ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

VIRUS GENERATION KITS: A SURVEY

Ankur Singh Bist
Computer Engineering, K.I.E.T, Ghaziabad, India

ABSTRACT

This paper is designed to make the survey of virus generation kits. Their capability of generating the viral files with different behaviour makes each of them distinct. In order to analyze the varying trend in computer virology, the study of these kits becomes important.

KEYWORDS: Kits, Replication.

INTRODUCTION

There are various processes that have been used in the direction of classification of computer viruses from normal files that will finally lead to worm detection. Machine learning techniques are widely used in this direction. As statistics says that the attacks of malicious codes are increasing day by day so there is requirement of strong techniques that can be used for their detection. Malicious code designers use lot of techniques that are difficult to analyse and detect. The static methods also seems not to work in the case where every time there are rapid dynamicity from attacker side so now a days main focus is going on towards the methods that are dynamic and are able to detect zero day computer viruses [1].

The rise in the malicious threats like computer viruses activities are required to be handled and observed strongly to make certain defence that can stand as a saviour of security domain. Other types of malware are:

1. Worms
2. Trojan horse
3. Botnets
4. Adware
5. Spyware

The mutating behaviour of metamorphic viruses is due to their adoption of code obfuscation techniques like dead code insertion, Variable Renaming, Break and join transformation. The given diagram shows the assembly file of the virus code.

Figure 1: Assembly code of Virus File

VIRUS GENERATION KITS

Computer virus generation kits are used to generate viruses but the basic purpose of these kits are not to create problems but these kits are used by computer virology researchers in order to analyze the behavior of viruses. The list of virus generation kits are as follows [3]:-

1. AMG
2. AVCS
3. BVGEN
4. CMK
5. CVCK
6. Demolition Kit
7. DNVG
8. DPVG
9. DVG
10. EMVCK
11. EZVCK
12. Genesis/ASM
13. IBBM
14. IPVCK
15. JBM
16. LANVL
17. LiME
18. ME
19. MSVG
20. MVDK

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

21. NEG
22. OMVCK
23. PMG
24. RAHC
25. SABV
26. SCVG
27. SkyVCL
28. SVG
29. TSWSVK
30. UVC
31. VBSWG
32. VCS
33. VGT
34. VKIT
35. NGVCK
36. MWOR

Other than this there are lot of virus generation kits and growing continuously. Some kits that are used frequently are given below with their date of release and functions.

Table 1 Example of Virus Generator Kits

Virus Kit	Release	Function
NRLG (NuKE's Randomic Life Generator)	Release-1994	It gives user friendly interface to create virus.
OMVCK (Odysseus Macro Virus Construction Kit	Release-1998	It can generate Word Basic macro-virus source code.
SSIWG (Senna Spy Internet Worm Generator)	Release-2000	This generator supports the creation of VBS worms.
NEG (No Mercy Excel Generator)	Release-1998	This was the first Excel macro virus generator kit. It creates .bas files.
VBSWG (VBS Worm Generator)	Release-2000	It generates various script worms.
AMG (Access Macro Generator)	Release-1998	To generate Access97 macro viruses.
DREG (Digital Hackers' Alliance Randomized Encryption Generator)	Release-1997	Supports advanced code morphing and anti-heuristics.

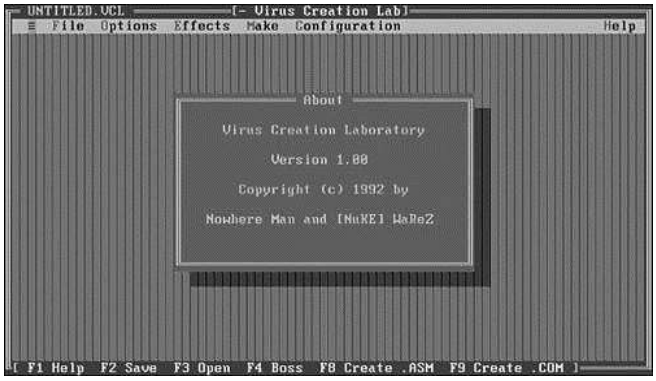

Figure 2: GUI of virus creation laboratory

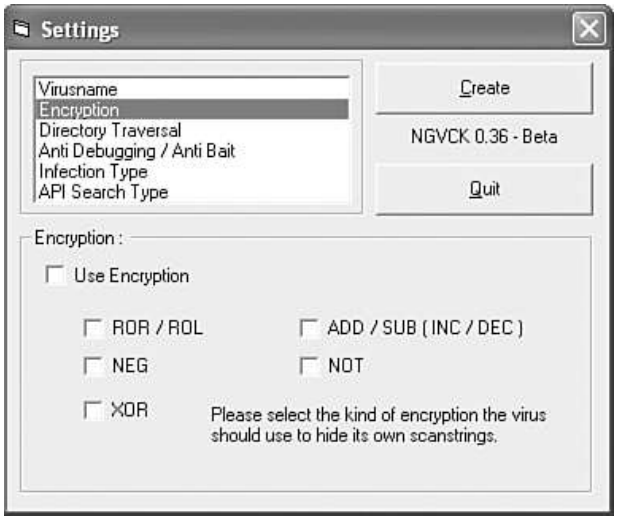

Figure 3: GUI of NGVCK kit

In order to visualize the scenario of virus generation kits the GUI of VCL and NGVCK are given above.

Now we will discuss two important kits that are being used for analysis of computer viruses.

1. NGVCK- It uses register swapping and various techniques of code reordering to generate morphed malwares. The statistical techniques are used to deal with the malware content produced by this kit.
2. MWOR- Metamorphic Worm (MWOR) uses its own morphing engine and produces malicious content that is of highly concealing nature not easily detected by

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

simple methods.

The following figure shows about the maximum, minimum, and average similarity scores between virus variants generated by each generator and between normal files. That diagram justifies the impact of NGVCK kit as compare with other kits

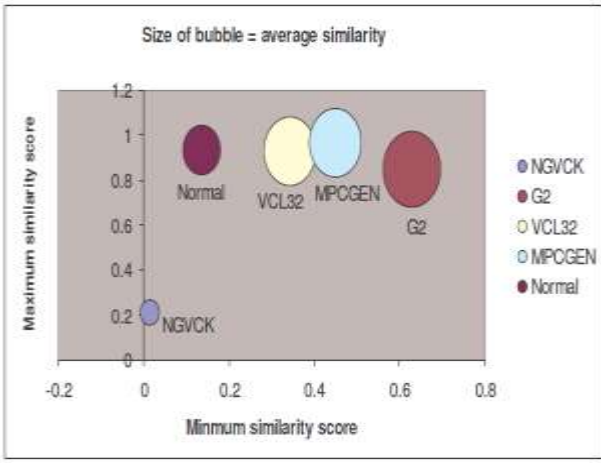

Figure 4 Bubble graph representing minimum, maximum, and average similarity between virus variants generated by each generator and between normal files **(Wong and Stamp, 2003) [2].**

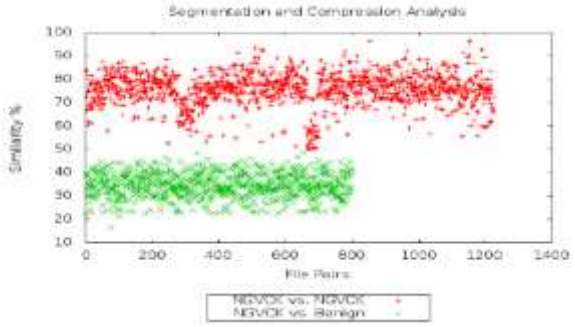

Figure 5: NGVCK similarity [4]

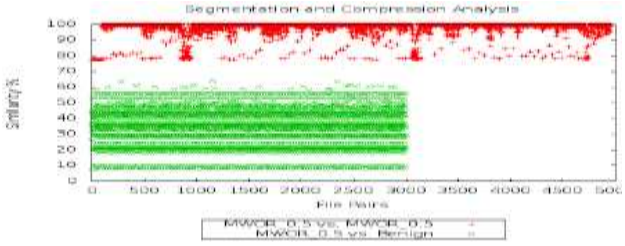

Figure 6: MWOR similarity [4]

Figure 4 and Figure 5 explains the analysis for virus classification based on NGVCK and MWOR kit.

CONCLUSION

The computer virus generation kits are used for research analysis in the field of computer virology. This paper involves the survey study of different kits used for malware generation. Some kits that are broadly used in research due to their property of generating challenging viruses that is not easy to detect. This study will be helpful for those working in the field of computer virology.

ACKNOWLEDGEMENT

I wish to express my special thanks to all who supported me directly or indirectly in this work.

REFERENCES

1. www.wikipedia.com
2. **Wong, W. 2006.** Analysis and detection of metamorphic computer viruses. Masters Thesis. Department of Computer Science, San Jose State University.
3. **VX Heavens.** http://vx.netlux.org/**Lee, Jared**, "Compression based analysis of metamorphic malware"