National College of Ireland

Assignment Submission Sheet – 2019/2020

Student Name:	Somesh Saxena		
Student ID:	X18176895		
Programme:	M.Sc Cyber Security	**Year:**	2019
Module:	Security Fundamentals		
Lecturer:	Mr. Vikas Sahni		
Submission Due Date:	13th October,2019		
Project Title:	Malwares		
Word Count:	2765		

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature: Somesh Saxena

Date: 13th October,2019

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**
5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

A Thorough Analysis of Malwares

Somesh Saxena
M.Sc. Cybersecurity
School of Computing
National College of Ireland
Dublin, Ireland
x18176895@student.ncirl.ie

***Abstract*—Malware or malicious software's is a program code that seeks to invade, damage computer systems or networks, mobiles phones taking complete or partial control over a device. This paper discusses detailed introduction of malware analysis The paper will begin with an introduction describing the various types of malware. Different types of malware described include Virus, Worms, Trojans, Adware, Spyware, Backdoors and Rootkits that can disastrously affect a Microsoft Windows operating system. Whilst discussing the abovementioned, we also briefly examine the devices and the systems that are most susceptible to getting exploited by malwares.**

Keywords—virus, worms, exploit, vulnerability, ransomwares

I. Introduction

The need for malwares analysis increases as the damage caused by malwares increases. Malware is all about making money off you implicitly. Although malware cannot damage the physical hardware of systems or network equipment, it can steal your data, encrypt, or delete your data, alter or hijack core computer functions, and spy on your computer activity without your knowledge or permission. In today's world, the amount of data an individual or organization has access to serves as a determining factor in establishing their value in the market. With an ever-increasing production of data on a daily basis and the perpetually dropping costs of digital storage media, collection of data by different entities seem rather natural for multiple purposes ranging from behavior analysis, trend modelling, estimation of the probability of situations and much more. However, it is mandatory for these entities to handle such sensitive information with care because if this information lands in the wrong hands, it can be exploited for monetary benefit, fame in the black-hat hacker community, social profiling to enforce outcomes, etc.

Malware does the damage as it is implanted in such a way that target's a computer and can take the form of and directly executables code, scripts, and any other forms of data. Some major types of malwares are computer viruses, worms, trojan horses, ransomwares, spyware, adware, scareware, etc. Malware has some malicious intent, acting against the interest of the computer user, and does not include software that causes unintentional harm due to some deficiency. The strategy for protecting against malwares is to prevent harmful software's from gaining access to the target computer. For this reason only antivirus software's, firewalls, Malwarebytes, and other strategies are used to help protect against the introduction of malwares.

Some high-profile malware attacks included:

- ILOVEYOU, a worm that spread like wildfire in 2000 and did more than $15 billion in damage.
- SQL Slammer, which ground internet traffic to a halt within minutes of its first rapid spread in 2003.
- Conficker, a worm that exploited unpatched flaws in Windows and leveraged a variety of attack vectors – from injecting malicious code to phishing emails – to ultimately crack passwords and hijack Windows devices into a botnet.
- Zeus, a late '00s keylogger Trojan that targeted banking information.
- CryptoLocker, the first widespread ransomware attack, whose code keeps getting repurposed in similar malware projects.
- Stuxnet, an extremely sophisticated worm that infected computers worldwide but only did real damage in one place: the Iranian nuclear facility at Natanz, where it destroyed uranium-enriching centrifuges, the mission it was built for by U.S. and Israeli intelligence agencies.

II. Business Impact

Malwares exploits generally result in massive financial losses for the industry or the loss of their reputation in the market. Examples of situations where malwares are exploited include, but are not limited to, steal your data, encrypt, or delete your data, alter or hijack core computer functions, and spy on your computer activity without your knowledge or permission, data breaches, and manipulation, etc.

When discussing malware, it is vital for the reader to have an understanding of cost of malware infections that occur in organizations. According to Computer Economics 2007 Malware Report, malware infections in 2006 cost $13.3 Billion dollars. Although the trend over the last two years is a down turn in the cost of malware infections, the cost of malware should concern companies of any size. The report states two factors for the reduction in malware infections cost, the wider spread deployment of Anti-Malware applications, and malware targeted at specific organizations and people (Computer Economics Online, 2007).

The inconvenience of data loss can have even bigger implications for your business when a large amount of data is lost:

- 94 percent of companies that experience severe data loss do not recover.
- 51 percent of these companies close within two years of the data loss.
- 43 percent of these companies do not reopen again.
- 70 percent of small firms go out of business within a year of a large data loss incident.

Leaving data unprotected is an expensive risk to take — A study in the year 2014 revealed that 20 percent of companies who experienced data loss from outages said it cost them between $50,000 and $5 million.

III. Types Of Malwares

- Virus:

A computer virus is an instance of malware that, when executed, replicates itself by inserting its own code into data files (often in the form of rogue macros), "boot sectors" of hard drives or SSDs, or other computer programs. Like biological viruses, computer viruses require hosts in order to spread. While viruses still inflict tremendous damage, the majority of serious malware threats today arrive in the form of Trojans and worms. (Note: The plural of computer virus is accepted as "viruses," even if one uses "viri" as the plural for a biological virus.)

- Worms

A computer worm is a standalone piece of malware that replicates itself without the need for any host in order to spread. Worms often propagate over networks by exploiting security vulnerabilities on target computers and networks. Because they normally consume network bandwidth, worms can inflict harm even without modifying systems or stealing data.

- Trojans

A Trojan (or Trojan horse) is malware disguised as non-malicious software or hidden within a legitimate application or piece of digital data. Trojans are typically spread by social engineering - for example, by tricking people into clicking a link, installing an app, or running some email attachment - and, as such, unlike viruses and worms, Trojans typically do not self-propagate - instead, they rely on human involvement.

- Ransomware

Ransomware is malware that demands that a ransom be paid to some criminal in exchange for the infected party not suffering some harm. Ransomware often encrypts user files and threatens to delete the encryption key if a ransom is not paid within some relatively short period of time, but other forms of ransomware involve a criminal actually stealing user data and threatening to publish it online if a ransom is not paid. Ransomware is most often delivered as a Trojan or a virus, but can be, and has been, also been packaged in a worm.

- Scareware

Scareware is malware that scares people into making some purchase. One common example is malware that displays a message on a device that the device is infected with some virus that only a particular security package can remove, with a link to purchase that "security software."

- Spyware

Spyware is software that surreptitiously, and without permission, collects information from a device. Spyware may capture a user's keystrokes (in which case it is called a keylogger), video from a video camera or audio from a microphone, screen images, etc. Some technologies that might technically be considered spyware if users have not been told that they are being tracked are in use by legitimate businesses; they include beacons that check if a user loaded a particular web page, and tracking cookies installed by websites or apps.

- Cryptocurrency Miners

Cryptocurrency mining malware is malware, that, without permission of a device's owner, uses the device's computing power to generate new units of a particular cryptocurrency (which it gives to the criminals operating the malware) by completing complex math problems that require significant processing power to solve.

- Adware

Adware is software that generates revenue for the party operating it by displaying online advertisements on a device. Adware may be malware - that is, installed and run without the permission of a device's owner - or may be a legitimate component of software (for example, installed knowingly by users as part of some free, ad-supported package.)

- Blended Malware

Blended malware is malware that utilizes multiple types of malware technology as part of an attack - for example, combining features of Trojans, worms, and viruses.

- Zero Day Malware

Zero Day malware is any malware that exploits a vulnerability not previously known to the public or to the vendor of the technology containing the vulnerability.

IV. Malwares Defence

To protect an network there are four layers of defense that need to be installed :

- Firewall System
- Web Filtering System
- Intrusion/Prevention Detection System (IDS/IPS)
- Host Base Intrusion Prevention System (HIPS)

Incident Response is an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs. Incident Response Plans should not be created during a security incident nor should one person be assigned to develop an Incident Response Plan. Incident response should be the responsibility of different members from different groups in an organization. Management buy-in is essential for an Incident Response Plan to work and an Incident Response team to be successful.

The six steps of incident response process follows:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

Stay vigilant. Pay particular attention if you see a domain name that ends in an odd set of letters, i.e., something other than com, org, edu, or biz, to name a few, as they can be an indicator for risky websites.

For all your devices, pay close attention to the early signs of malware infection to prevent them from burrowing in. Avoid clicking on pop-up ads while browsing the Internet. Stay away from opening unsolicited email attachments or downloading software from untrustworthy websites or peer-to-peer file transfer networks.

Make sure your operating system, browsers, and plugins are always up to date, because keeping your software patched can keep online criminals at bay. For mobile users, only download apps from Google Play Store (the App Store is the iPhone’s only choice). Every time you download an app, check the ratings and reviews first. If it has a low rating and a low number of downloads, it is best to avoid that app. Do not download apps from third-party sources. The best way to make sure of this is to turn off this function on your Android phone. Go to Settings on your Android device and open up the Security section. Here, make sure Unknown Sources is disabled to avoid installation of apps from marketplaces other than the Play Store.

Do not click on strange, unverified links in emails, texts, and WhatsApp messages of unknown origin. Strange links from friends and contacts should be avoided too unless you have verified it to be safe. To keep their businesses safe, organizations can prevent malicious apps from threatening their networks by creating strong mobile security policies and by deploying a mobile security solution that can enforce those policies. This is vital in the business environment that exists today—with multiple operating systems at work under multiple roofs.

Finally, get yourself a good anti-malware program. It should include layered protection (the ability to scan and detect malware such as adware and spyware while maintaining a proactive real-time defense that can block threats such as ransomware). Your security program should also provide remediation to correct any system changes from the malware it cleans, so everything goes back to normal.

Use Antivirus Software:
Antivirus software can be effective at combating basic, “non targeted" malware that might be used by criminals against hundreds, or even thousands, of targets. However, antivirus software is usually ineffective against targeted attacks, such as the ones used by the Chinese Government to compromise USA Defense. EFF recommends using antivirus software on your computer and your smartphone, though we cannot recommend any particular antivirus products as being superior to others.

Be Wary of Suspicious Attachments:
The best way to avoid being infected with *targeted* malware is to avoid opening suspicious documents and installing the malware in the first place. People with more computer and technical expertise will have somewhat better instincts about what might be malware and what might not be, but well-targeted attacks can be very convincing.

If you are using Gmail, open suspicious attachments in Google Drive rather than downloading them—this may protect your computer from infection. Using a less common computing platform, like Ubuntu or ChromeOS, significantly improves your odds against many malware delivery tricks, but will not protect against the most sophisticated adversaries.

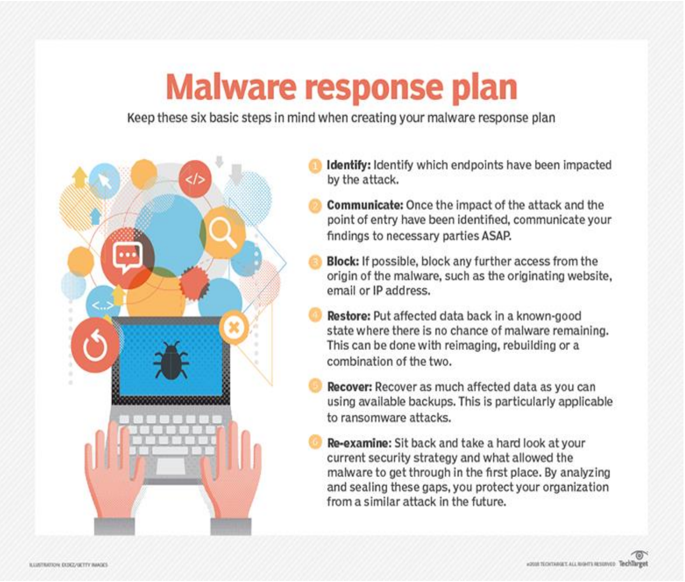
Run Software Updates
As new vulnerabilities are discovered in software, companies can fix those problems and offer that fix as a software update, but you will not reap the benefits of their work unless you install the update on your computer.

Configure laptops, workstations, and servers so that they will not auto-run content from USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, Firewire devices, external serial advanced technology attachment devices, mounted network shares, or other removable media.

Deploy network access control tools to verify security configuration and patch-level compliance before granting access to a network. All attachments entering an e-mail gateway should be scanned and blocked if they contain malicious code or, where appropriate, file types unneeded for the business.

Employ automated tools to continuously monitor workstations, servers, and mobile devices for active, up-to-date anti-malware protection with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality.

Employ anti-malware software and signature auto update features or have administrators manually push updates to all machines on a daily basis.



Malware response plan

Keep these six basic steps in mind when creating your malware response plan

1. **Identify:** Identify which endpoints have been impacted by the attack.
2. **Communicate:** Once the impact of the attack and the point of entry have been identified, communicate your findings to necessary parties ASAP.
3. **Block:** If possible, block any further access from the origin of the malware, such as the originating website, email or IP address.
4. **Restore:** Put affected data back in a known-good state where there is no chance of malware remaining. This can be done with reimaging, rebuilding or a combination of the two.
5. **Recover:** Recover as much affected data as you can using available backups. This is particularly applicable to ransomware attacks.
6. **Re-examine:** Sit back and take a hard look at your current security strategy and what allowed the malware to get through in the first place. By analyzing and sealing these gaps, you protect your organization from a similar attack in the future.

ILLUSTRATION: DXDIZ/GETTY IMAGES

CONCLUSION

The reader should now have a basic understanding of malware analysis as well as a view of the exciting and ever evolving field of malware analysis. Throughout the paper, critical elements have been discussed which began with the key terms of malware analysis. This purpose has been two-fold: to allow the reader to see the underlying's of how malware analysis fits into an organizations' Incident Response Plan as well as shed light on the value malware analysis brings to an organization. By defining and identifying malware analysis, tools used to perform the analysis, an introduction to malware analysis has been provided. Detailed methodology is outlined so that the reader can perform a successful analysis on malware, as well as build defenses with information gathered in the analysis to protect their organization utilizing the defense-in-depth philosophy. However, this does not imply that one should not incorporate security features in an application. It only tries to highlight the fact that given enough time, testing and knowledge, an attacker will eventually be able to bypass any specific security mechanism present in an application. This is the sole reason why new exploits and vulnerabilities are discovered on a daily basis. Such discovery only helps strengthen the standards of implementations of security mechanisms employed, after its public disclosure. And to achieve that, one must set up proper logging services to study, and take necessary measures to counteract the exploit.

ACKNOWLEDGMENT

I want to thank the authors of the referred links for providing me with relevant information for me to be able to complete this CA Assignment well within time.

I would also like to thank my lecturer Mr. Vikas Sahni for allotting me this fascinating topic that encompasses multiple domains of cyberattacks. This topic helped get me up to speed with the current affairs in the cybersecurity world.

REFERENCES

[1] Malwarebytes. (2019). *Malware definition – What is it and how to remove it*. [online] Available at: https://www.malwarebytes.com/malware/ [Accessed 12 Oct. 2019].

[2] Sans.org. (2019). *SANS Institute: Reading Room - Malicious Code*. [online] Available at: https://www.sans.org/reading-room/whitepapers/malicious/paper/2103 [Accessed 13 Oct. 2019]

[3] Sans.org. (2019). *SANS Institute: Reading Room - Malicious Code*. [online] Available at: https://www.sans.org/reading-room/whitepapers/malicious/malware-analysis-introduction-2103 [Accessed 13 Oct. 2019].

[4] En.wikipedia.org. (2019). *Malware*. [online] Available at: https://en.wikipedia.org/wiki/Malware [Accessed 13 Oct. 2019].

[5] Consolidated Technologies, Inc. (2019). *Data Loss: Causes of it, Effects on Businesses & How to Prevent*. [online] Available at: https://consoltech.com/blog/10-common-causes-of-data-loss/ [Accessed 13 Oct. 2019].

[6] Fruhlinger, J. (2019). Malware explained: Definition, examples, detection and recovery. [online] CSO Online. Available at: https://www.csoonline.com/article/3295877/what-is-malware-viruses-worms-trojans-and-beyond.html [Accessed 13 Oct. 2019].

[7] Ibm.com. (2019). [online] Available at: https://www.ibm.com/downloads/cas/L5OLVZ0V [Accessed 13 Oct. 2019].

[8] Security.uci.edu. (2019). *Malware Defenses*. [online] Available at: https://security.uci.edu/security-plan/plan-control5.html [Accessed 13 Oct. 2019].

[9] SearchSecurity. (2019). *What is Malware? - Definition from WhatIs.com*. [online] Available at: https://searchsecurity.techtarget.com/definition/malware [Accessed 13 Oct. 2019].

[10] Cdn.ttgtmedia.com. (2019). [online] Available at: https://cdn.ttgtmedia.com/rms/onlineimages/disaster_recovery-malware_plan_desktop.png [Accessed 13 Oct. 2019].