International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

Malware Types and Different Detection and Prevention Methods

Seelam Sowjanya & capt.Tesfaye Shiferaw

Assistant Professor, Department of Computer Science and Information Technology, Defense University College of Engineering, Bishoftu, Ethiopia

Department of Computer Science and Information Technology, Defense University College of Engineering, Bishoftu, Ethiopia

ABSTRACT

Everyone knows about computer viruses. Just over twenty years ago, the first virus for PCs was written, apparently with the intention of protecting software on old-style floppy disks from bootleggers. Since then, hundreds of thousands of viruses and other malware‖ email viruses, Trojans, internet worms, keystroke loggers have appeared some spreading worldwide and making headlines. Many people have heard about viruses that fill your computer screen with garbage or delete your files. Today, malware is unlikely to delete your hard disk, corrupt your spreadsheet, or display a message. Such cyber vandalism has given way to more lucrative exploits. Today's virus might encrypt all your files and demand a ransom. Or a hacker might blackmail a large company by threatening to launch a denial of service attack, which prevents customers from accessing their website.

KEYWORDS: Malware, Malware detection, Malware analysis

INTRODUCTION

With the speedy development of the net, malware became one amongst the most important cyber threats today. Any package playacting malicious actions, together with info stealing, espionage, etc. are often named as malware. Kaspersky Labs (2017) outline malware as "a sort of trojan horse designed to infect a legitimate user's laptop and visit hurt thereon in multiple ways in which." whereas the variety of malware is increasing, anti-virus scanners cannot fulfill the requirements of protection, leading to variant hosts being attacked. per Kaspersky Labs (2016), half-dozen 563 one hundred forty five completely different hosts were attacked, and 4,000000 distinctive malware objects were detected in 2015. In turn, Juniper analysis (2016) predicts the value of information breaches to extend to $2.1 trillion globally by 2019. Additionally thereto, there's a decrease in the talent level that's needed for malware development, attributable to the high availableness of offensive tools on the net today. High availableness of anti-detection techniques, furthermore as an ability to shop for malware on the black market end for the chance to become associate assaulter for anyone, not looking at the talent level. Current studies show that additional and additional attacks are being issued by script-kiddies or are machine-driven. (Aliyev 2010). Therefore, malware protection of laptop systems is one amongst the foremost vital cybersecurity tasks for single users and businesses, since even one attack may end up in compromised knowledge and spare losses. Huge losses and frequent attacks dictate the necessity for correct and timely detection strategies. Current static and dynamic strategies don't give economical detection, particularly

once handling zero-day attacks. For this reason, machine learning-based techniques are often used. This paper discusses the most points and considerations of machine learning-based malware detection, furthermore as an appearance for the most effective feature illustration and classification strategies.

MALWARE TYPES

To have a better understanding of the methods and logic behind the malware, it is useful to classify it. Malware can be divided into several classes depending on its purpose. The classes are as follows:

Virus: This is the simplest form of software. It is simply any piece of software that is loaded and launched without user's permission while reproducing itself or infecting (modifying) other software (Horton and Seberry 1997).

Worm: This malware type is very similar to the virus. The difference is that worm can spread over the network and replicate to other machines (Smith, et al. 2009).

Trojan: This malware class is used to define the malware types that aim to appear as legitimate software. Because of this, the general spreading vector utilized in this class is social engineering, i.e. making people think that they are downloading the legitimate software (Moffie, et al. 2006).

Adware: The only purpose of this malware type is displaying advertisements on the computer. Often adware can be seen as a subclass of spyware and it will very unlikely lead to dramatic results.

Spyware: As it implies the name, the malware that performs espionage can be referred to as spyware. Typical actions of spyware include tracking search history to send personalized advertisements, tracking activities to sell them to the third parties subsequently (Chien 2005).

Rootkit: Its functionality enables the attacker to access the data with higher permissions than is allowed. For example, it can be used to give an unauthorized user administrative access. Rootkits always hide its existence and quite often are unnoticeable on the system, making the detection and therefore removal incredibly hard. (Chuvakin 2003).

Backdoor: The backdoor is a type of malware that provides an additional secret "entrance" to the system for attackers. By itself, it does not cause any harm but provides attackers with broader attack surface. Because of this, backdoors are never used independently. Usually, they are preceding malware attacks of other types.

Keylogger: The idea behind this malware class is to log all the keys pressed by the user, and, therefore, store all data, including passwords, bank card numbers and other sensitive information (Lopez, et al. 2013).

Ransomware: This type of malware aims to encrypt all the data on the machine and ask a victim to transfer some money to get the decryption key. Usually, a machine infected by ransomware is "frozen" as the user cannot open any file, and the desktop picture is used to provide information on attacker's demands. (Savage, Coogan and Lau 2015).

Remote Administration Tools (RAT): This malware type allows an attacker to gain access to the system and make possible modifications as if it was accessed physically. Intuitively, it can be described in the example of the Team Viewer, but with malicious intentions.

MALWARE DETECTION METHODS

All malware detection techniques can be divided into two types, and it is essential to understand the basics of two malware approaches: static and dynamic malware analysis. As it implies from the name, static analysis is performed "statically", i.e. without execution of the file. In contrast, dynamic analysis is conducted on the file while it is being executed for example in the virtual machine.

Static analysis can be viewed as "reading" the source code of the malware and trying to infer the behavioral properties of the file. Static analysis can include various techniques (Prasad, Annangi and Pendyala 2016) :

1. **File Format Inspection:** file metadata can provide useful information. For example, Windows PE (portable executable) files can provide much information on compile time, imported and exported functions, etc.

2. **String Extraction**: this refers to the examination of the software output (e.g. status or error messages) and inferring information about the malware operation.

3. **Fingerprinting**: this includes cryptographic hash computation, finding the environmental artifacts, such as hardcoded username, filename, registry strings.

4. **AV scanning:** if the inspected file is a well-known malware, most likely all anti-virus scanners will be able to detect it. Although it might seem irrelevant, this way of detection is often used by AV vendors or sandboxes to "confirm" their results.

5. Disassembly: this refers to reversing the machine code to assembly language and inferring the software logic and intentions. This is the most common and reliable method of static analysis.

Another analysis type is dynamic analysis. Unlike static analysis, here the behavior of the file is monitored while it is executing and the properties and intentions of the file are inferred from that information. Usually, the file is run in the virtual environment, for example in the sandbox. During this kind of analysis, it is possible to find all behavioral attributes, such as opened files, created mutexes, etc. Moreover, it is much faster than static analysis. On the other hand, the static analysis only shows the behavioral scenario relevant to the current system properties. For example, if our virtual machine has Windows 7 installed, the results might be different from the malware running under Windows 8.1. (Egele, et al. 2012).

PREVENTION TOOLS:

There are some ways that a deadly disease will infect your laptop. There are several laptop hindrance tools are accessible like Anti-virus software package, firewall, security updates and lots of additional. At an equivalent time, each user cannot use all kinds of tools. Each tool doesn't provide full protection to your laptop. These laptop hindrance tools are delineating as given below;

1. Anti-virus Protection Software: Anti-virus software package will defend you against viruses, Trojans, worms and – counting on the merchandise spyware and different kinds of malware. Most of the people apprehend that Anti-virus software package may be a necessity and most computers go with some kind of program already put in. Anti-virus software package uses a scanner to spot programs that are, or maybe, malicious. Scanners will detect; proverbial viruses, antecedently unknown viruses, suspicious files. This kind of software package will observe and block viruses before they need an opportunity to cause any damage. a decent program will scan for viruses on your drive or any program, files, or documents. If it finds any viruses, it will take away the virus, quarantine it or delete the file safely from your laptop. To be affection, your Antivirus protection software package must be updated often, ideally mechanically. Detection of proverbial viruses depends on frequent change with the latest virus identities.

2. Antispam software: Antispam programs will observe unwanted email and stop it from reaching users'inboxes. These programs use a combination of ways to decide whether or not associate email is probably to be spam. They'll perform in following ways in which like Block email that comes from computers on a block list. this could be a commercially accessible list or a native list of laptop addresses that have sent spam to your company before, block email that includes sure net addresses, check whether or not email comes from a real name or net address. Spammers typically use faux addresses to strive to avoid opposed spam programs, look for keywords or phrases that occur in spam. The program combines all the data it finds to make your mind up the chance of associate email being spam. If the chance is high enough, it will block the email or delete it, relying on the settings you opt for. Antispam software package desires frequent change with new rules that change it to acknowledge the most recent techniques utilized by spammers.

3.Security Patch: A Security Patch is program code that fixes and closes Vulnerabilities in Microsoft software on PCs or servers. Some patches boost security and reliability, and others increase performance or fix problems. Microsoft releases their patches on a monthly basis. In some cases, the vulnerability that has been identified is so severe, that urgent and immediate deployment is essential. Information Systems automatically install new updates to Windows and Office when they come available.

4. Firewalls A firewall prevents unauthorized access to a computer or a network. As the name suggests, a firewall acts as a barrier between networks or parts of a network, blocking malicious traffic or preventing hacking attempts. Firewalls also block some viruses from spreading from computer to computer. They keep an eye on which programs on your computer try to make Internet connections. Firewalls can filter traffic on the basis of the source and destination addresses and port numbers, the type of network traffic, the attributes or state of the packets of information sent.

5. Spyware and Trojan removers This is separate software specifically for removing spyware and other Trojans. It included in the better commercial suites Good Antivirus programs should stop most Trojans but won't help with spyware. A firewall will warn you if something on your system tries to call out and alert you to many Trojans and spyware. However, if you download and install a lot of programs or you want another line of defense, you should get a separate program specifically for detecting and cleaning out Trojans and spyware. There are at least two good free programs, Adware and Spybot Search and Destroy.

CONCLUSION

From the time once the primary virus for PCs was written twenty years past to the current time many thousands of viruses and different malware'email viruses, Trojans, net worm, keystroke loggers – have appeared some spreading worldwide and creating headlines. A bug symptom could be a sign or indication of one thing. Now, there is the range of various styles of bug attacks in our automatic data processing system. Every bug sorts have completely different significance and role to break our pc. There are completely different glorious ways in which of injury done to an automatic data processing system and additionally the cause and result relationship. The harm that an endemic will do your system is indicated by bound

symptoms which will be computer code or hardware based mostly. Supported these there is some mechanism to safeguard info and system resources with regard to confidentiality and integrity. It is important to stay viruses in perspective. They're however one threat to your information and programs. They have not be thought to be mysterious. There are many ways that an endemic will infect your pc. There are several pc interference tools are accessible like Anti-virus computer code, firewall, security updates and lots of additional. At a similar time, each user cannot use every kind of tools. Each tool doesn't provide full protection to your pc.

REFERENCES

1. Olivier Henchiri, Nathalie Japkowicz, A Feature Selection and Evaluation Scheme for Computer Virus Detection, International Conference on Data Mining (2006), pp. 891-895

2. Ward Takamiya and Jocelyn Kasamoto, An Introduction to Computer Viruses, Information Technology Services, University of Hawai, Nov 2000

3. M. Costa, Jon Crowcroft, M. Castro and A. Rowstron, Can we contain Internet worms?, Workshop on Hot Topics in Networks, November 2004

4. Alisa Shevchenko, Malicious code recognition advances, White Paper, Kaspersky Lab, 2008

5. Side effects, Stephanie D

6. Beth Allen, The Spread of Computer Viruses, Accounting and Management Science Seminars Spring, 2008

7. Juergen Haber, What Do Computer Viruses Do and Five Easy Ways To Avoid Infection, Nov 2010

8. Bhaskar Mukherjee, Threats to Digitization: Computer Virus, International CALIBER-2008, 299 – 308

9. Greg Day, A Practical Understanding Of Malware Security, Virus Bulletin Conference October 2005

10. Against infection Defense in Depth Guide, Microsoft Security for arrangement, 2004, ISBN: 0-7356-2155-1

11. Hostile to infection Software - AV An Essential Element in Your IT Security Toolbox, A White Paper by TRUSTIX INC, 2004

12. Sandy Chockey, Susan Adams, Computer Virus Detection 2003, Maricopa County Internal Audit Department, 2003

13. ShenYanmei , XieHong Computer Virus Preventing and Controlling Method Discussion, Proceedings of the Third International Symposium on Electronic Commerce and Security Workshops(ISECS '10)

14. Dr. Waqar Ahmad, Computer Viruses as a Threat to Home Users, International Journal of Electrical and Computer Sciences IJECS, 2010

15. Marshall Brain, Manitoba E-Association's, How Computer Viruses Work, How stuff work, 2010

16. Rizwan Rehman, Dr. G.C. Hazarika, Gunadeep Chetia, Malware Threats and Mitigation Strategies: A Survey, Journal of Theoretical and Applied Information Technology, 2011