IOSR Journal of Mobile Computing & Application (IOSR-JMCA)
e- ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 5, Issue 2 (Mar. - Apr. 2018), PP 29-34
www.iosrjournals.org

Analysis of Malware Attack and Strategies for Curbing The Threat

Michael K. Adu[1], Kayode Okanlawon[2], Wakilu O. Adesanya[3] And Rashidat Idris-Tajudeen[4]

[1,2,4] *Department of Computer Science, Federal Polytechnic, Ado-Ekiti, Nigeria*
[3]*Department of Computer Science, Federal College of Agriculture, Akure, Ondo State, Nigeria*
Corresponding Author: Michael K. Adu

Abstract: *Malicious Software otherwise known as Malware is software used or developed by attackers with the intent of disrupting computer operations. It can also be used to gather sensitive information, or to gain access to private computer systems. Today, devastating effects of Malware are not limited to individuals, but also governments, industries and financial institutions. It is very easy to send Malware to targets even at a very remote distance. Most of the users and other beneficiaries of the computer and Information Technology facilities are oblivious of the fact that there are Malware that often bypass their traditional security protection techniques and reside on their computer systems undetected. Users of computer systems face evolving challenges that they are not prepared to deal with. It is very pertinent that these challenges must be attended to with the application of the proper and adequate strategies and technologies. This paper is not only intended to assist stakeholders by creating awareness and bringing to fore the risks involved and other nasty activities associated with Malware in our day-to-day operations with the computer systems, it is also an attempt to bring to the understanding of all, especially security units of organizations and other interested parties, the effective methods and necessary steps to take in order to curb the menace.*

Keywords: *Software, Malicious, Awareness, Methods, Protection.*

Date of Submission: 03-05-2018 Date of acceptance: 18-05-2018

I. Introduction

The major risk in the use and application of the Information and Communication Technology tools especially with regard to the Internet and its associated platforms for communication and social interaction is the malware attack. **Malware**, short for M**alicious** S**oftware**, is software used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software entity. 'Malware' is a general term used to refer to different forms of unfavorable or intrusive software. Malware includes computer viruses, worms, trojan horses, spyware and other malicious programs. Malicious software is used by cybercriminals to disrupt computer operations, steal personal or professional data, bypass installed access controls and cause harm to the host system.

It is an established fact that the technologies of attackers continue to advance in order to remain ahead of security measures being put in place, and they have resulted in the constant invention of new fraud mechanics to evade existing security solutions (Babu, et al 2012). The users remain the major facilitators of malware propagation, and raising awareness alone may not be enough in the efforts at tackling the menace. Understanding the concept, propagation trends and effective methods of tracking attackers are inevitable path to curbing malware attack.

Malware first appeared on Personal Computers in 1986, named Brain A. Brain A was developed in Pakistan by two brothers that wanted to prove that Personal Computer (PC) was not a secured platform, so they created virus that was replicating using floppy disks (Zamparelli, 1998). Malware today is the major challenge and external threat to computer facilities belonging to individuals, industries and government establishments all over the world. The damage cause by malware is enormous and the efforts in term of finance, personnel and time expended on recovery are extensive and huge. The coming of the internet and associated social networks, enable users to create their semi-public profile. Semi-public profile is a profile that some information is public and some is private, it enables communication with those who are friends and thereby build an online community (Acquisti, et al, 2006). Most importantly, it enables direct communication with these associates (pals) without restriction. Therefore large amount of their private information is shared in this social network space. The information shared ranges from bio-data information, contact information, comments, images, videos, et cetera (Benevenuto, et al. 2009). Today, threats to Online Social Networks (OSN) are so pervasive

that even academic community has not been able to provide or even suggest a holistic approach to curb the crimes often associated with online social network. Efforts have been expended on identity protection that has not provided the needed results. In recent studies and from day-to-day experiences, many online social network users expose personal and intimate details about themselves, their friends, and their personality whether by posting photos or by directly providing information such as a home address and a phone number. As the use of online social networks becomes progressively more embedded into the everyday lives of users, personal information becomes easily exposed and abused. Information harvesting, by both the online social networks operators and by third-party commercial companies have recently been identified as a significant security concern (Brenner, et al, 2013). It creates fertile land for attack.

II. Clasification Of Malware

Malware can manifest on host computers in various forms. The difference in manifestation could be in mode of propagation, agent for execution, target of attack and operating platform (IATF 2015), which all together form the basis for categorizing malware.

2.1 Viruses: A virus is a self-replicate program that inserts copies of itself into host programs or data files. Viruses are often triggered through user interaction, such as opening a file or running a program. Viruses can be divided into the following two subcategories:

2,1.1 Compiled viruses: A compiled virus is executed by an operating system. Types of compiled viruses include file infector viruses, which attach themselves to executable programs; boot sector viruses, which infect the master boot records of hard drives or the boot sectors of removable media.

2.1.2 Interpreted viruses: Interpreted viruses are executed by an application. Macro viruses for example take advantage of the capabilities of applications' macro programming language to infect application documents and its templates, while on the other hand, there are scripting viruses that infect scripts that are understood by scripting languages on the operating system.

2.2 Worms: A worm is a self-replicating, self-contained program but unlike virus, it usually executes itself without user's intervention. Worms are divided into two categories:

2.2.1 Network Service Worms: A network service worm takes advantage of vulnerability in a network service to propagate itself and infect other hosts.

2.2.2 Mass Mailing Worms: A mass mailing worm is similar to an email-borne virus but is self-contained, rather than infecting an existing file.

2.3 Trojan Horses. A Trojan horse is a self-contained, non-replicating program that, while appearing to be benevolent, actually has a hidden malicious purpose. Trojan horses either replace existing files with malicious versions or add new malicious files to hosts. They often deliver other attacker tools to hosts.

2.4 Malicious Mobile Code. Malicious mobile code is software with malicious intent that is transmitted from a remote host to a local host and then executed on the local host, typically without the user's explicit instruction.

III. Understanding The Nature Of Malware Today

The characteristic of today's malware that most distinguishes it from previous generations of malware is its degree of customization, encouraged by the internet and the social networks. It has become a minor task for attackers to create their own malware by acquiring malware toolkits and consequently customizing the malware produced by those toolkits to meet their individual needs. Many of these toolkits are available for purchase, while others are open source, and most have user-friendly interfaces that make it simple for unskilled attackers to create customized, high-capability malware.

Many attackers further customize their malware by tailoring each instance of malware to a particular person or small group of people. For example, many attackers harvest information through social networks, then use that affiliation and relationship information to craft superior social engineering malware customization that causes significant problems and makes detection very difficult. This greatly increases the variety of malware that antivirus software and other security controls need to detect and block. When attackers are capable of sending a unique attack to each potential victim, it should not be surprising that largely signature-based security controls, such as antivirus software, cannot keep up with them.

In addition to customization, another important characteristic of today's malware is its stealthy nature. Unlike most malware several years ago, which tended to be easy to notice, much of today's malware is specifically designed to quietly, slowly spread to other hosts, gathering information over extended periods of time and eventually leading to accessing of sensitive data as well as launching many other processes with negative impacts. The term *advanced persistent threats* (APTs) is generally used to refer to such types of malware. APTs may conduct surveillance for weeks, months, or even years, potentially causing extensive damage to an organization with just one compromise. APTs are also notoriously difficult to remove from hosts, often requiring the host's operating system and applications to be reinstalled and all data restored from known good backups.

In summary, today's malware is often harder to detect, more damaging, and harder to remove than previous generations of malware. And there is no indication that this evolution is at an end. When today's hardest malware problems become routine to address, expect new challenges to emerge.

IV. Attacker Tools/Operations On Social Networks

There are different types of attacker tools. They are delivered to host computers by malware. These tools allow attackers to have unauthorized access to or use hosts files and data, or to launch additional attacks (Danezis, 2004). Popular types of attacker tools are as follows:

4.1.1 Backdoors: A backdoor is a malicious program that listens for commands on a certain Transmission Control Protocol (TCP) port. Most backdoors allow an attacker to perform a certain set of actions on a host, such as acquiring passwords or executing arbitrary commands (Pleeger, et al, 1997). Types of backdoors include zombies (better known as bots), which are installed on a host to cause it to attack other hosts, and remote administration tools, which are installed on a host to enable a remote attacker to gain access to the host's functions and data as needed.

4.1.2 Keystroke Loggers: A keystroke logger monitors and records keyboard use. Some require the attacker to retrieve the data from the host, whereas other loggers actively transfer the data to another host through email, file transfer, or other means.

4.1.3 Web Browser Plug-Ins: A web browser plug-in provides a way for certain types of content to be displayed or executed through a web browser. Malicious web browser plug-ins can monitor all use of a browser.

4.1.4 E-mail Generators: An email generating program can be used to create and send large quantities of email, such as malware and spam, to other hosts without the user's permission or knowledge.

4.1.5 Attacker Toolkits: Many attackers use toolkits containing several different types of utilities and scripts that can be used to probe and attack hosts, such as packet sniffers, port scanners, vulnerability scanners, and password crackers.

V. Typical Activities Of Attackers

Considering Figure 1, two modes of operation of malware attackers are conceptualized.

Mode 1: Attacker sends out multiple spam relays.
The spam email is launched on thousands of users' computers
Users' interactions will commence attacks on accessing the mail
Attack takes place. Malware is installed.
Captured data from victims are transmitted to the attacker's server.

Mode 2: Attacker launches websites with Uniform Resource Locator (URL) for victims to click on.
The website for example www.clickme.com is hosted by the attacker
Users visit the sites
Attacker maintains a dropper server, and tailored messages are delivered to the compromised users.
Captured data from victims are transmitted to the attacker's server.

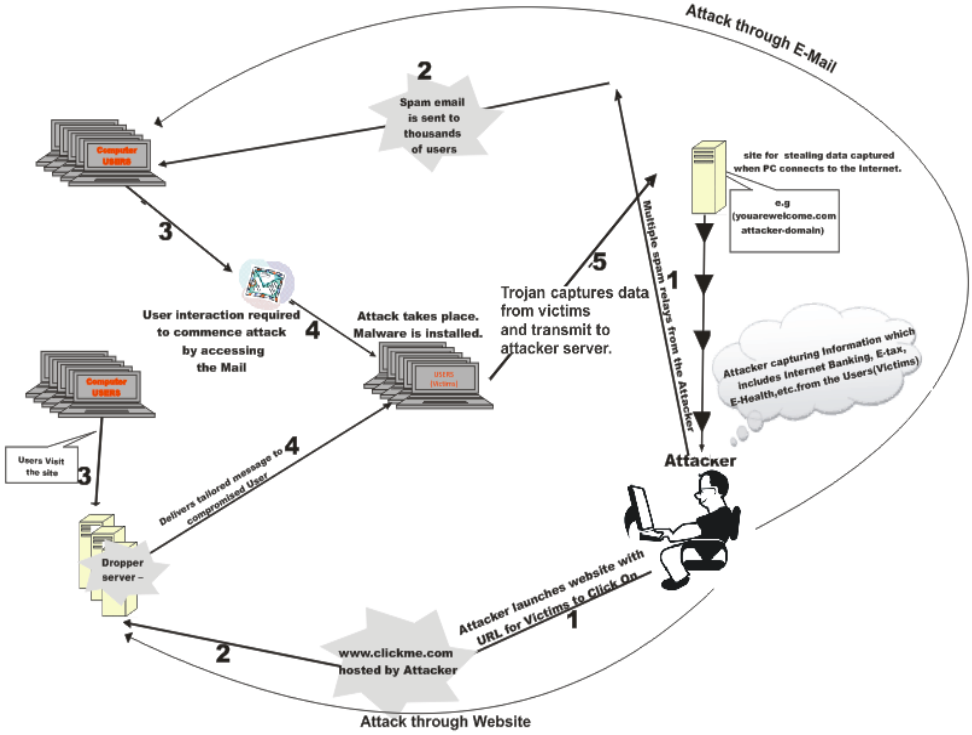

Figure 1: Typical Activities of Attackers.

VI. Strategies For Curbing Malware Attack

It is very important for individuals, governments at all levels, industries and financial Institutions to have a good understanding of the mode of operation of attackers as detailed in Figure 1. The knowledge of this is the first and the most important step in protecting computer systems and other related components against malware attack. The protection should put into consideration the protection of the enclave boundaries and protection of the computing environment. Firewall and Intrusion Detection/Prevention Systems are very common systems for protection of the enclave boundaries.

6.1 Enclave Boundary Protection

The enclave boundary is the point at which the organization's network interacts with the internet. This refers to closed protection arrangement within the computer system.

6.1.1 Firewalls: The main purpose of a firewall is access control. By limiting inbound (from the Internet to the internal network) and outbound communications (from the internal network to the Internet), various attack vectors can be reduced (NIST, 2015a). Acceptable inbound communication types for the organization need to be explicitly defined in the firewall policies. As the firewall is usually one of the first lines of defense, access to the firewall device itself needs to be strictly controlled. Conversely, the firewall also needs to be configured for authorized outbound network traffic.

6.1.2 Intrusion Detection Systems (IDS): The goal of an IDS is to identify network traffic in real time. Most IDSs use signatures to detect port scans, malware, and other abnormal network communications. The ideal placement of an IDS is external to the organization as well as internally, just behind the firewall (NIST 2015b). This way, an organization will have visibility to the traffic approaching the organization as well as the traffic that successfully passed through the firewall. Conversely, there will be visibility on internal traffic trying to communicate external to the network particularly useful for situations where malicious activity originates from inside the firewall.

6.2 Computing Environment

Defending computing hardware and software from attack may be the first line of defense against the malicious *insider* or it may be the last line of defense against the *outsider* who penetrates the enclave boundary defenses. In either case, defending or guiding the computing environment is necessary to establish an adequate information assurance posture.

6.2.1 Authorized Local Network Devices: Ensure that the only devices connected to the organization's network are those items provided by the organization. USB thumb-drives, MP3 players, personal or consultant laptops may be a threat to your environment, therefore if an exception is required by business case, the owner should ensure the device is free of malware before being allowed to connect to the network.

6.2.2 Operating System Patching/Updating

Organizations should have a documented *patching* policy as well as a systematic, accountable, and documented set of processes and procedures for handling patches. The patching policy should specify what techniques an organization will use to monitor vendor sites for new patches and vulnerabilities and which personnel will be responsible for monitoring, retrieving and implementing those patches. It should also include a methodology for testing and safely installing patches. Pay particular attention to vendor reboot requirements as part of the patch process. Failure to execute this requirement can make computer systems vulnerable to attack.

6.2.3 Operating System Hardening

Operating systems should be hardened to improve the ability to withstand attacks.

6.2.4 Anti-Virus Updating

`New viruses are discovered on daily basis. It is therefore recommended to set anti-virus applications to automatically update signature files and scan engines whenever the vendor publishes updates. Mobile and remote users should be required to connect at least weekly and if possible daily to obtain updated signatures. The organization should monitor anti-virus console logs to correct any systems that failed to be updated.

6.2.5Change Control Process

Implement a change control process to document and review firewall and other network changes before they are implemented.

6.2.6 Host-based Firewall

Consider implementing host-based firewalls running on each internal computer and especially laptops assigned to mobile users. Aside from the primary firewall functionality, many host-based firewalls have application hashing capabilities. This is helpful to identify applications that may have been trojanized after initial installation. It is also useful to validate whether an application has been legitimately updated or modified.

6.2.7Vulnerability Scanning

Routine vulnerability scanning is a valuable practice for every organization. Host scanning mimics the malicious network activity that networked hosts may encounter. Consequently, scan results can indicate which hosts are vulnerable to various types of attacks. These devices should be targeted by system administrators for immediate patching and remediation.

VII. Conclusion

The fact that malware writers are becoming more skillful in developing unwanted codes, there are several steps individuals, governments at all levels, industries, most especially financial institutions could take prior to an infection in order to mitigate the attack. This paper has brought to fore the concept of malware and the various forms. The protection mechanisms against malware attack. Most importantly, the mode of operations of the attackers is practically opened-up. This is a necessary step in order to have proper understanding and prepare stakeholders to identifying and guiding against any form of malware attack. The two levels of protection, the enclave boundaries and protection of the computing environment should be adhered to in any installation to properly safe guide applications and data.

References

[1]. Acquisti A, et al (2006), "Imagined Communities Awareness, Information Sharing and Privacy on the Facebook" in 6th Workshop on Privacy Enhancing Technologies.
[2]. Babu M. et al (2012), "What is Cybercrime"http://www.ncpc.org/resources/files/pdf/Internet-safety.
[3]. Benevenuto, F. et al (2009), "Detection Spammers and Content Promoters in Online Video Social Networks", In proceedings of the 32nd International ACM SIGIR Conference on Research and Development in Information Retrieval, pages 620-627. ACM , 2009.
[4]. Brenner J et al (2013), "Online Adults are Social Networking Site Users", http://pewinternet.org/Reports/2013/social-networking - sites/Findings.aspx,2013
[5]. Danezis G. (2004), 'Better Anonymous Communications' PhD thesis, University of Cambridge, 2004.
[6]. IATF (2015), Information Assurance Technical Framework Manual, available at http://www.iatf.net/framework_docs/version-3_1/zipfile.cfm?chapter=version-3
[7]. NIST (2015a), Computer Security Incident Handling Guide :available at http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

[8]. NIST (2015b), Guidelines on Firewalls and Firewall Policy: available **at**http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf
[9]. Pleeger, C. (1997), Is there a security problem in Computing? Security in Computing, Chapter 1, 1-19.
[10]. Zamparelli, R. (1998), Digital Distribution Models and copyright enforcement, http//www.ftp.cogsci.ed.ac.uk/pub/roberto/diglib.ps.

Michael K. Adu. " Analysis of Malware Attack And Strategies For Curbing The Threat." IOSR Journal of Mobile Computing & Application (IOSR-JMCA) 5.2 (2018): 29-34.