History of malware

Nikola Milošević

inspiratron.org

Abstract

In past three decades almost everything has changed in the field of malware and malware analysis. From malware created as proof of some security concept and malware created for financial gain to malware created to sabotage infrastructure. In this work we will focus on history and evolution of malware and describe most important malwares.

1. Introduction

Malware, short for **malicious** (or malevolent) **software**, is software used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software. Malware includes computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs and other malicious programs; the majority of active malware threats are usually worms or trojans rather than viruses [1].

History of malware can be split to several categories that will also represent timeframe in which events from that category happened. So we will split history of malware in 5 categories. First category is early phase of malware. This is time when first malwares come to life. Second phase is early Windows phase. It will describe first Windows malwares, first mail worms and macro worms. Third part is evolution of network worms. These threats become popular when internet becomes wide spread.

Forth part is rootkits and ransomwares. These were the most dangerous malware before 2010. Then came malware that was made for virtual espionage and sabotage. This malwares were created by secret services of some countries. This is the last phase of malware evolution that we are now facing.

In this work we will describe malware evolution in these five phases. Also in this work we will not describe all malware, but just malware that were great game changers, and was most famous by introduced new things in malware world.

2. Beginnings of malware

There were some malware for other platforms before 1986., but in 1986. appeared first malware for PC. It was virus called Brain.A. Brain.A was developed in Pakistan, by two brothers - Basit and Amjad. They wanted to prove that PC is not secure platform, so they created virus that was replicating using floppy disks. It infected booting sector of floppy drive and booting sector of every inserted floppy disk. So anytime infected floppy would be inserted into PC, it would infect it's drive, so the drive would infected again every disk inserted.

This virus did no harm, and authors were signed in code, with phone numbers and address [2]. Intention of early malware writers was to point on problems, rather than make some harm or damage. But later of course malware become more and more destructive.

After Brain there were other viruses. One of the interesting is **Omega** virus. It was called Omega because of omega sign that it was writing in some conditions in console. It was infecting boot sector, but was not doing much damage unless it was Friday 13th. On that day PC could not boot. **Michelangelo** virus would on Michelangelo's birthday in year 1992 rewrite first 100 sectors of hard disk[3]. Doing this, file allocation table would be destroyed and PC could not boot. **V-sign** is virus that also infected boot sector and wrote V sign on screen every month. **Walker** is next virus that was quite visual and appeared in 1992. It was animating walker walking from one side of screen to the other. **Ambulance** virus was quite similar to Walker, animating ambulance car driving from one side of screen to the other, but it also added sound effects of ambulance car. One of the most interesting virus from the beginning of 1990' was **Casino virus**. Casino virus would copy file allocation table to memory and delete original file allocation table. Then he will offer a slot game to user. User had to get 3 £ signs if he wants to use his PC and user could try three times. If user restarts machine the file allocation table would be gone, and machine would not be able to boot. Same would happen if user loses - file allocation table would be deleted from memory as well. If user wins the game, virus would copy back file allocation table from memory, and PC could be used normally.

Next big step in malware evolution was introduction of **mutation engine (MtE)**. Mutation Engine was created by Bulgarian hacker who called himself Dark Avenger. It was tool that could add mutation functionality to viruses, so they would be harder detected by anti-viruses. Basically this was first polymorphism module that could take any virus and make it far more invisible. Until mutation engine anti-virus software were finding viruses on PCs using file signatures and changes in file signatures. Introduction of polymorphism made this method ineffective[5].

Virus creation laboratory was first UI tool for creating viruses. User could select features of virus and create it. This made virus creation easy. It has some disadvantages, but almost anyone using this GUI tool could create virus[6].

3. First windows malwares

When Windows was released it was interesting for many users since it gives powerful user interface. That simplicity of use attracted many users. Everything that has many users in computing world soon becomes interesting also for attackers and malware creators.

WinVir was first Microsoft Windows virus. It was also not doing much harm, it's main feature was that it was replicating, and that it was first virus that has ability to infect windows PE (Portable Executable) files. WinVir was doing little changes to infected files. When infected file was executed, WinVir was looking for other PE files and was infecting them. While WinVir was infecting other files original executed was rolled back to it's original state. To say it simple WinVir was deleting itself.

Monkey was virus that was infecting master boot record of hard drives and floppies. Monkey was moving first block of master boot record to third and inserting it's own code into first block. When infected computer was booted it was running normally, unless it was booted from floppy. In this case "Invalid drive specification" message was printed.

One-half or **Slovak bomber** was one interesting and might be quite destructive virus. It infected master boot record, EXE and COM files, but did not infected files that in name contained words like SCAN, CLEAN, FINDVIRU, GUARD, NOD, VSAFE, MSAV or CHKDSK. These files were not infected because they might belong to some antivirus software, so the virus might be caught by auto-checking algorithms. It was crypting parts of users hard drive using XOR function with some key known to virus. But if user tries to access some crypted file, file was decrypted and user wouldn't notice anything. The problem with this virus was, that if it was cleared inappropriately, crypted files couldn't be retrieved anymore[7]. Virus was showing message every 4th, 8th, 10th, 14th, 18th, 20th, 24th, 28th and 30th every month under particular circumstances:

Dis is one half.

Press any key to continue …

Concept (WM.Concept) was first macro virus and it was detected in 1995. It was written in Microsoft Word macro language, and it was spreading by sharing documents. It worked on PC computers and on Macintosh computers if on computer was installed Microsoft Word. When document infected with Concept was opened on some PC, virus would copy it's malicious template over master template, so every new document created on that computer would be infected[8].

Laroux (X97M/Laroux) was first Microsoft Excel macro virus. It was written in Visual Basic for Application (VBA), macro language for Office documents that was based on Visual Basic. It worked on Excel 5.x and Excel 7.x. It also could be run on Windows 3.x, Windows 95 and Windows NT. It was not making any harm, it was just replicating.

Boza was first virus that was written specifically for Windows 95. It was infecting Portable EXE files - files that were using Windows 95 and Windows NT. But it was not attacking Windows NT. So far, there was no virus detected that was written particularly for Windows NT. Virus was detected on January 1996. It had Australian origins, but it was detected all over the world. When file infected with Boza would be run, it would infect other files in that directory. One to three files would be infected on each run. After this Boza would run original program. Virus would not be active in memory anymore.

Boza virus message window

Boza was spreading quite slow, but also the spreading algorithm was fast enough that it could not be detected by user. Boza had no destructive routines, but it has one error that caused that under some circumstances infected files could

raise to several megabytes. This was problem on machines which hard disks were just few tens on megabytes large. Virus had activation routine that showed message window on every 31st of any month. Messages were: "The taste of fame just got tastier!" and "From the old school to the new".

Marburg (Win95/Marburg) is virus that started to circulate in August 1998., when it has infected master CD of MGM/EA PC game called Wargames. Publisher MGM on 12th of August 1998. released apologies to users:
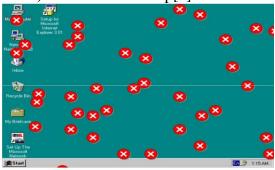
From: "K.Egan (MGM)" <kegan@mgm.com>
Subject: MGM WarGames Statement
Date: Wed, 12 Aug 1998 18:03:39 -0700

MGM Interactive recently learned that its WarGames PC game shipped with the Win32/Marburg.a virus contained in the electronic registration program. The company is working as fast as it can to resolve the problem ... MGM Interactive is committed to delivering top quality products to consumers. This is an unfortunate circumstance and we sincerely apologize for any convenience this has caused you. ... If you have any questions or if you would like to receive a replacement disc, please contact MGM Interactive.

Same virus was on CD that covered Austrian PC magazine Power Play in August 1998.

Maburg is polymorphic virus that infected Win32 and SCR (screen saver) files and encrypted it's code with polymorphic variable layer of encryption. Polymorphic engine of virus was quite advanced since it was encrypting virus with 8,16 and 32 bit keys and several different methods. Virus was using slow polymorphism, which means that it was changing it's

decryptor slowly. Maburg was deleting integrity database of several antivirus programmes. Also it was avoiding infecting files that was belonging to antivirus software and it was not infecting files containing V in name. This was done to prevent auto checking of antivirus software. Maburg was activated 3 months after infection if infected file was run at same hour as hour of infection showing standard MS Windows error icon (white cross in red circle) all over the desktop[9].

Maburg

Happy99 is first mail virus. It was spreading as attachment of e-mail as executable and was detected in 1998. At that time spam filters barely existed, and was allowing sending of executables. If user clicked and run the attachment, it would show him screen with fireworks, but also virus would replicate attachment and send mail to all user's contacts.

Melissa was virus that combined techniques of macro virus and mail virus. It was coming with attached infected MS Word file. If file was opened it would replicate to randomly chosen document from user's hard disk and send it to all contacts. This was quite problematic because of information leakage. Also virus was sometimes adding quotes from The Simpsons to infected documents[3].

LoveLetter was one of most successful social engineering virus. It was using premises of love, attracting user to open attachment. Attachment file would run

the virus. Virus was rewriting some quite important files on victim's system. Using premises of love virus convicted millions to open attachment, what caused financial damage of 5,5 billion dollars over the world. **Anakurnikova** was similar virus that was sending executable file, and convicting victims that there are sexy photos of Ana Kurnikova, sexy tennis player. Many was convinced to open file, and even when antivirus companies made detection and blocking of running malicious attachment, many asked support of companies, how they can see the pictures.

Worms

At the end of 1980's accidently was created first PC worm. In 1988. Robert Tappan Moris, who was at that time student of MIT wrote a program that will be big game change event in malware history. As part of his project Morris wanted to count computers connected to internet. So he wrote little program that would replicate from one connected computer to another and count. But Morris made a bug, the worm was also visiting computers that it has already visited before. Actually worm was replicating from infected computer to all other connected computers all the time. This generated a lot of network traffic and almost crushed internet of that time. Because of this mistake Morris was arrested and convicted by Computer Fraud and Abuse Act from 1986[10]. This was also first case that someone was convicted by this law. At that time computers had open ports and connections and replications could be done without use of exploits. In the beginning of internet no one really thought about internet security. This made easy for Morris to make his worm.

But later security mechanisms was implemented and later worms had to use exploits to gain access to computer on network.

Internet worms work in way that they have scanning algorithm that scans network. In most cases it tries public or both public and private IP addresses. IP address could be unassigned, or it can be assigned to device that could not be attacked (wrong platform) or patched and protected computer. In this cases worm would not attack. But if computer on IP address is running on right unpatched platform, worm would use exploit to gain access to that computer. After that it would add some payload, that could trigger on some time or do some bad things to system. Then it would again start scanning network and try to propagate from that computer.

Code Red is first internet worm that came after Morris worm and that did not needed any user interaction. Also Code Red is first intentionally written worm (Morris worm was malicious by accident). Code Red was spreading in year 2000., and spread over the world in couple of hours. It was successfully hiding from defending mechanisms and had several capabilities that was triggered in cycles. It was attacking IIS (Internet Information service) web servers. First 19 days it only spread over the network using vulnerability in IIS. From day 20 do day 27 it lunched denial of service attacks on couple of websites (ie. Whitehouse). Last 3-4 days of month it would just rest.

Nimda was discovered on September 18th 2001.. Nimda fast spread over the world as internet worm. If Nimda letters switch position it would be admiN. Nimda was quite similar to Code Red by scanning network and propagating, but it had additional features. Scanning

algorithm of Nimda was scanning all IP addresses while Code Red was scanning just public IP range. Because of this feature Nimda could go further infecting private networks[3]. Nimda also had ability to change hosted website, so they would offer download of infected files. This way spreading of Nimda was even faster and more dangerous, because with user interaction Nimda could overcome firewalls and spread from that private computer hosts. It could spread to Windows 95,98, Me, NT 4 and Windows 2000. Nimda had one error because of which it was under some circumstances crushing and could not spread more.

Fizzer is mail worm from 2003. This was not internet worm, but we will describe it here, because of timeframe when it was found. Fizzer was first malware which only purpose was to generate revenue and money. It came in infected attachment, and was turning infected machine in spam sender.

In this period changes the structure of malware writers. Before Fuzzer, malware was written by enthusiasts that would like to proof something or to show up. From Fuzzer main focus on malware writers is gaining profit. After Fuzzer many malware come that sent spam or that blackmailed computer users. Also malware writers were not mostly from developed countries like it was in 1980' and 1990'. Main sources of malware came on 2000' by people from third world countries, mainly Russia, China, Pakistan, India etc.

Slammer was found on September 13th 2003., and brought some new things. It was internet worm that used vulnerability in OpenSSL and it is one of first malwares that attacked Linux machines and Apache servers. It also had a backdoor, so attacker could use infected machine, upload to it some additional tools or malwares. Backdoor was creating UDP socket with attacker. Actually it was listening on UDP port 2002 for attacker's connection.

In years 2003 and 2004 was discovered 3 most destructive internet worms that have introduced consideration in security of real systems (factories, power plants, airports and other transportation systems) and virtual sabotage.

Slammer was internet worm that was spreading in 2003. using vulnerability in Microsoft SQL Server and Microsoft Data Engine 2000. Every application that used some of these two services was potential target and entrance point for Slammer. Some of applications that Slammer used to gain access to system were:

- Microsoft Biztalk Server
- Microsoft Office XP Developer Edition
- Microsoft Project
- Microsoft SharePoint Portal Server
- Microsoft Visio 2000
- Microsoft Visual FoxPro
- Microsoft Visual Studio.NET
- Microsoft .NET Framework SDK
- Compaq Insight Manager
- Crystal Reports Enterprise
- Dell OpenManage
- HP Openview Internet Services Monitor
- McAfee Centralized Virus Admin
- McAfee Epolicy Orchestrator
- Trend Micro Damage Cleanup Server
- Websense Reporter
- Veritas Backup Exec
- WebBoard Conferencing Server[11]

Slammer was spreading as an memory process. It never wrote anything on hard disk. So when PC would be restarted, infection would disappear. But since PC was connected to other PCs, from where it got infection, or where it replicated infection to, soon infection would be back. Slammer was creating great network traffic, so many packages become lost. This way it caused great damage - for example ATM network of Bank of America was down, 911 service in Seattle was down for couple of days, flight control systems on couple of airports were infected and some flight were delayed. Also there was a problem in nuclear power plant in Ohio.

Blaster was detected in August 2003. It used buffer overflow vulnerability in DCOM RPC (Distributed Component Object Model Remote Procedure Call). Blaster was used to create SYN flood to windowsupdate.com website, but since it was wrong website, real one was windowsupdate.microsoft.com, it did not caused much damage to Microsoft. But since it created traffic it did slow down and disable several systems like Air Canada planes were landed, US train company CSX stopped etc.

Sasser in 2004 used buffer overflow in Local Security Authority Subsistem Servis (LSAS). It spread over the network and it was quite often crashing LSAS service, which caused restart in one minute. When Microsoft released patch it was quite large to download and install in less time than time malware needed to crush LSAS service. This caused a lot of frustration for users, so soon new model of automatic updates was developed. Sasser caused Railcop trains to stop in Australia, Delta airlines problem and delays on British Airways flights, Hong Kong government department of energy was infected, two

hospitals in Sweden was infected and could not run scanners, EU commission was infected, Heathrow airport had problems with this malware, as well as UK Coastguard and several Banks closed their offices for couple of days because of internal infection.

5. Rootkits and ransomware

RootKits are malware tools that modify existing operating system software so that an attacker can keep access to and hide on a machine. RootKits can operate at two different levels, depending on which software they replace or alter on the target system. They could alter existing binary executables or libraries on the system. In other words, a RootKit could alter the very programs that users and administrators run (for example ls, cd, ps or other programs). We'll call such tools user-mode RootKits because they manipulate these user-level operating system elements. Alternatively, a RootKit could go for the jugular, or in our case, the centerpiece of the operating system, the kernel itself. We'll call that type of RootKit a kernel-mode RootKit [3].

First RootKit ever made was made by SONY Entertainment, and had quite bad impact on SONY's reputation. **SONY BMG RootKit** was born in year 2005, as idea of SONY to protect copyright of their publications. They had idea to detect and disable coping of their publications using this RootKit to other media. Sony BMG RootKit was part of 52 publications of Sony amongst them albums by Ricky Martin and Kelly Minogue. When CD was inserted in normal CD player or discman nothing would happen. But when CD was inserted in PC, RootKit would be installed, hide itself and all files starting with sys. Also it would control how

user accesses music. If user tries to copy RootKit would prevent it. Functionality to hide all files starting with sys used other malware writers to hide their files on system calling malware files with starting sys. When RootKit was detected, there was great scandal because Thomas Hesse, Director of global sales in Sony BMG made statement in which he said "Most people, I think, don't even know what a rootkit is, so why should they care about it?". This caused heavy public reaction and had bad impact on SONY image. This is also shown as good example of bad public relations. There was also a law suit which epilogue was that SONY offered customers refund and free music downloads from website.

StormWorm was mail worm that came 7 years after LoveLetter, and same as LoveLetter used social engineering to spread. It used fear and horror instead of love, as LoveLetter did. StormWorm start spreading using mail with subject "230 dead as storm batters Europe". Also there was other manifestations as time passes, so some of the subjects of StromWorm were:

- A killer at 11, he's free at 21 and kill again!
- U.S. Secretary of State Condoleezza Rice has kicked German Chancellor Angela Merkel
- British Muslims Genocide
- Naked teens attack home director.
- 230 dead as storm batters Europe.
- Re: Your text
- Radical Muslim drinking enemies's blood.

- Chinese/Russian missile shot down Russian/Chinese satellite/aircraft
- Saddam Husain safe and sound!
- Saddam Hussein alive!
- Venezuelan leader: "Let's the War beginning".
- Fidel Castro dead.
- If I Knew
- FBI vs. Facebook

Infected machines were creating a botnet network. But, since most botnet networks are controlled by one central server, this was not case with StormWorm, which was acting more like peer-to-peer network, so controlling node could change from host to host. StormWorm was installing also RootKit which it used to hide itself. Later variants, starting around July 2007, loaded the rootkit component by patching existing Windows drivers such as tcpip.sys and cdrom.sys with a stub of code that loads the rootkit driver module without requiring it to have an entry in the Windows driver list.

Mebroot from 2008 brought one new thing that changed the game - victim could be infected just by surfing internet from browser. It used exploit in browser to gain access to system, and one of the first websites used to spread this malware was official website of Monica Belluci. When Mebroot gained access to victims PC it would install rootkit that could hide him from RootKit detectors, which become part of many antivirus solutions. Mebroot was spying what victim was typing and it was sending this data to attacker. Also this malware was quite good debugged, so it almost never caused crashes of system. Even if it caused crash, it could collect and send traces to attacker so he can debug and fix

the problem. Doing this it was the most advanced malware at that time.

Conficer is one of the greatest mysteries in malware history. The intention of malware creator was not found. It used vulnerability in windows and cracking weak passwords for spreading. It would install backdoor, rootkit and created a botnet node on infect machine. It had infected about 10 millions of host. Great mystery is that it had very complex botnet network that was never used for any attack.

Interesting ransomware is malware that had crypted victims hard disk, changed desktop background with message and demanded 120$ for decryption key. Interesting thing was that attackers were giving away keys if they were paid. For spreading it used browser vulnerability and infected PDF files with script that downloads and installs this malware. It would change desktop background and place on desktop how-to-decrypt.txt file in which was this text:

```
Attention!!!

All your personal files (photo,
documents, texts, databases,
certificates, kwm-files, video)
have been encrypted by a very
strong cypher RSA-1024. The
original files are deleted. You
can check this by yourself -
just look for files in all
folders.

There is no possibility to
decrypt these files without a
special decrypt program! Nobody
can help you - even don't try to
find another method or tell
anybody. Also after n days all
encrypted files will be
completely deleted and you will
have no chance to get it back.

We can help to solve this task
for 120$ via wire transfer (bank
```

```
transfer SWIFT/IBAN). And
remember: any harmful or bad
words to our side will be a
reason for ingoring your message
and nothing will be done.

For details you have to send
your request on this e-mail
(attach to message a full serial
key shown below in this 'how
to..' file on desktop): [email
address]
```

Files that were crypted on disk had extensions: .jpg, .jpeg, .psd, .cdr, .dwg, .max, .mov, .m2v, .3gp, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .rar, .zip, .mdb, .mp3, .cer, .p12, .pfx, .kwm, .pwm, .txt, .pdf, .avi, .flv, .lnk, .bmp, .1cd, .md, .mdf, .dbf, .mdb, .odt, .vob, .ifo, .mpeg, .mpg, .doc, .docx, .xls, and .xlsx..

6. Virtual sabotage and espionage

In year 2010., one big step in malware evolution happened. Malware is no more seen just like thread for businesses, personal finances or files. Military, police forces and secret agencies of several countries got involved in malware creation. Malware is now seen similar as any other weapon. US government declared that any US army keeps right to respond to cyber attack with physical attack. Dropping bombs and cyber attacks using malware are seen as equal things. Also, malware become capable of doing almost same damage as bomb, but without risking human lives. The best example for that is malware called **Stuxnet**, which was discovered in summer 2010.

Stuxnet is a first so called super malware, found in June 2010., but when it was found it is realized that it was spreading undetected for about a year. When Stuxnet was detected it has

already done what it was built for. It is believed that Stuxnet was created to destroy or at least slower down Iranian nuclear program. Stuxnet physically sabotaged turbines for uranium enrichment by changing rotation frequencies. This was done in way that was not seen before. Stuxnet was spreading over the USB stick, where turned off auto run or auto play option would not help. If USB stick was inserted in infected PC it would be infected and if infected USB was inserted in PC, PC would be infected. No anti-virus was able to detect it. Stuxnet used rootkit to hide itself on infected machine and it would do nothing else but replicating to other inserted USB sticks. For gaining control over the PC it used 5 exploits from which 4 was on the day when Stuxnet was first detected 0-day exploits. It would activate it's routines just in case it PC was attached to particular Siemens Step 7 controller, and the PC would be used for programming of controller. Even in that case it would not do anything, if the controller is not attached to particular industrial system. In that case it would changes frequencies of rotation system, and it would also reprogram tools for automatic response, so it would look for them as the system works correctly. Stuxnet contained valid certificate, and when it was blacklisted in one day period it changed its certificate. It had death date set on June 24th 2012., when all instances of Stuxnet would kill itself. It is believed that this malware was created by secret services of USA and Israel. None of these countries confute or confirmed this[12].

DoQu is malware which had similar code base as Stuxnet. It is believed that Stuxnet and DoQu have same origin and same authors. Operation Stuxnet and DoQu are also in correlation in many sources. DoQu used same exploits as Stuxnet, but it has different purpose. It had purpose to gather information about victims, in other words its purpose was to spy infected PCs. DoQu was written in higher programming languages, which is unusual for malware, because most of malware is written either in assembler, C or eventually in C++, or in some of scripting languages as Python or Lua. DoQu was written in object oriented C, and it is believed that is was compiled using Microsoft Visual Studio 2008.

Flame is the most complex malware that have been seen. It was found in 2012. and most of computers was infected in Near and Middle East. It is also believed that was created by Israel and US secret services and military. This is modular malware, that can be controlled by attacker and he can add new modules remotely. With all its modules it can be 20MB large. Flame could spread over the USB port or by network. It used rootkit capability to hide itself on infected system. It had capability to record audio, video, skype calls, network activity, to steal files from hard disk and send to attacker. In the moment when antivirus companies gathered sample of Flame for analysis, Flame was destroyed remotely by attacker who send kill command, which destroyed all the instances of Flame malware. Flame is written in Lua and C++, and as Stuxnet and DoQu it had valid stolen certificate.

7. Conclusion

It has passed more than 25 years since first malware for PC came out. Malware evolved, but some of the principles remained the same. First malware Brain.A spread over floppy disks, Stuxnet - one of the most complex malware - spread over the USB drives.

Purposes and motives for malware creation changed from exibitionism, over revenge and profit to espionage and sabotage. Profit is still great motivator for malware creation, and it will continue to be in future. Military purposes such as espionage and sabotage were proven as success for malware creators. We can expect more of military malware and cyber warfare in future, since it is quite safe for attackers and can cause same damage as military attacks with all its fire power. It has to be seen how antivirus companies would deal with this kind of attackers with almost limitless resources for malware creation on one field and profit wanting malware creators on the other field. Still we might see some other purpose of malware creation in future in some game changing event such was Stuxnet when we are talking about military use of malware.

8. Works cited

[1] Wikipedia, *Malware,*Internet: http://en.wikipedia.org/wiki/Malware, 03.02.2013.

[2] Brain: Searching for first PC Virus, Mikko Hypponen, F-Secure, 2011.

[3] *Malware: Fighting Malicious Code***,** Ed Skoudis, Lenny Zeltser, Prentice Hall PTR, 2003

[4] Wikipedia, Storm Worm,Internet: http://en.wikipedia.org/wiki/Storm_Worm, 10.02.2013.

[5] Virus Wikia, Dark Avanger's Mutation Engine, http://virus.wikia.com/wiki/Dark_Avenger_Mutation_Engine, 17.02.2013.

[6] Virus creation laboratory documentation, Internet, http://www.textfiles.com/virus/DOCUMENTATION/vcl.txt

[7] One_half, ESET Threat enciclopedia, Internet http://go.eset.com/us/threat-center/encyclopedia/threats/onehalf/

[8] Concept.A, FSecure Threat description, Internet, http://www.f-secure.com/v-descs/concept.shtml

[9] Maburg, FSecure Threat descripotion, Interner, http://www.f-secure.com/v-descs/marburg.shtml

[10] Dressler, J. (2007). "United States v. Morris". *Cases and Materials on Criminal Law*. St. Paul, MN: Thomson/West

[11] Slammer, FSecure Threat description, Internet, http://www.f-secure.com/v-descs/mssqlm.shtml

[12] Stuxnet dossier, Simantec, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf