ASH1925014M

by Iftekhar Efat

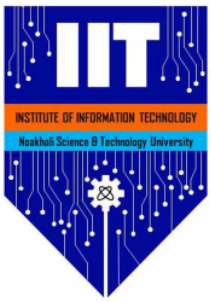
Submission date: 13-Mar-2022 01:17AM (UTC-0500)
Submission ID: 1782983544
File name: ASH1925014M.pdf (210.45K)
Word count: 2032
Character count: 10176

Infiltrating a Mac OS X operating system

Abdullah AL Tahmid
ASH1925014M

March 13, 2022

Report submitted for **SE2206: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University



Project Area: **Information Security .....**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

In submitting this work I am indicating that I have read the University's Academic Integrity Policy. I declare that all material in this assessment is my own work except where there is clear acknowledgement and reference to the work of others.

I give permission for this work to be reproduced and submitted to other academic staff for educational purposes.

OPTIONAL: I give permission this work to be reproduced and provided to future students as an exemplar report.

1 Introduction

This paper give knowledge about infiltrating mac operating system X operating system.

1. Give broad knowledge about infiltrating.
2. Describe infiltrating mac Os X operating system.
3. Describe different threats and vulnerabilities of MAC OS
4. How to protect MAC OS

The intention is that we can understand about infiltrating.
Let's discuss infiltrating. Here the question arises what is infiltrating?

Infiltrating is entering or gaining access to (an organization, place, etc.) surreptitiously and gradually, especially in order to acquire secret information.

In other words, we can say that an Infiltration is a piece of malicious software that attempts to enter and/or damage a user's computer.
As we know an operating system (OS) is system software that manages computer hardware, software resources, and provides common services for computer programs. So this is the core of computers. There are various types of OS available now a day's. Like Microsoft Windows, MAC OS, Linux, Unix etc.

In less than three minutes, a Windows 10 laptop can be compromised. A hacker may delete all antivirus software, create a backdoor, and grab camera images and passwords, among other highly sensitive personal data, with just a few keystrokes.

Mac OS X operating systems are based on UNIX. Mac OS gives us a great protection from unauthorized access in our system. It has several layer of security :

- Apple antivirus : MAC OS includes its own antivirus software built in.
- Privacy and phishing : Apple's web browser, Safari also offers various ways of protecting you online.
- Safe surfing : Mac OS protects your security online also protects your privacy.
- Password protections : Mac Os

With over 10 million users and one million new Macs supplied each quarter, Apple's Mac OS X is the most popular Unix-based operating system currently available. Apple has a distinct focus on both the individual and business markets. [1]

Though MAC OS gives us great security protection there have been cases where Macs have been accessed by hackers. So it is not totally secure.

2 Background

Back in 1982, one of the first viruses was developed for the Apple II computer. The malware was quite innocuous, displaying a rather infantile poem on the screen. The computer's built-in security, on the other hand, had been compromised.

Besides this, nearly 30,000 Apple Mac Books Are Hacked in the Expansive Malware Campaign.

Missing "," ETS

According to Ars Technica, spyware that went undiscovered for a long time has been discovered on roughly 30,000 Macs throughout the world. This spyware, dubbed "Silver Sparrow," is extremely intriguing.

Malware-infected Macs are set up to check a control server every hour to see if there are any new commands or programs to run. Researchers have yet to see any payload delivered by this virus, implying that they have no idea what this software's purpose is.

That means there's a chance that it's commands could be unleashed once some unknown condition is met.

Confused ETS

The fact that the malware is programmed to self-destruct is much more intriguing. 'High-stealth operations' are normally reserved for this type of capability.

2.1 What Types of Macs Were Targeted?

What's more shocking is that this spyware was designed to function on Apple's new M1 CPU. When you consider that these chips were only released in late 2020, it's quite astounding.

Silver Sparrow is a "potentially serious threat," according to Red Canary research analysts.
12 Silver Sparrow has been identified in over 153 territories, with higher populations in the United States, Canada, France, the United Kingdom, and Germany.

2.2 Should You Be Worried?

Silver Sparrow has yet to cause any actual damage or deliver any malicious payloads, despite its classification as a "reasonably dangerous challenge." 'Apple has revoked the certifications of the developer accounts used to sign the packages,' an Apple spokeswoman informed Ars Technica. This must make it impossible for fresh devices to become infected.

3 Mac OS X Vulnerability

A series of high-impact security flaws have been discovered as a result of research, allowing a sandboxed malicious program allowed by the Apple Stores to get unauthorized access to other apps' sensitive data. We discovered that the malware may use the inter-app interaction services, such as the keychain, WebSocket, and connection on OS X, and URL Scheme on the MAC OS and iOS, to steal personal information including iCloud, email, and bank passwords, as well as the Evernote secret token. Further, the design of the app sandbox on OS X was found to be vulnerable, exposing an app's private directory to the sandboxed malware that hijacks its Apple Bundle ID. As a result, sensitive user data, like the notes and user contacts under Evernote and photos under WeChat, have all been disclosed. Fundamentally, these problems are caused by the lack of app-to-app and app-to-OS authentications. To better understand their impacts, we developed a scanner that automatically analyzes the binaries of MAC OS and iOS apps to determine whether proper protection is missing in their code. We proved the pervasiveness of the flaws among high-impact Apple programs by running it on hundreds of binaries. Because the faults may not be quickly remedied, we created a simple software that detects exploit attempts on OS X, assisting in the protection of vulnerable programs while the issues are being resolved. [2]

3.1 MAC OS Threat

Figure 1: MAC OS Threat

Although it is relatively rare compared to Windows, there have been instances where hackers have gained access to Macs.

As you can see from our rundown of the many risks affecting macOS, this can take various forms, and there are various varieties of Mac malware that have been

detected 'in the wild' on Macs: Viruses, malware, and security issues for Mac. Malware has even been discovered on the M1 Mac - read about Silver Sparrow and the first malware case affecting M1 Macs.

Below, we'll go over the types that are most relevant to Mac hacking:

Cryptojacking: This is where someone uses your Mac's processor and RAM to mine cryptocurrency. If your Mac has slowed right down this could be the culprit.

Spyware: Hackers try to obtain private information about you here, such as your log in credentials. They might perform key loggers to track what you enter so they can log into your accounts later. The OSX/OpinionSpy spyware, for example, was taking data from infected Macs and selling it on the dark web in one case.

Ransomware: Some criminals try to extort money from you by using Ransomware. Hackers could have encrypted files on Macs in cases like KeRanger and then demand money to decrypt them. Fortunately, security researchers discovered KeRanger before it infected Macs, allowing it to be removed before it became a severe problem.

Botnet: In this scenario, your system becomes a spam machine commanded from afar. In the case of the OSX botnet Trojan Horse, Over 600,000 Mac systems have been flashed back.

Proof-of-concept: The danger is sometimes a proof of concept based on a loophole or vulnerability in Apple's programming, rather than a real threat. While this is a less serious issue, the concern is that if Apple does not act quickly enough to shut the hole, criminals may exploit it. In one case, Google's Project Zero team created Buggy Cos, a proof-of-concept that exploited a weakness in macOS' memory manager to get access to elements of the operating system.

Port exploits: It isn't always the case that the attack was made feasible by malware installed on the Mac. Macs have been hacked in the past after anything was connected into a port. It's likely that Macs can be hacked through the USB and Thunderbolt ports, which is a good reason to be cautious about what you plug into your Mac and never leave it unattended. In the checkm8 attack, for example, hackers may have had access to the T2 chip by plugging in a modified USB-C cable. Similarly, a significant vulnerability with the Thunderbolt interface may have given a hacker access to a Mac in the case of Thunderspy.

4 How to protect your Mac from hackers ?

There's no need to fear because MAC OS is a fairly secure operating system, but there are a few things you can do to decrease your chances of being hacked.

1. The first is to try to only download software from either the Mac App Store or the official websites of manufacturers.
2. You should also avoid clicking on links in emails - just in case they lead you to spoof websites and malware.
3. Don't use USB cables, other cables, or memory sticks, that if you can't be sure that they are safe.
4. When you are browsing the web surf in private or incognito mode.
5. If you ever receive a ransomware request or a phishing email do not respond as all this does is confirm that you exist.
6. Another thing to remember is to make sure you get MAC OS updates as soon as they are released, as they usually include security fixes. In fact, you can set up your Mac to get such updates automatically. In System Preferences ¿ Software Update, select Automatically keep my Mac up to date and turn on Automatic Updates.
7. Finally, a specialised security software package should be considered. In top Mac antivirus, you'll find our pick of the current solutions. Intego Mac Internet Safety X9 is our current favorite, although we also prefer McAfee Total Protection 2021 and Norton 360 Deluxe.
8. Consider utilizing a password manager, which will allow you to have several, complex login details across all of your accounts without having to know them. LastPass, 1Password, and NordPass are our top picks in this category.

5 Conclusion

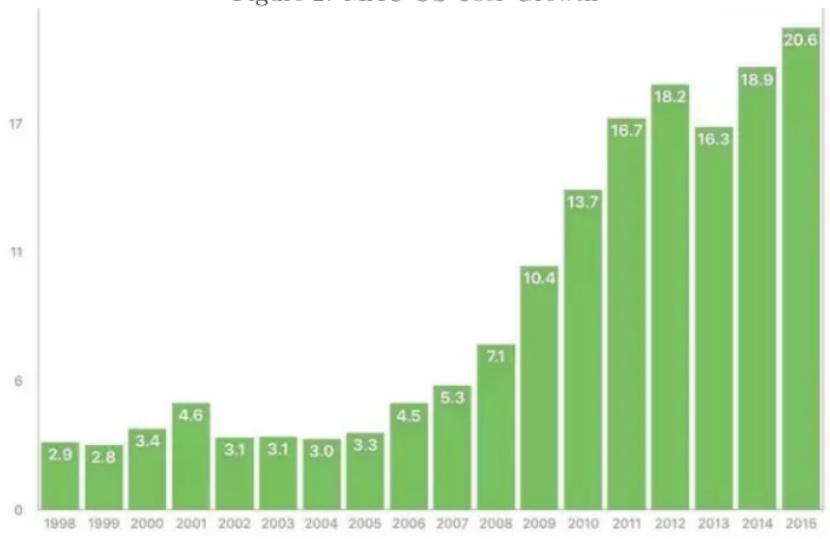
Here we can conclude that no system is totally safe or secure from hackers. Different companies apply different strategies to protect their system and they continuously improve their security system.

They regularly check their security systems and try to find out the system's vulnerability. If there is any issue found related to security or system vulnerability immediately they take respective steps to solve the problem.

Day by day new technology is being invented to secure our system. This new technology is more secure and more powerful than the older version. And they give better security than the old technology.

OS X malware (formerly an uncommon occurrence) is now more widespread than ever as Mac OS X grows in popularity. As a result, information security and spyware analysts must have a complete knowledge of OS X and whether it can be exploited by persistent, harmful programs.

Figure 2: MAC OS User Growth



References

[1] Brad Arkin, Scott Stender, and Gary McGraw. Software penetration testing. *IEEE Security & Privacy*, 3(1):84–87, 2005.

[2] Luyi Xing, Xiaolong Bai, Tongxin Li, XiaoFeng Wang, Kai Chen, Xiaojing Liao, Shi-Min Hu, and Xinhui Han. Unauthorized cross-app resource access on mac os x and ios. *arXiv preprint arXiv:1505.06836*, 2015.

ASH1925014M

ORIGINALITY REPORT

38%	35%	9%	10%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.macworld.co.uk Internet Source	20%
2	cps-vo.org Internet Source	6%
3	Submitted to University of Adelaide Student Paper	4%
4	dl.acm.org Internet Source	1%
5	Marteau, L.. "Mac OS X & security - an overview", Network Security, 200505 Publication	1%
6	www.bongos.net.au Internet Source	1%
7	answersdrive.com Internet Source	1%
8	Submitted to Southern New Hampshire University - Continuing Education Student Paper	1%
9	Submitted to Chamblee High School	

	Student Paper	1%
10	Luyi Xing, Xiaolong Bai, Tongxin Li, XiaoFeng Wang, Kai Chen, Xiaojing Liao, Shi-Min Hu, Xinhui Han. "Cracking App Isolation on Apple", Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15, 2015 Publication	1%
11	www.coursehero.com Internet Source	1%
12	en.unionpedia.org Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

ASH1925014M

PAGE 1

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 2

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Sentence Cap. Remember to capitalize the first word of each sentence.

Possessive This word may be a plural noun and may not need an apostrophe.

Missing "," You may need to place a comma after this word.

Prep. You may be using the wrong preposition.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Article Error You may need to use an article before this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 3

Missing "," You may need to place a comma after this word.

Confused You have used **it** in this sentence. You may need to use **its** instead.

PAGE 4

Article Error You may need to use an article before this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Missing "," You may need to place a comma after this word.

Confused You have used **its** in this sentence. You may need to use **it's** instead.

Wrong Form You may have used the wrong form of this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 5

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Prep. You may be using the wrong preposition.

Article Error You may need to remove this article.

Article Error You may need to remove this article.

PAGE 6

PAGE 7

PAGE 8