MALICIOUS SOFTWARES THREATS AND RISKS

Symptoms and Impacts

Nooh Bany Muhammad, American University of Kuwait, Kuwait

nmuhammad@auk.edu.kw

Abstract— *The current security technologies are faced with various challenges that make protecting critical information difficult. State-sponsored espionage is a problem that highlights the need to protect valuable information from financially and politically motivated threats. Essential information includes data that is required to run the network attached infrastructure in addition to the intellectual property and how it sued to drive innovative solutions and manage businesses. The second challenge of that faces the current security technologies is the issue of hacking of mobile phones and other non-traditional payment systems. In the present world, many financial transactions that are paperless are used in the modern commerce, and thus many malware authors have increased their efforts to steal funds from the consumers. This paper will mainly discuss the different types of malware and their effects on individuals and the society, as well as compare and contrast how advances in technology can lead to more dangers and harms, and progressions in malicious software.*

Keywords; Malware; Risks; Threats; Security.

I. INTRODUCTION

With the advances of technology, it became a must to have daily interactions with computers. It is important to keep up with technology and more important to get the most benefits possible from them. However, with the increase of the use of technology, there lies a world with cyber criminals who are waiting their next oblivious prey. These criminals will plant different vicious methods around the internet to ease their attack, as they catch the next prey who falls into the trick. One of the most important types of attack is malicious software.

Malicious software, commonly known as malware, is a program planted by an agent with a malicious motive to cause unanticipated or undesired effects that bring harm to a computer system. Malware has several 'malicious' intentions as they can be in several forms: worms, viruses, Trojan horses, spyware, key loggers, adware and rootkits, etc. It can steal protected data, delete documents or add software not approved by a user. Malware is considered an enemy to the computer world as it can have various negative effects towards both the computer and the user. The typical example of a computer malicious programs is an advertising supported software package that automatically sends advertisements so as to generate revenue for its author [5]. In most cases, the advertisements are in the user interface of the software or on a screen which is usually presented to the user especially during the installation process. The functions of the adware are designed to analyze the sites that the user visits frequently and offering to advertise pertinent to the nature of the services and goods presented on the sites. The last example of the computer spyware is the Trojan which defines a broad range of malicious software that is commonly used to dupe the internet user of their true nature and end up hacking into their systems.

II. MALICIOUS PROGRAMS

A. Viruses

A virus is a computer program designed to duplicate itself without the user's knowledge or permission, which can severely affect the computer. The virus normally attaches itself to an executable program and systematically replicates itself when the program is run. It is also possible for viruses to spread through documents, script files, and cross-site scripting vulnerabilities in web applications.

There are many harms that come with viruses. Harming host computers and networks are a few, but they are mostly used to steal information, which will ultimately result in them stealing money. When downloading unknown resources from the

internet, the user can also be at a risk of having a virus in their computer. With the expansion of technology, it would be very common that many users have at least had their computers get infected with a virus at least once in their life [6]. Added to that, the fact that people are accepting the global computing world, they are willing to trust unknown resources more and this makes them more vulnerable to attacks.

B. Worms

Worms are notably one of the most common types of malware. It is a malware that can replicate itself through a network; this is usually done by the exploitation of an operating system's vulnerabilities. The impact of worms is usually a degraded performance as they mostly cause harm to their host by consuming bandwidth and overloading web servers. Some of them also contain payloads which also damage host computers. Payloads are pieces of code that are designed to perform impairments to the computers; these vary from stealing data, deleting files or even creating botnets. Worms are occasionally seen as a type of virus, but the principal difference is that worms have the ability to replicate themselves and travel independently while viruses mostly rely on activities that are input by the user, such as opening a file containing a virus or downloading programs from unknown sources that include viruses in them. On the other hand, worms spread by sending numerous emails with attachments that contain worms to users' contacts. Since worms mainly degrade the performance of computers, there would not be anyone who is not affected by this. When it comes to individuals, this can cause frustration as the computer may encounter difficulties and problems involving speed and it can delay any tasks that the user would like to perform on the computer. For larger organizations such as universities, it can lag the computer system as well as cause delays that can interrupt the work.

C. Trojan Horse

A Trojan horse, which is namely renowned as a 'Trojan', is a type of malware disguised as a trusted program, however it contains hidden features permitting it to pass the security mechanisms of a particular system which –when downloaded and installed- allows it to access to view, modify or destroy the user's files. Once an attacker enters an infected computer, the attacker can easily take advantage of the user by monitoring their activities, installing more malware, use the computer in botnets, and potentially steal data such as logins, electronic money or financial information. The Trojan, however, does not duplicate as opposed to the worm for it remains a harmless program (such as in games and other utilities) until it is put into action.

There are many scenarios on how a Trojan horse can enter a computer system, for example, a user decides to download to what seems a trusted email attachment from an unknown user (usually a spammer or a phisher) and the Trojan would be hidden in the attachment. This Trojan would usually have a devious purpose which will exploit the network vulnerabilities that the user might has and most likely be able to steal sensitive information [7]. This does not only concern individuals, as every single user of computers could be affected and this could build up to threats for larger communities. When considering the effects of the Trojan on the users, it would seem like the excessive openness to computing should somewhat be reserved.

D. Key Logger

A key logger is software that's role is to record all keystrokes done by a user. Unlike other types of malicious program, key loggers present no threat to the system itself. However, they can cause serious threats to users as they can be used to intercept passwords and other confidential information entered via the keyboard. As a result, the criminals that assigned the key loggers can get bank account information as well as email address information etc. which can make users at risk of having huge losses. The criminal can basically transfer money from the user's banking account into their own account which leads the user to a huge loss of money. Also, there are confidential information that criminals are able to access (using the users' email accounts) which can lead to more serious consequences than just loss of money. When considering the societal and global effects, key loggers have been detected to be used in both industrial and political spying purposes. Accessing data may include proprietary information and confidential government information which can threaten the security of commercial and governmental organizations. An example would be stealing private encryption keys.

E. Spyware

A Spyware is a software program constructed specifically for gathering personal information about users of the infected system and exposing that data to an unknown transaction through the Internet or computer network while lacking the user's approval. It is a form of malware that's purpose is to secretly spy on user activity without the user's acknowledgement. Through their detecting capabilities, it is possible to monitor the user's activities, collect keystrokes, harvest data such as financial information, logins, account data and more. Spyware also possesses other abilities like altering security settings of a certain software or browsers or interfering with network connections. Spyware propagates by manipulating and exploiting a software's weak areas, combining itself with valid software, or through a Trojan. One of the most harmful effects that occur from spyware is having an identity theft. This means that because of spyware, there is a cyber-criminal pretending to be a user

by using all of the personal information and even their bank account information [8]. This causes many harms and dangers to the user as well as those surrounding the user. When the criminal impersonates a certain user, those who trust the user such as friends or family may send unreliable or personal information to the criminal thinking that they are sending the information to the user.

These software aim to gather information about an organization or a person without their knowledge or consent from a computer when it online. Notably, the software can send information to another entity without the approval of the owner or asserts control over a computer without control of the proprietor. There are several examples of spyware that include system monitors, tracking cookies, Trojans, and adware. First of all, the system monitors are mostly used to keep track of system resources such as the central processing unit usage and frequency, or the free amount of random access memory of a computer. Additionally, they are used to monitor the amount of free space in one or more hard drives and the temperature of the central processing unit and other crucial components in a system [9]. Notably, the monitors are also used to control the networking information of a system such as an internet protocol address and the up to date rates of downloads and uploads in a system [4]. Remarkably, there are more displays that system monitors can display including the date and time of a system, computer name, username, system uptime, fan speed, the amount of power drawn from the power supply and self- monitoring analysis and reporting technology of the hard drives [1]. On the other hand, tracking cookies are additional examples of spyware, and they are texts stored on a personal computer with data sent from a web browser.

Notably, the information in most cases include preferences of the user or contents from a shopping cart. In most cases, tracking cookies are an invasion of privacy of the user, and most of the users prefer deleting them. Additionally, other users feel that the cookies are taking much of the computer space. However, there are many ways in which computer users can delete the tracking cookies.

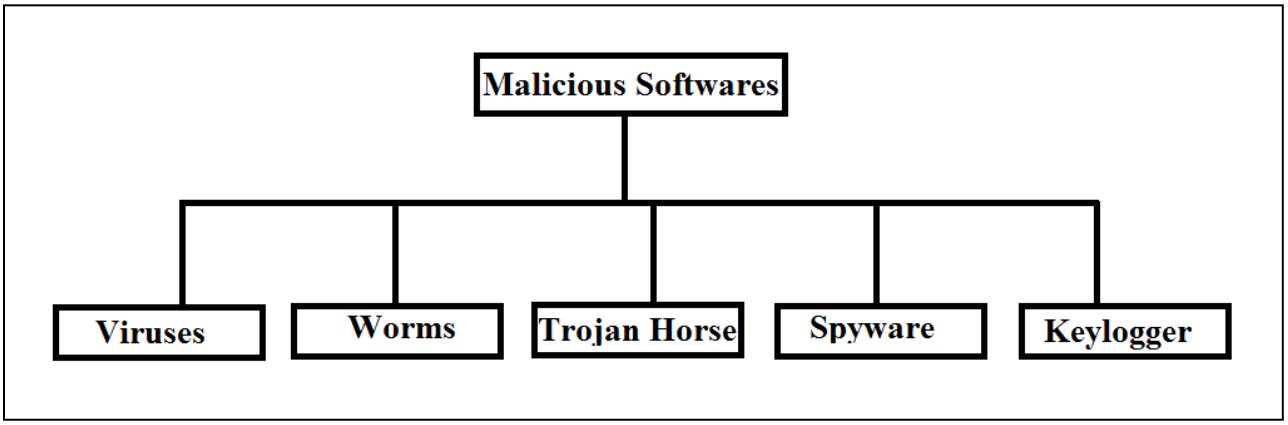

Figure 1. Malicious Software Types.

III. MALWARE SYMPTOMS

Many malicious programs such as spyware are freely available on the internet, and they have simple procedures to download, install, or operate. Notably, many mainstream websites and portal do offer spyware removal programs resulting in a wide choice for the users. However, some disadvantages are related to spyware programs in computer systems.

The free spyware removal programs do not offer a comprehensive preventive or security features, and many of the software are known to contain malicious features that could make the contents of the user's computer, passwords, and other confidential data be lost or making it vulnerable to potential misuse or harm. Additionally, spyware software can collect information about the sites that have been previously visited by the user and thus track the user internet surfing habits. Also, the spyware can harm the user who controls the computer by redirecting web browsers, installing additional software, diverting advertising revenue to a third party, and accessing a website that may contain malicious malware. The most dangerous effect of spyware is to change the settings of the computer, loss of programs, slow connections, and directing the user to different homepages.

Despite the vast differences held by each individual malware installment, they are connected via the similarity of the symptoms they exhibit. To save a computer from malicious software, the user must be cautious of any unusual activity regarded their computers like:

- Constant crashing and freezing.
- Self-reconfiguration.
- Degraded performance of the computer system

- Issues with network connections.
- Slow-paced browsers.
- Altered/deleted files.
- Automatically sent email responses to recipients without user knowledge.
- Sudden appearances of foreign files, icons and programs.

IV. MALICIOUSE SOFTWARE IMPACT ON INDIVIDUALS AND ORGANIZATIONS

The impact of malicious programs on individuals and organizations is felt especially in the field of using information technology for innovation in products and services. Among the key business strategies that are affected by computing include reusability that uses information captured for one purpose and using it for other purposes, portability that takes products and services closer to the user [10]. Additionally, time extension that offers an unsurpassed service, simultaneity that makes information instantly available in several systems, and sequencing that includes parallel processing of databases are added strategies.

A. Impacts on Individuals

When considering the effects of malware on our lives, many measures are taken to ensure the safety and security of our technological devices when they are being used. It is now a necessity to enforce passwords and passcodes to access emails, bank account information as well as access to certain places like factories or company towers. With the continuously increasing popularity of our portable technological devices such as smartphones, laptop and plenty of other web-enabled products, malware and viruses can still very easily infuse harmful effects into them. Malware induces a lot of negative effects on the computer device such as the theft of bank information which can lead of bankruptcy or even identity theft. This strongly suggests that there is a massive issue regarding trust where the entity of humankind will continue to live in paranoia as the lack of trustworthiness results in a life of danger. As the role of hacking is expanding towards our technological devices, it is a duty for us to remain cautious for the case of hacking is only worsening at a world-wide spectrum.

In many instances, the consequences of the spyware activity on a personal computer are hardly detected over time, but in the long run, they end up causing system failure. In severe cases, the user may face up to 50% failure of the system in addition to many stability issues such as hangs and crashes [2]. Difficulty in connecting to the internet is another added problem. Notably, many visits to the professional computer repairers by personal computer owners are caused by problems related to spyware. Particularly, the user finds it difficult to attach the computer malfunctions regarding system performance and stability, and connectivity issues to effects of spyware. Many end up imagining the misbehavior of equipment is caused by connectivity matters related to Windows installation problems, hardware or the effect of a virus. As a result individuals need to protect their devices from malwares.

B. Impacts on Organizations

The effects of malware on companies and organizations can be ruinous. One scenario would be that while the computers contain malicious software, they may decrease performance or even halt their computers which may slow their work or even stop it for some period of time. Another scenario which has a greater impact is: corporate secrets being stolen and sold to competitors, financial information being compromised, internal messages being used to defame high ranking employees, and much more. The larger the company or organization is, the more potential there is for damage.

V. MALWARE PREVENTION AND REMOVAL

There are countless basic procedures that organizations and individual users can carry out to block out malware infections. Certain malware cases require different prevention and treatment processes, but abiding these changes and suggestions will massively stabilize a user's protection from a wider set of malware programs, these methods include installing firewalls and running anti-malware. During the software selection process, it is most preferred to decide on a program that provides tools for detecting, quarantining, and the removal of multiple malware types. Anti-malware software should at least offer protection against viruses, spyware, adware, Trojans, and worms.

When Anti-malware software and a firewall come into unison, it will ensure that all incoming and existing data are scanned and searched for any malware programs and that it can be safely extracted from the system once detected. Other safety routes to take are: being cautious with the installment of files and programs that are downloaded from foreign/unknown sources and

reassuring that all operating systems remain current with vulnerability patches that are used to capture and patch flaws in the security system.

Based on online research and expert's [3][11][12][13][14][15] opinion there are many tips users must follow to protect their data which are:

- Change passwords frequently and don't let the computer save your passwords
- Don't click on email links and disable the preview pane in all inboxes
- Read email in plain text and don't open email attachments
- Never run a program unless it is trusted and read the user Agreement on downloads
- Block untrusted Pop-Ups
- Reject any application asks for additional or different authorities.
- Download and buy applications from trusted stores and avoid free download offers from third-parties sources

IV CONCLUSION

Malicious software is extremely harmful and it keeps increasing over the years. The significance of this topic should never be minimal as having awareness is important to prevent attacks and harms from occurring to our computers. What is currently witnessed is that a lot of computer systems are being attacked whether they concern the individuals, the community and society and even globally. Therefore, it is recommended to have installed a good antivirus or antispyware that is up to date so as to be able to fight malicious software at each time. Also, it is essential to inform the users about the harms of malware and all of their different types so that they do not fall into the trap of installing any malware to their computer systems.

REFERENCES

[1] Axelrod, Warren. "Outsourcing Information Security. Norwood", Artech House, 2012

[2] Bhatnagar, Kartik. Cisco Security. Cincinnati, Ohio, Premier Press, 2010

[3] Mutrux, Zac. "Protecting Your Organization from Spyware, Viruses, and Other Malware." TechSoup.org. Creative Commons Attribution-NonCommercial-NoDerivs 4.0 International License., 12 Feb. 2012. Web. 8 Apr. 2017.

[4] Shim, Jae K. The International Handbook Of Computer Security. Chicago, Ill., Glenlake Pub., 2000..

[5] Laurie, Victor. "An Explanation Of Different Kinds Of Malicious Software (Malware)". Vlaurie.com. N.p., 2017. Web. 11 Apr. 2017.

[6] Villas-Boas, Antonio. "The Company behind the Galaxy S8's Iris Recognition Says It's Superior to the FBI's Fingerprint Tech." Business Insider, 13 Apr. 2017, www.businessinsider.com/samsung-galaxy-s8-iris-scanner-fbi-fingerprint-tech-princeton-identity-2017-4. Accessed 25 Apr. 2017.

[7] Hang, Frederick R. "Is Your Computer Secure?" Science, vol. 325, no. 5940, 2009, pp. 550–551.

[8] Erbschloe, Michael. Trojans, Worms, And Spyware., Amsterdam, Elsevier Butterworth Heinemann, 2014.

[9] Garfinkel, Simson." Practical UNIX And Internet Security. Sebastopol", O'reilly Media, Inc., 2011.

[10] "Strategies For Managing Malware Risks". Msdn.microsoft.com. N.p., 2017. https://msdn.microsoft.com/en-us/library/cc875818.aspx
Web access. 13 Apr. 2017.

[11] Orfano, Finn. "What Are The Effects Of Computer Hacking?". Bright Hub. N.p., 2017. http://www.brighthub.com/computing/smb-security/articles/63719.aspx ,Web aceesed. 21 Apr. 2017.

[12] Gehrmann, Christian. "Bluetooth Security". Boston, Artech House, 2013,.

[13] The Information Security for the Application of IoT Technology : Jia Jiang and Donghai Yang

[14] T. V. Nguyen, N. Sae-Bae, and N. Memon. DRAW-A-PIN: Authentication using nger-drawn pin on touch devices. Computers & Security, Volume 66:115 { 128, 2017.

[15] Benton, Brian. "Infected! 10 Tips How To Prevent Malware On Your Computer". Redshift. N.p., 2017. Web. 23 Apr. 2017.