DESIGN OF MULTIBOOT DRIVE USING BART-PE AND BCD FILE

INTERNATIONAL JOURNAL OF APPLIED SCIENCE RESEARCH
(INJASR)
FEDERAL POLYTECHNIC, OKO.
ANAMBRA STATE.

[1]Engr. Okwueze C.N
cyokwueze@gmail.com
08066868222

[2] Nwene Ogbonnaya Vincent
nwenevin@gmail.com
08066867988

[3]Ayodele Sheyi Jonathan
Sheyijoe.sj@gmail.com
07065026954

[1,2&3]Department of Computer Engineering
School of Engineering Technology
Federal Polytechnic Oko

ABSTRACT

The design and configuration of MULTI-BOOT windows BART - Pre-Installation Environment (BART-PE) bootable CD and Flash drive bootable disks below was achieved using BCD file which seek to help in solving the recurrent cases of loss of documents and files when A PC has been attacked by dangerous virus or that the system could no longer boot to window. This design and configuration is purely for installation, maintenance and repair purpose. MULTI-BOOT windows comprising of windows 8, windows 7 and window vista. BART-PE bootable CD used for files and document recovery during emergency cases when a PC cannot boot to windows. Flash drive bootable disks to enable access to a PC that cannot boot to window it`s DOS command prompt to recover files and document. What this research work seek to solve, is to enable the individual computer or the company server that may have been hit by this virus attack, should be able to get all their document and files in one piece without losing any, Despite the system is not able to boot to windows. The Bart PE disk that has been programmed will enable this function to be executed.

This is a designed program that is capable of creating its own window in order to provide access to the system drives and folders so as to enable copying those vital documents without losing any of them.

Keywords: BART-PE, Windows, Virus, BCD FILE Boot Configuration Data file

INTRODUCTION

Today's enterprise networks are distributed to different geographical locations, and applications are more centrally located. Every company's data is most valuable asset and must be treated as such. With the ever growing number of malicious threats; such as Viruses, Spyware and Hackers, it has become mandatory to protect oneself against them. The most powerful way for communication and data transfer is Internet; and because the speed of internet does increase day by day, people can transfer large amount of data within few minutes from one location to another location worldwide.

Computers are used extensively to process the data and to provide information for decision making; therefore it is necessary to control its use. Due to organizational cost of data loss, cost of incorrect decision making, and value of computer software, hardware organisations suffer a major loss therefore the integrity of data and information must be maintained there are thousands of different viruses these days which improve every day. From these virus, performance of computer goes slowly, entire disk will be crashed, programs are modified and more.

INFORMATION ABOUT VIRUS

A computer virus is self-replicating program containing code that explicitly copies itself which then that can infect other programs by modifying them or their environment [1]. Harmful program code refers to any part of programmed code which adds any sort of functionality against the specification. [2] A virus is a program which is able to replicate with little or no user intervention, and the replicated program(s) are able to replicate further. [4] Malicious software or malware for short, are "programs intentionally designed to perform some unauthorized – often harmful or undesirable act." Malware is a generic term and is used to describe many types of malicious software, such as viruses and worms. A typical structure of a computer virus contains three subroutines. The first subroutine which infects executable is responsible for finding available executable files and infecting them by copying its code into them. The subroutine do-damage, also known as the payload of the virus, is the code responsible for delivering the malicious part of the virus. The last subroutine, trigger-pulled, checks if the desired conditions are met in order

LITERATURE REVIEW

A virus is basically an unknown software/program which can create a harmful effect and accessing an unauthorized output for our computer. Now a day computer virus became a big issue for us.

Aboobucker (2017), stated that it is very important to prevent the virus attack and also follow some prevent mechanism through it.

Joseph (1998), mentioned in his research that the main part of virus is the block of code/program or set of instruction that execute when it spreads itself from one file to another file and sometime somewhere network to network that's why we call it as self-replicating software. In our computer different kind of viruses which are already there in the computer mainly take place in memory. When we shut down computer it may remove but not permanently, maximum of those virus are stay there. There are some well-known techniques for destructing viruses from the computer system.

Bhaskar V., and Prof. Milind. J,.(2015) mentioned in their research paper that in the era of internet hackers are very active on their way and computer virus takes some dangerous updated version like-worm, Trojan horse, spam etc.

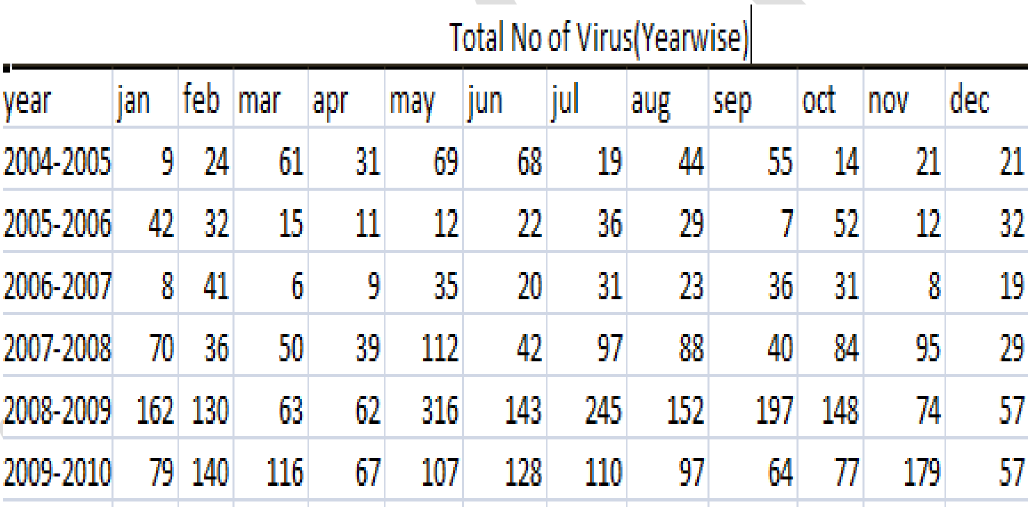
Jeffery H., and Jennifer S., Stated that computer virus may exist in different way for creating problem. So some virus awareness is also needed. Users must have some knowledge about hoe simple virus can cure, how they remove from their P.C.'s.

(Roshan K., mentioned that virus is make our machine less potential and fall it under risky situation. For that reason student are afraid with this topic. so, user have to grow attention on this topic as well as gather some knowledge for give a safe state to his/her own computer .

HISTORY OF COMPUTER VIRUS

Here shows some virus creation history from year 2004 to 2010.The table focus that every year how much Virus is created [12].

Table 1 : Total of number of Virus



Total No of Virus(Yearwise)

year	jan	feb	mar	apr	may	jun	jul	aug	sep	oct	nov	dec
2004-2005	9	24	61	31	69	68	19	44	55	14	21	21
2005-2006	42	32	15	11	12	22	36	29	7	52	12	32
2006-2007	8	41	6	9	35	20	31	23	36	31	8	19
2007-2008	70	36	50	39	112	42	97	88	40	84	95	29
2008-2009	162	130	63	62	316	143	245	152	197	148	74	57
2009-2010	79	140	116	67	107	128	110	97	64	77	179	57

Chart 1: Total no of Viruses (Year wise)

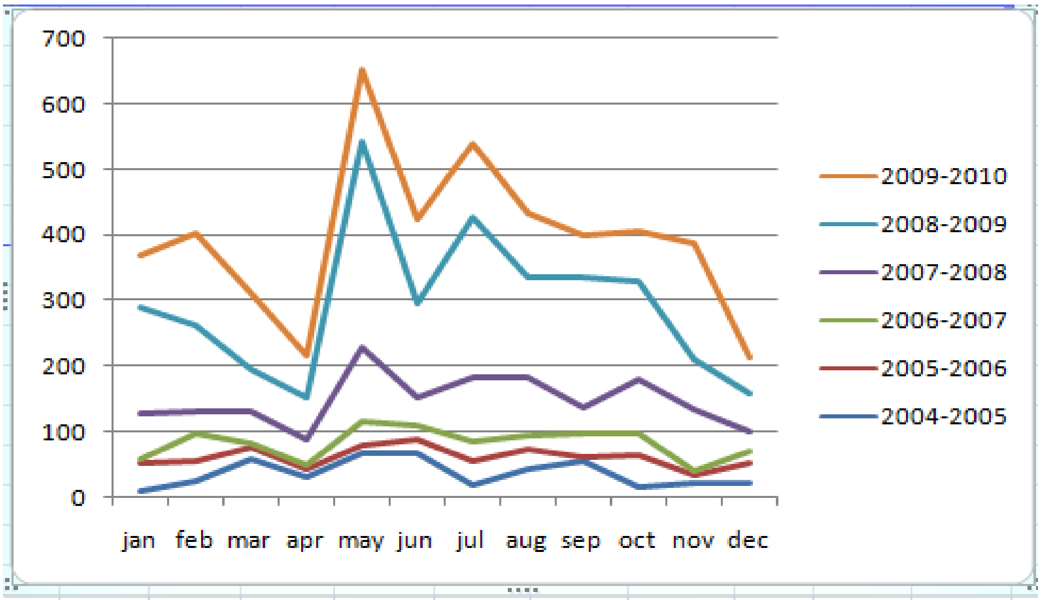

700
600
500
400
300
200
100
0
jan
feb
mar
apr
may
jun
jul
aug
sep
oct
nov
dec
2009-2010
2008-2009
2007-2008
2006-2007
2005-2006
2004-2005

Table 2: Comparison of Viruses

Virus	Type	Isolation date	Notes
1260	DOS	1990	First Virus to use Encryption
5lo	DOS	1992-10	Infects .EXE files only
Acid	DOS, Windows 95, 98	1992	Infects COM files.
ANTI	Classic Mac OS	1989-02	First MAC OS Virus.
Autostart	Classic Mac OS	1998	
Christmas Tree		1987-12	
Form	DOS	1990	Common Boot Virus
I Love You	Microsoft	2000-05-05	It is a worm, attacking 10 Millions of Windows PCs.
Kama Sutra		2006-01-16	It is designed to destroy some common files like-Word, Excel, Ppt etc.
Pikachu Virus		2000-06-28	First Virus which is created only for Children.
Fun	Windows	2008	In Windows OS it registered itself then sent mail with spreading attachments in Outlook Express.

TYPES OF COMPUTER VIRUS

Resident_Viruses: It installs them into the systems memory and gets working when the O.S. runs and create some unauthorized issue for all the files as then opened. It hides in the RAM and if the malicious code is not executed it stays there.* E.g.:-Randex, Direct action_viruses: It comes into action when a file containing the virus is executed. E.g.:-Vienna Virus Overwrite_Viruses: it removes any information which is contained in the files .It furnish them partially or totally useless once they have been infected. E.g.:-Trojan reboot

Boot_Sector_Viruses:_It affects the boot sector part of a Hard Disk. It is also called the “Master Boot Sector Virus”.

E.g.:- Polyboot.b

Macros_Viruses:_It affects files which are created using application and certain programs like .doc, .put, .xls etc. Macro Virus hides in documents and spreads via E-mail and network connectivity.

FAT_Virus: It is basically used to attacks the file information location of file's expandable space. The FAT virus execute like an index, it keeps track of all information where hard Drive materials are stored [12].

E.g.:- Link Virus

Multi_Variant_(Partite)_Virus:_- It comes in computer systems from different resources and gets. The chance of unauthorized access power but it does not

Infects on hard disk.

Trojan_Horses:-A Trojan or Trojan horse is a duplicate type of malware which is performed for

Fetching purposes but takes the facilities of unauthorized access to the user's computer system

.

*The term comes from the "Trojan horse story in Greek Mythology" because Trojan horses created a form of social engineering which presents themselves as a unique gifts in order

RESEARCH METHODOLOGY

The bcd file is used by bios to boot image into the computer.

The bcd file is also used to load windows vista,window 7 and window 8 boot images and setup.The bcd file used in conjunction with windows boot manager file "bootmgr"to load boot images and it can also be used in conjunction with window xp boot manager file "ntlr" to load windows xp boot image.

The bcd file is configured separately for window 8, window 7 and window vista.however,bcd file can be created and configured for MULTIBOOT purposes.we are going to configure a bcd file that will load windows 8 setup, windows 7 and windows vista. Setup. All from one usb hard drive.

The application that is used to create and configure bcd file is bcdedith.The bcd file must be created and configured in a boot folder.

CREATING MULTIBOOT BCD FILE

The bcd file s created in three sections.

A .Boot manager

B. Ramdisk option

C. Application OSloader

CREATING BOOT MANAGER

```
bcdedith  /createstore  c:\boot\bcd
bcdedith  /store  c:\boot\bcd  /create{bootmgr}
bcdedith /store  c:\boot\bcd  /set {bootmgr} description “boot manager”
bcdedith/store c:\boot\bcd  /set {bootmgr} device boot
bcdedith/store  c:\boot\bcd  /set {bootmgr} timeout 30
```

CREATING RAMDISK OPTION

```
bcdedith  /store  c:\bcd  /create  /device            [a ramdisk _guid is created]
```

A guid is a unique number to represent an object.

```
Bcdedith  /store  c:\boot\bcd  /set {ramdisk_guid} ramdisksdevice boot
Bcdedith  /store  c:\boot\bcd  /set {ramdisk_guid} ramdiskdipath
\boot\  boot.sdi  {for windows 8}
\boot2\  boot.sdi {for windows 7}
\boot3\boot.sdi {for window cista}
```

CREATING APPLICATION OSLOADER

WINDOWS 8

```
bcdedith  /store  c:\boot\bcd   /create  /application osloader {a guid is created}
bcdedith  /store  c:\boot\bcd  /set{guid}  systemroot  \windows
bcdedith  /store  c:\boot\bcd  /set{guid}  custom:250000c2    1
bcdedith  /store  c:\boot\bcd  /set{guid}  detecthal   yes
bcdedith  /store  c:\boot\bcd  /set{guid}}  winpe  yes
bcdedith  /store  c:\boot\bcd  /set{guid}   ems       No

bcdedith  /store  c:\boot\bcd  /set{guid}   path  \window\system32\boot\winloader.exe

bcdedith  /store  c:\boot\bcd  /set{guid}   device
ramdisk=[boot]\sources\boot.win,{ramdisk_guid}

bcdedith  /store  c:\boot\bcd  /set {guid}  osdevice
ramdisk=[boot]\sources\boot.win,{ramdisk.guid}

bcdedith  /store  c:\boot\bcd  /set {guid}  description “window 8 setup”

bcdedith  /store  c:\boot\bcd  /displayorder {guid}  /addlast
```

WINDOWS 7

```
bcdedith  /store  c:\boot\bcd   /create  /application osloader {a guid is created}

bcdedith  /store  c:\boot\bcd  /set{guid}  systemroot  \windows

bcdedith  /store  c:\boot\bcd  /set{guid}  detecthal   yes

bcdedith  /store  c:\boot\bcd  /set{guid}}  winpe  yes

bcdedith  /store  c:\boot\bcd  /set{guid}   ems      Yes

bcdedith  /store  c:\boot\bcd  /set{guid}   path  \window\system32\boot\winloader.exe

bcdedith  /store  c:\boot\bcd  /set{guid}   device
ramdisk=[boot]\sources2\boot.win,{ramdisk_guid}

bcdedith  /store  c:\boot\bcd  /set {guid}  osdevice
ramdisk=[boot]\sources2\boot.win,{ramdisk.guid}

bcdedith  /store  c:\boot\bcd  /set {guid}  description “window 7 setup”

bcdedith  /store  c:\boot\bcd  /displayorder {guid}  /addlast
```

WINDOWS VISTA

```
bcdedith  /store  c:\boot\bcd   /create  /application osloader {a guid is created}

bcdedith  /store  c:\boot\bcd  /set{guid}  systemroot  \windows

bcdedith  /store  c:\boot\bcd  /set{guid}  detecthal   yes

bcdedith  /store  c:\boot\bcd  /set{guid}}  winpe  yes
bcdedith  /store  c:\boot\bcd  /set{guid}   ems      yes

bcdedith  /store  c:\boot\bcd  /set{guid}   path  \window\system32\boot\winloader.exe

bcdedith  /store  c:\boot\bcd  /set{guid}   device
ramdisk=[boot]\sources3\boot.win,{ramdisk_guid}

bcdedith  /store  c:\boot\bcd  /set {guid}  osdevice
ramdisk=[boot]\sources3\boot.win,{ramdisk.guid}

bcdedith  /store  c:\boot\bcd  /set {guid}  description “window vista setup”

bcdedith  /store  c:\boot\bcd  /displayorder {guid}  /addlast
```

RAMDISK_GUID	{850dc469-1461-11e4-acd1-f8d644c91736}
WINDOWS 8 GUID	{225fd41d-1463-11e4-acd1- f8d644c91736}
WINDOWS 7 GUID	{857F9CF5-1465-11e4-acd1- f8d644c91736}
WINDOWS VISTA	{355C248B-1467-11e4-acd1- f8d644c91736}

```
Xcopy   D:\users\okwueze\ducuments\*.*

Xcopy  D:\user\**/E/S/Q S:\USER / 1
```

REFERENCES

1. WWW.MICROFOFT.COM

2. The Wild List Organization International, www.wildlist.org

3. Digg, Worst Computer Virus Attacks in History, (2009 September).

4. Paul R., Mitch H., David D., Robert E., & Wenke

Lee. P.,: Automating the Hidden-Code Extraction of Unpack-Executing Malware, in the 22th Annual Computer Security

Applications Conference (ACSAC 2006), Miami Beach, FL, (2006 December).

5. Solomon’s Virus Encyclopedia, ISBN, 1897661002, (1995).

6. Brunnstein, K. “Antivirus to Antimalware Software and Beyond”, (1999).

7. Coulthard, A., & Vouri, T., “Computer Viruses: a quantitative analysis Logistics Information Management”, Volume 15. Number 5/6, ISSN 0957 – 6053, 2002, PP.400- 409.

8. Rad, B., Masrom, M., & .Brahim, “Evolution of Computer Virus Concealment and Anti-Virus Techniques: A Short Survey”, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 1, 2011.

9. F-Secure Corporation, “Computer Viruses – from an Annoyance to a Serious Threat”. White Paper, (2001).

10. J. W. H,”Internet computer virus protection policy, Journal of Information Management & Computer Security”, Number 6/2, MCB University Press. ISSN 0968-5227, 1998, PP.-66–71 T. Micro, “Virus and Malicious Code Protection for Wireless Devices”, (2001 February).

11. F-Secure. Corporation, “Computer Viruses - Theory and Experiments”,”Computer Security: A Global Challenge”, Elsevier Science Publishers B. V. (North-Holland), (1984), pp. 143-158.

12. Royal, P., Haplin, M., Dagon, D., Edmonds, R., & Lee, W., Poly Unpack: “Automating the Hidden-Code Extraction of Unpack- Executing Malware”. In The 22th Annual Computer Security Applications Conference, Miami Beach, FL, (2006 December).