Systems in Danger: A Short Review on Metamorphic Computer Viruses

Seyed Amirhossein Mousavi[1], Babak Bashari Rad[2], Teh Ying Wah[3]
[1,2]Asia Pacific University of Technology & Innovation, [1,3]University of Malaya
[1,2]Technology Park Malaysia, Bukit Jalil, 57000 Kuala Lumpur, Malaysia, [1,3]University of Malaya, Jalan Universiti, 50603 Kuala Lumpur, Malaysia
[1]seyed.amir@apu.edu.my, [2]dr.babak.basharirad@apu.edu.my, [3]tehyw@um.edu.my

ABSTRACT

In current times, anti-virus scanners are usually built on signatures which look for known patterns in order to decide if a file is virus infected. Hackers have incorporated the code obfuscation methods to generate highly metamorphic system malware in order to evade detection of signature based scanners. The scanners which are signature based may not be able to detect all existence of such viruses. Since, the metamorphic malware changes their appearance from one generation to another. Metamorphic malware is one of the many techniques that hackers use to attack systems. This paper explores the common types of computer malwares and metamorphic computer viruses while reviewing the different techniques of metamorphic malwares which are able to avoid detection.

KEYWORDS

Malware, Compute Virus, Metamorphic virus, Polymorphic Virus, Obfuscation.

1 INTRODUCTION

As information technology is growing and improving, the need for endpoint protection is getting more imperative. An end point can be a laptop, desktop, server, or a mobile device that connects to a network (internet). According to Internet Live States, the number of Internet users have amplified remarkably from 1999 to 2013 to the tenfold and today more than 40 % of the world population has access to internet connection [1]. Therefore, the impressive growth of these facts in the recent years, show that the end point devices need to be protected from the enormous number of malwares which attempts to infiltrate such systems via the network and internet connected devices.

In this paper, firstly the metamorphic malware characteristics will be explored. In order to achieve this goal, we initially outline different types of malwares that have been developed to defeat signature based antivirus scanners, then we discuss about the common types of computer viruses and the complexity of metamorphic malware along with its characteristics.

This paper discusses the sections in the following order: In next section, we describe the common types of malwares. Section 3 explores polymorphic and metamorphic computer viruses, and the complexity of metamorphic malware. Section 4 is a research about the previous related works. Finally, the conclusion will be given in the final section.

2 COMMON TYPES OF MALWARE

Following sections discuss the common types of malware which can be broadly classified into different categories.

2.1 Adware

Adware or Advertising sustained software is a type of computer malware that can spontaneously deliver advertisements. An

adware will display or download advertisement to a computer after a malicious software is installed or application is used [2].
This software is programmed to determine which internet site is most visited by the user and then displays advertisements relevant to the user's interests. The most common adware programs are online free games, peer to peer software such as torrents, etc.

2.2 Spyware

These type of malwares are either spying on or monitoring users and gather information about the web sites frequently visited by the users, which may include credit cards or online banking details, email addresses etc. This software helps the hackers to collect information about victim's system without the consent of the victim. A good example of this malware is a keylogger software which is used to monitor activities of a victim system [3].

2.3 Worms

It is a program which copies itself repeatedly and eliminates all the data and files on the victim computer. This program is designed to steal data, delete files or create botnets. According to Cisco, computer worms are similar to viruses and can cause the same type of damage [4]. The major difference is that worms have the ability to work as a standalone software and spread independently while viruses need human help to propagate [2]. One technique of distributing worm is via sending large number of emails with infected attachments to a user's contact list.

2.4 Trojan Horse

Trojan Horse is a malicious program that acts to be a harmless software. However, according to Cisco, Trojan viruses are not able to re-create themselves by infecting other files nor do they self-replicate. In order to spread itself, this type of malware requires the end user to interact with the virus though mediums such as downloading and executing a file from internet or just by opening an email attachment [4].
Trojan Horses are accruing to different classifications depending on how the systems are breached and the amount of the damages caused by it. Some major types of Trojan Horses are inclusive of remote access Trojans, proxy Trojans, FTP Trojans, Destructive Trojans etc. [5].

2.5 Botnet

Botnet, also known as zombie army, is a type of malware that an attacker can use to control the infected computer or any remote devices. The word Botnet is a comprised version of the words: bot and net. In this context, Bot is derived from the word "robot" which usually refers to a computer or device which is infected by malicious software. On the other hand, Net is generated from the word "network" which is a group of interconnected computers connected together. Attackers developing a malicious application might not be able to log onto individual computers which they might have infected, therefore attackers utilize botnets in order to control a massive quantity of infected computers automatically [6].

2.6 Ransomware

This is a type of malicious software that blocks or limits the user from accessing the computer or the files contained by the computer. These destructors work by locking either the system's screen or the user's files and the scammer demanding a ransom in exchange for them to be unlocked. It is also considered a scareware as it forces user to pay a fee by scaring or intimidating them [7].

2.7 Rootkit

A rootkit is another type of computer malware that is intended to distantly access a system

without detection by any user or security program [2].
The prevention of rootkit attack can be very difficult and the hardest of all Malwares to detect because of their stealthy operation and attempt to continually hide their presence. Therefore, the detection process relies on other methods such as manual detection like monitoring computer behavior for irregular activity, signature scanning and etc. [8].

2.8 Virus

A virus is another variant of malicious software which is a smaller sized program with harmful intent which copies itself and spreads to other systems. This malicious software most often spreads by sharing software or files between different computers [4].
The two common types of viruses are known as polymorphic and metamorphic viruses which will be discussed in the next chapter.

3 POLYMORPHIC AND METOMORPHIC COMPUTER VIRUSES

As discussed in the previous section a virus is another type of malicious software that is a small in size with harmful intent that will easily copy itself and spread to other systems. This section relates to the field of computer viruses, and discusses about two (2) common types- polymorphic and metamorphic viruses.

3.1 Polymorphic

It is one of the most complicated types of system malwares that can affect data types and functions. It is a self-encrypted virus which is categorized by the following behavior: encryption, self-multiplication and ability to change one or more components of itself to remain elusive. It is designed to avoid detection by a scanner and is capable of creating modified copies of itself [9].
Therefore, a polymorphic virus has the tendency to change itself more than one way before propagation onto the same computer or interconnected network computers. Since this malicious software is changing its components properly and they are encrypted, it is very difficult for anti-virus applications to detect them and can be said to be one of the most intelligent viruses as they are hard to identify.
Polymorphic viruses are able to create an infinite number of new decryptors which require to use different types of encryption methods in order to encrypt the constant part of the virus body. The following figure represents generation of a polymorphic virus.

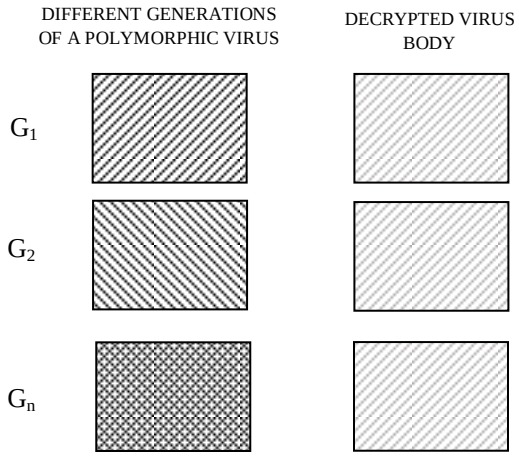

Figure 1. Generation of a polymorphic computer virus [15]

3.2 Metamorphic

According to Kaspersky, A metamorphic malware is the one that can transform based on the ability to edit, translate and rewrite its own codes. Metamorphic malware is considered the most infectious malicious software and can cause serious damage to a system if it is not detected quickly [10].
It is very difficult for antivirus programs to detect metamorphic malware as it has the ability to change the internal structure of the code; reprogram and rewrite after each infection to a computer system [14]. To prevent computers in networks of infectious metamorphic malware, user administrator

should use a multi-layered approach to blended management including: a well-defined set of security policies, restrictions for remote access control and usage of an antivirus that is frequently updated.

Metamorphism can change the appearance of the virus while maintaining its functionality. Metamorphic virus does not require decryption or encryption techniques. They present new bodies of viruses on each infection. Metamorphic engine can either be embedded in the virus itself or can be either left isolated [14]. Figure 2 illustrates the generations of a metamorphic virus whose shape changes but the functionality stays the same.

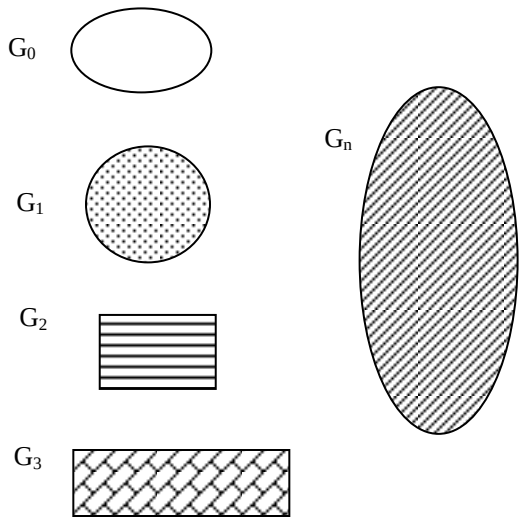

Figure 2. Generation of a metamorphic computer virus [15]

3.3 Obfuscation Techniques

Virus writer generally uses different techniques to develop a highly morphed metamorphic virus. The following sections show the common techniques of programming a metamorphic virus.

3.3.1 Register Swap Technique

This is the simplest technique of metamorphic malware. In this technique a malware changes its body via the implementation of different types of registers, regardless the opcodes are still similar across generations. A good example of this technique is W95/RegSwap virus. Although the new transformed version of the virus is not the same with the previous one, the variability still is not in high level and the virus can be easily detected by using simple techniques such as Half-Byte wildcard in signature string scanning [11]. This technique is also called registers exchange or registers renaming.

a.)

```
5A              pop     edx
BF04000000      mov     edi,004h
8BF5            mov     esi,ebp
B80C000000      mov     eax,000ch
81C288000000    add     edx,0088h
8B1A            mov     ebx, [edx]
899C8618110000  mov     [esi+eax*4+00001118],ebx
```

b.)

```
58              pop     eax
BB04000000      mov     ebx,0004h
8BD5            mov     edx,ebp
BF0C000000      mov     edi,000Ch
81C088000000    add     eax,0088h
8B30            mov     esi, [eax]
89B4BA18110000  mov     [edx+edi*4+00001118],esi
```

Figure 3. Two different generations of RegSwaps [11]

3.3.2 Subroutine Permutation Technique

In this technique, by reordering the virus' subroutines, the appearance of a virus would be changed too. For example, when a virus has 'n' unique number of subroutines, it can generate n factorial various generations without repetition. A good example of this virus that incorporates in this technique is W32/Ghost. This malicious application contains 10 subroutines from which it is able to generate 10 factorial or 3,628,800 discrete replicated items. Nonetheless, the virus may still be detected with the usage of search

strings [12] as the content of every subroutine stays the same.

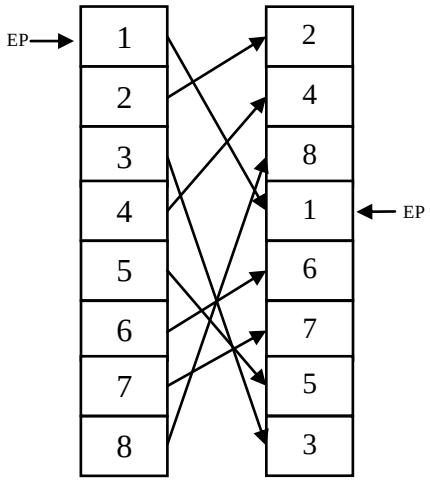

Figure 4. Subroutine permutation Technique [12]

3.3.3 Garbage Instruction Insertion Technique

Some Metamorphic viruses utilize the removal and insertion of garbage instruction codes to produce morphed copies. This technique is also familiarized as "do nothing code" which does not alter the function of an application when executed, but rather will cause the size of the code to be increased [13].

Viruses containing garbage instructions are difficult to detect via the usage of signature, because this technique breaks the signature of the virus. This instruction may be added within a threshold value. The intrusion detection systems are definitely able to identify the anomaly in the code if the quantity of garbage instructions are greater in number. The following table is shown as an example of garbage instruction codes.

Garbage Instructions	Comments
push cx pop cx	Before any effects, it returns the value to the register form stack
inc ax sub ax,1	Value of ax remain unchanged

Figure 5. Example of Garbage Codes [13]

4 RELATED WORKS

A research about metamorphic malware dynamic analysis by Nair, V.P. [16] discuss a technique for identifying unnoticed malware samples via STraceNTx which basically executes files in an emulated framework was proposed. However the results of the test concluded that NGVCK produced variants showed lower level of inter and intra constructor proximity. Another research in opcode graph similarity and metamorphic detection by Runwal,N. [17] in 2012 discusses about the development of another graph based malware detection tool. The deconstructed malware files were used in order to generate an opcode graph. The conclusion drawn was that the HMM based scanner was not competent against the graph based technique.

The journal in structural entropy and metamorphic malware by Baysa, D [18] discusses how a statistical malware detector was developed which was based on structural entropy and wavelet transform. For the G2 Viruses and MWORM a detection percentage of 100 was achieved. Nonetheless, a false positive rate was achieved for NGVCK virus of larger capacity. The research by Vinod, P. in 2012 talks about implementing Bioinformatics Multiple Sequence Alignment (MSA) technique in order to detect metamorphic malware. [19] This detector however was able to achieve a better detection at the rate of 73.2% and was awarded the third most accurate in comparison to other malware commercial scanners.

The research paper by Raphel, J and Vinod, P in 2015, proposed a system which is non-signature based and is able to create a meta feature area in order to detect metamorphic malware [20]. In this paper it was discussed how metamorphic malware was detected by collecting metamorphic malware samples where three combinations of function are taken out from the files which are branch opcodes, unigrams and bigrams. Toderici, A.H and Stamp, M in 2015, constructed a hybrid malware detector via combining HMM and

Chi-Square methods. The aforementioned hybrid tool demonstrated improved accuracy when differentiated with other malware detectors autonomously exhibited with HMM and CSD [21].

Sridhara, S. M and Stamp, M in 2013 proposed the development of a metamorphic worm. The results from the experiments demonstrated that MWORM expanded with nonthreatening subroutine in order to evade detection via signatures [22]. To find dead code in malware specimen, code emulation is used in another research by Priyadarshi in 2011 [23]**.** This emulator was applied on the metamorphic worms consequently maintaining the HMM approach. Linear Discriminant Analysis (LDA) was used for metamorphic malware detection in another research by Kuriakose, J and Vinod, P in 2014**.** When using LDA ranked features for classification, a 99.7% of detection level is acquired [24].

5 CONCLUSION

The evolution of malware has become a great challenge of this decade. Malwares are getting more intelligent and spreading faster among the worldwide computer networks. It will be an interesting time for antivirus researchers to explore some new methods for detection of these destructors. Metamorphic malware family is the most challenging threat today as they are quite advanced and furthermore reduced the significance of signature-based detection.

For an attacker, writing a metamorphic malware is considered to be more difficult than writing polymorphic, which needs to be programmed to use multiple transformation techniques such as register renaming, code shrinking, code permutation and garbage code insertion. Consequently, for detection of this malware, different techniques such as generic decryption techniques, negative heuristic analysis and etc. are required to be applied.

In this research, we briefly surveyed the common malware types such as adware, spyware, worms, Trojan horse, botnet, ransomware, rootkit and viruses which can also be classified in further categories. Also, we surveyed different techniques of metamorphic malware as register swap, subroutine and garbage instruction which have been created mainly to help metamorphic malware to evade antivirus scanners. The future trend is to research about artificial intelligent techniques to provide a more efficient technique to increase the accuracy of detection of metamorphic malwares.

REFERENCES

[1] Internet Live State. 2016. Internet User in the World [Online].Available: http:// internetlivestats.com/internet-users/. [Accessed 31th July 2016].

[2] Nate Lord. 2012. Common Malware Types: Cybersecurity [Online].Available:https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101 [Accessed 1th August 2016].

[3] Vinod P, and V.Laxmi,M.S.Gaur. 2009. Survey on Malware Detection Methods, in Proceedings of the 3rd Hackers' Workshop on computer and internet security (IITKHACK'09).

[4] Cisco. What Is the Difference: Viruses, Worms, Trojans, and Bots?[Online].Available:hhttp://www.cisco.com/c/en/us/about/security-center/virus-differences.html#2 [Accessed 25th July 2016].

[5] Webopedia. Trojan horse [Online].Available: http://www.webopedia.com/TERM/T/Trojan_horse.html [Accessed 26th Juky 2016].

[6] Stephen Cobb. 2014. Botnet malware: What it is and how to fight it[Online].Available: http://www.welivesecurity.com/2014/10/22/botnet-malware-fight/ [Accessed 30th July 2016].

[7] scamwatch. 2016. Malware & ransomware [Online].Available: https://www.scamwatch.gov.au/types-of-scams/threats-extortion/malware-ransomware [Accessed 5th August 2016].

[8] Malwaretruth. 2016. List of Common Malware Types [Online].Availablehttp://www.malwaretruth.com/the-list-of-malware-types/ [Accessed 4th August 2016].

[9] Arun Kumar. 2016. What is a Polymorphic Virus and how do you deal with it [Online]. Available http://www.thewindowsclub.com/polymorphic-virus [Accessed 5th August 2016].

[10] Kaspersky. 2016. What is Metamorphic Virus? [Online]. Available https://usa.kaspersky.com/internet-security-center/definitions/metamorphic-virus#.V6nfErh94_5 [Accessed 7th August 2016].

[11] Gayathri Shanmugam. 2012. Simple Substitution Distance and Metamorphic Detection
[Online]. Available
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.344.865&rep=rep1&type=pdf [Accessed 2th August 2016].

[12] J. Borello and L. Me, "Code Obfuscation Techniques for Metamorphic Viruses," Feb 2008, Journal in Computer Virology

[13] E. Daoud and I. Jebril, "Computer Virus Strategies and Detection Methods," Int. J. Open Problems Compt. Math., Vol. 1, No. 2, September 2008

[14] Babak Bashari Rad, Maslin Masrom, and Suhaimi Ibrahim, "Camouflage in Malware: from Encryption to Metamorphism," IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.8, August 2012.

[15] Peter Ferrie. 2003. Hunting For Metamorphic
[Online]. Available
https://www.symantec.com/avcenter/reference/hunting.for.metamorphic.pdf [Accessed 7th August 2016].

[16] Nair, V. P., Jain, H., Golecha, Y. K., Gaur, M. S., & Laxmi, V, "MEDUSA: MEtamorphic malware dynamic analysis using signature from API," Proceedings of the 3rd International Conference on Security of Information and Networks, pp. 263-269, 2010.

[17] Runwal, N., Low, R. M., & Stamp, M, "Opcode graph similarity and metamorphic detection," Journal in Computer Virology, 8(1-2), 37-52, 2012.

[18] Baysa, D., Low, R. M., & Stamp, M., "Structural entropy and metamorphic malware," Journal of Computer Virology and Hacking Techniques, 9(4), 179-192, 2013.

[19] Vinod, P., Laxmi, V., Gaur, M., & Chauhan, G, "MOMENTUM: Metamorphic malware exploration techniques using MSA signatures," Innovations in Information Technology (IIT), International Conference on, pp. 232-237, 2012.

[20] Raphel, J., & Vinod, P., "Pruned feature space for metamorphic malware detection using markov blanket," Contemporary Computing (IC3), 2015 Eighth International Conference on, pp. 377-382., 2015.

[21] Toderici, A. H., & Stamp, M., "Chi-squared distance and metamorphic virus detection," Journal of Computer Virology and Hacking Techniques, 9(1), 1-14, 2014.

[22] Sridhara, S. M., & Stamp, M, "Metamorphic worm that carries its own morphing engine," Journal of Computer Virology and Hacking Techniques, 9(2), 49-58, 2013.

[23] Priyadarshi, S. 2013. Metamorphic detection via emulation [Online]. Available
http://www.cs.sjsu.edu/faculty/stamp/students/priyadarshi_sushant.pdf [Accessed 22th August 2016].

[24] Kuriakose, J., & Vinod, P., "Ranked linear discriminant analysis features for metamorphic malware detection," Advance Computing Conference (IACC), IEEE International, pp. 112-117, 2014