8%
DE (Germany)	99	2.4%
AR (Argentina)	56	1.3%
PL (Poland)	54	1.3%
CL (Chile)	43	1.0%
Other	599	14.4%

BY ASN

ASN	Number of hosts	Percentage
AS12322 (PROXAD)	237	5.8%
AS20115 (Unknown)	158	3.9%
AS6739 (ONO-AS)	147	3.6%
AS7132 (SBIS-AS)	119	2.9%
AS7922 (COMCAST-7922)	117	2.9%
AS5089 (NTL)	116	2.9%
AS33491 (COMCAST-33491)	104	2.6%
AS7015 (Unknown)	96	2.4%
AS7725 (COMCAST-7725)	95	2.3%
AS33651 (CMCS)	90	2.2%
Other	2781	68.5%

Fig. 7. ATLAS Fast-flux statistics: Country and ASN.

5. TRENDS FOR 2011

I have here listed unsorted trends/predictions from different sources. It is a common understanding in computer security business that we are expecting to see worse situations in the future (as paranoid we are). Symantec predicted a stormful malware year 2010, and we can all agree on that when we look back [Vicario 2009].

—Commercial malware builders/programmers will continue to work for both the legal and the illegal group of customers. It is the same as the industry building military weapons; *"we are just building the tools"*.

—SPAM emails will become culturally and linguistically diverse. The amount of SPAM emails in English will fall from today's 95% down under 90%. The content will also be more geographically reflected.

—An organisations or company's reputation will be a more definitive factor in why they are attacked/targeted from cyber criminals. The hackers will use the IP and DNS systems reputation mechanism to focus on the easiest targets.

—The cyber war will continue to the next level. Botnet detecting and abnormal network traffic detecting systems will need to take a faster grip on Internet traffic.

—Malware authors will increase the use of existing social networks etc. for the botnets communication channel. Social networks used so far are e.g. `Twitter.com`, micro-blogging sites and free network storage sites.

—Redundant/resilience in botnets will increase. The bots will be more sophisticated in hiding itself in zombie (the infected computer).

—Compromised systems/part of botnets will be more frequent sold/exchanged in cyber criminal organisations.

—Cyber criminals will cooperate more in developing better malware/botnets etc.

—We will face more exploits using URL Shortening Services. This is a way to hide the server origin destination.

—We will face more narrowed attacks similar to Stuxnet [Symantec Corp. 2010] against industrial business.

—Many nations worldwide are spending a lot of money in arming and educate their government cyber police force. This kind of activity will rise after the challenging 2010.

Sources: [Ollmann 2010] [Lewis 2010b] [Lewis 2010a] [Lewis 2010c] [ESET 2010]

6. ACKNOWLEDGEMENT

Thanks to my employee Austevoll Kraftlag BA for giving me the opportunity to study for master in information security. Thanks to Gjøvik University College for letting me use their subversion serves as common repository for my documents. Thanks to my families and especially my Kari for their/her patients with me now two weeks before Christmas.

7. CONCLUSION

In this paper i have covered malware in general including some historical facts. I have covered botnets in general and botnets Fast-Flux Service Network in details

with an example from the real world. Finally I listed up some trends that are expected to happend in 2011.
Computer malware is a enormous subject. Even the frightening amount of malware discovered every day (60.000 each 24 hour regarding McAfee Inc.
[McAfee, Inc. 2010]) we must not start running hiding and be scared.
I think we have to change the way we use Internet compared to today's situation. Many of us just enjoy *"The Net"* and its fascination services and offers for free. Our private households may not be the first victim of this change - but all companies/organisations/government offices may really change their approach to the Internet. I think we as a baseline will face two main security zones in each office of either category (companies/organisations/government offices etc.). One zone for the administration of the offices basic needs (internal emails, documents, financial applications etc.) that have several security layers between them and Internet (e.g. traffic washing (IDS/sandbox/anti-malware-functions)). The other zone will have a sloppier security layer. The latter zone will be for information gathering, application testing, social networking etc.
But despite the frightening development of malware and especially botnets we must stick together worldwide and sharpen our weapons in this battle. Nations worldwide spend a lot of money on computer security after latest years experience. Nations laws and legislations must be changed/tuned (or just used!) to stop cyber criminals. We must use a more sophisticated security software then good old antivirus on our computers. Fortunately, mechanisms for detecting unwanted software and/or unwanted network behaviour are getting better every day. We will need to cooperate much more over the nations borders and exchange information to win this ongoing cyber war. Finally, we must all remember that mankind are not evil by nature, and computer software are made by us humans.
My conclusion is all of us play a role in this cyber war against cyber criminals with their complex malware. Botnets are dangerous malware either they use Fast-flux mechanism or not, but they can be beaten. By more cooperation nation- and worldwide we can reduce the power and impact that these serious botnet attacks have had so far.

REFERENCES

Agence France-Presse. 2010. New cyber attack linked to nobel peace prize. URL. http://www.abs-cbnnews.com/lifestyle/gadgets-and-tech/11/11/10/new-cyber-attack-linked-nobel-peace-prize.

Arbor Networks, Inc. 2010. Summary report, global fast flux. URL. http://atlas.arbor.net/summary/fastflux.

Barford, P. and Yegneswaran, V. 2007. An inside look at botnets. In *Malware Detection*, M. Christodorescu, S. Jha, D. Maughan, D. Song, and C. Wang, Eds. Advances in Information Security, vol. 27. Springer US, 171–191. http://dx.doi.org/10.1007/978-0-387-44599-1_8.

Bishop, M. 2003. *Computer Security: Art and Science*. Addison Wesley Professional.

Brussee, R., Eertink, H., Huijsen, W., Hulsebosch, B., Rougoor, M., Teeuw, W., Wibbels, M., and Zandbelt, H. 2001. Content distribution networks, state of the art. URL. Date : June 1, 2001 Version : 1.0 Change : Project reference: CDN2 TI reference : TI-RS-2001xx https://doc.novay.nl/dsweb/Get/Document-15534.

ESET. 2010. Global threat report. URL. http://www.eset.com/resources/threat-trends/Global_Threat_Trends_October_2010.pdf.

Famento Inc. 2008. History of computer viruses. URL. http://www.xtimeline.com/timeline/History-of-Computer-Viruses.

Federal Bureau of Investigation, U.S. 2010. Cyber banking fraud. URL. http://www.fbi.gov/news/stories/2010/october/cyber-banking-fraud.

Fisher, D. 2010. Rethinking stuxnet. URL. http://threatpost.com/en_us/blogs/rethinking-stuxnet-100410.

Gollmann, D. 1999. *Computer security*. John Wiley & Sons, Inc., New York, NY, USA.

Holz, T., Gorecki, C., Rieck, K., and Freiling, F., Eds. 2008. *Detection and Mitigation of Fast-Flux Service Networks*. http://www.isoc.org/isoc/conferences/ndss/08/.

Honeynet Project. 2008a. Fast flux dns diagram. URL. http://www.honeynet.org/node/135.

Honeynet Project. 2008b. Know your enemy: Tracking botnets. URL. http://www.honeynet.org/papers/bots.

Information Please. 2007. Computer virus timeline. URL. Information Please® Database, © 2007 Pearson Education, Inc. http://www.infoplease.com/ipa/A0872842.html.

Internet Systems Consortium, Inc. 2010. Bind software. URL.

Krebs, B. 2003. A short history of computer viruses and attacks. URL. http://www.washingtonpost.com/ac2/wp-dyn/A50636-2002Jun26.

Lewis, D. 2010a. 2011 trends: Cybercriminals usurp url shortening services. URL. http://www.symantec.com/connect/blogs/2011-trends-cybercriminals-usurp-url-shortening-services.

Lewis, D. 2010b. 2011 trends: Global spam. URL. http://www.symantec.com/connect/blogs/2011-trends-global-spam.

Lewis, D. 2010c. 2011 trends: Targeted attacks diversify. URL. http://www.symantec.com/connect/blogs/2011-trends-targeted-attacks-diversify.

McAfee, Inc. 2010. Mcafee threats report: Third quarter 2010. Threat report, McAfee, Inc., McAfee, Inc. Headquarters 2821 Mission College Blvd. Santa Clara, CA 95054 USA. Dec. http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2010.pdf.

Microsoft Corp. 2010. Illustration of a botnets activity. URL.

Mukamurenzi, N. M. 2008. Mastersthesis, Norwegian University of Science and Technology, Norwegian University of Science and Technology, Department of TelematicsGamle Fysikk, Sem Sælands vei 5, 7034 Trondheim. http://daim.idi.ntnu.no/masteroppgaver/IME/ITEM/2007/3795/masteroppgave.pdf.

Naraine, R. 2010. Firefox zero-day under attack at nobel peace prize site. URL. http://www.zdnet.com/blog/security/firefox-zero-day-under-attack-at-nobel-peace-prize-site/7550.

Ollmann, G. 2009. Botnet communication topologies, understanding the intricacies of botnet command-and-control. Tech. rep., Damballa, Inc.

Ollmann, G. 2010. 2011 threat predictions. URL. http://blog.damballa.com/?p=1049.

Panda Security,S.L. 2009. Annual report pandalabs 2009. URL.

Paquette, J. 2001. A history of viruses. URL. http://www.symantec.com/connect/articles/history-viruses.

Poulsen, K. 2010. Cyberattack against wikileaks was weak. URL. http://www.wired.com/threatlevel/2010/11/wikileaks-attack/.

Schluting, C. 2008. All about botnets. URL. http://reslife.saf.uwplatt.edu/resnet/files/BotNets.pdf.

Single, R. 2010. Joining pro-wikileaks attacks is as easy as clicking a button. URL. http://www.wired.com/threatlevel/2010/12/web20-attack-anonymous/.

Stewart, W. 2007. Domain name system (dns) history. URL. http://www.livinginternet.com/i/iw_dns_history.htm.

Symantec Corp. 2010. W32.stuxnet dossier. URL. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Telegraph Media Group Limited. 2010. Wikileaks hackers threaten british government. URL. http://www.telegraph.co.uk/news/worldnews/wikileaks/8193210/WikiLeaks-hackers-threaten-British-Government.html.

Thompson, M. 2010. Mariposa botnet analysis. URL. http://defintel.com/docs/Mariposa_Analysis.pdf.

Vicario, M. 2009. The worst is yet to come, symantecs 2010 security predictions. URL. http://www.symantec.com/connect/blogs/worst-yet-come-symantec-s-2010-security-predictions.

Wolthusen, S. 2010. Lecture notes. applied information security. fall 2010. Lecture Notes. Applied Information Security. Fall 2010. Gjøvik University College, Norway.

ZDNet. 2010. Police arrest mariposa botnet masters, 12m+ hosts compromised. URL. http://www.zdnet.com/blog/security/police-arrest-mariposa-botnet-masters-12m-hosts-compromised/5587.

Zhang, Z., Ando, R., and Kadobayashi, Y. 2009. Hardening botnet by a rational botmaster. In *Information Security and Cryptology*, M. Yung, P. Liu, and D. Lin, Eds. Lecture Notes in Computer Science, vol. 5487. Springer Berlin / Heidelberg, 348–369. 10.1007/978-3-642-01440-6_27, http://dx.doi.org/10.1007/978-3-642-01440-6_27.

ZoneEdit, LLC. 2010. Dns related rfcs. URL. http://www.zoneedit.com/doc/rfc/.

8. APPENDIX

A. APPENDIX - DEFINITIONS

Keyword	Description
`Bot`	A bot is a malware that can be controlled by the botmaster (short for "software robot").
`Botherder`	A botherder is another word for botmaster.
`Botnets`	Botnets are a network or networks of many bots.
`Botmaster`	A botmaster is the master of a botnet. He/she controls a botnet.
`Computer Worm`	Code that copies/replicates itself from one computer to another over the network.
`Computer Virus`	Code that inserts itself into one or more (executable) files and typically performs a malicious function.
`Macro virus`	A virus that uses local command interpretors to execute its included macro code.
`Malicious logic`	A malware with set of instructions that cause a site's security policy to be violated.
`Malware`	Short for malicious software.
`Mothership`	A common description of the main server(s) in a botnet.
`Polymorphic virus`	A virus that can change its form and signature when it infects binary programs.
`Rootkit`	A rootkit is a set of malicious tools that inserted by an adversary into a target system so as to conceal the presence of modifications performed by the adversary and to permit the adversary to take control over the compromised system.
`Trojan Horse`	A malware with program code with an overt (documented or known) effect and a *covert* (undocumented or unexpected) effect.
`Worm`	The same as Computer Worm (see above).
`Virus`	The same as Computer Virus (see above).
`Zombie`	A zombie is a infected/compromised computer.

Table VIII. Definitions

Sources: [Bishop 2003], [Wolthusen 2010], [Gollmann 1999]

B. APPENDIX - MALWARE TIMELINE

Year	Description
1949	Hungarian scientist John von Neumann (1903-1957) devises the theory of self-replicating programs, providing the theoretical foundation for computers that hold information in their "memory."
1971	The Creeper virus, an experimental self-replicating program, is written by Bob Thomas at BBN Technologies.[2] Creeper infected DEC PDP-10 computers running the TENEX operating system. Creeper gained access via the ARPANET and copied itself to the remote system where the message, "I'm the creeper, catch me if you can!" was displayed.
1881	A program called Elk Cloner, written for Apple II systems and created by Richard Skrenta. Elk Cloner's design combined with public ignorance about what malware was and how to protect against it led to Elk Cloner being responsible for the first large-scale computer virus outbreak in history
1986	The first virus on the most common microcomputer in the world; the IBM PC. Basit Farooq Alvi and Amjad Farooq Alvi were running a computer store in Lahore, Pakistan. The name of their store was Brain Computer Services.
1988	The first worm that was spread in large scale. Twenty-three-year-old programmer Robert Morris unleashes a worm that invades ARPANET computers. The small program disables roughly 6,000 computers on the network by flooding their memory banks with copies of itself.
1992	1300 viruses are in existence, an increase of 420% from December of 1990. The Dark Avenger Mutation Engine (DAME) is created. It is a toolkit that turns ordinary viruses into polymorphic viruses. It is the first actual virus creation kit.
1996	Baza, Laroux (a macro virus), and Staog viruses are the first to infect Windows95 files, Excel, and Linux respectively.
1999	A macro-virus author turned his attention to the use of e-mail as a distribution mechanism. Melissa, the first infamous global virus, was born.
1999	Sub7 and Pretty Park (a Trojan and a worm) are seen as malware that helped initiate the rise of the botnet. Since they were born, hackers began to get really creative.

Table IX. Malware timeline

Source: Sources: [Information Please 2007] [Famento Inc. 2008] [Krebs 2003] [Panda Security,S.L. 2009] [Paquette 2001] [Symantec Corp. 2010]