DOI: 10.14421/ijid.2020.09101 IJID (International Journal on Informatics for Development), *e-ISSN:2549-7448*
Vol. 9, No. 1, 2020, Pp. 1-8

Malware in Computer Systems: Problems and Solutions

Mariwan Ahmed Hama Saeed
College of Basic Education
University of Halabja
Iraq
mariwan.ahmad@hotmail.com

Article History
Received January 31st, 2020
Revised February 9th, 2020
Accepted March 30th, 2020
Published June, 2020

***Abstract*—Malware is a harmful programme, which infects computer systems, deletes data files and steals valuable information. Malware can attack personal and organization computer systems. In this paper, the most recent and dangerous types of malware, including CovidLock Ransomware, have been analysed and the most suitable countermeasures of malware have been provided. The purpose of this paper is to suggest manually removing malware through a range of tools. It investigates whether the University of Halabja employees are protected against malware or not and it hypothesizes that the university of Halabja employees are not protected in a great level against malware attacks. A questionnaire has been conducted and analysed. The results of the questionnaire confirmed that the university of Halabja employees are not crucially protected. Therefore, it works to propose a sufficient way to make the whole organization protected. This research can be extended to include public and private universities across Kurdistan region in order to identify the most secure university in this region against malware attacks.**

Keywords-CovidLock; Covid-19 TRACKING App; Ransomware; Firewall; Security Software; Privacy; Computer Security; Malware Attacks

1 INTRODUCTION

Malware is a contraction of malicious software, is designed to destroy computer systems and programmes. It has many forms such as virus, worm, Trojan and spyware. Each year, many computer systems around the world will be damaged as a result of malware. Recently, ref. [1] reported that files, systems, emails and servers have been infected by Cookie.Weborama, Cookie.Rub and Exploit.Iframe viruses respectively. Despite that, in 2019 attacks by new Ransomware and PowerShell viruses have been increased by 118% and 460% [2]. Thus, any computer systems whether personal or organizations need to be protected and users need to have information on how to stay protected. Therefore, the purpose of this paper is to analyse the problems and the best solutions for malware on computer systems. For collecting data, the University of Halabja will be used. A questionnaire will be used to investigate whether the University of Halabja employees are protected or not and hypothesize that they are not protected. Therefore. It tries to recommend the best solutions for the University administration in this regard. The rest of this paper is structured as follows: Malware is analysed in Section 2 as well as the method. The result and discussion in section 3, The paper concludes major conclusions and plans for future work in Section 4.

2 METHOD

2.1 Analysis of Malware

According to [3]–[5]malware is described as any computer applications or codes which have been designed to destroy, interrupt the use of devices, use system resources and ask for ransom. Malware has several types such as Viruses, Worms, Spyware, Adware, Trojans, Bots, Rootkits, Backdoors, Ransomware and Spam [6]. Some types of malware are illustrated in Figure 1 and the most common types will be explained in the following sections [7].

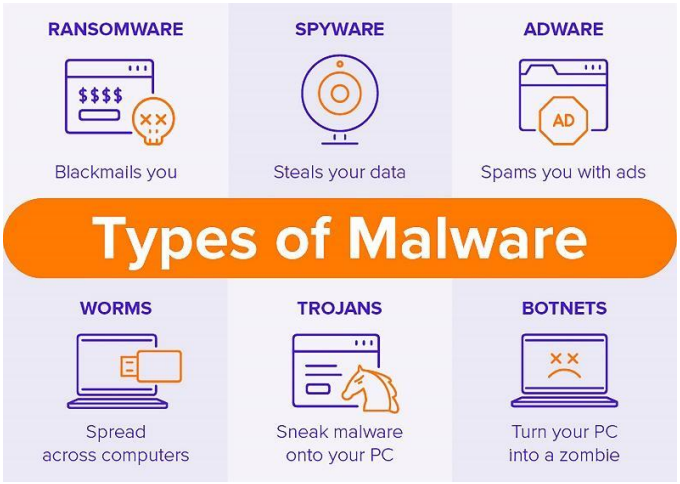

Figure 1. Types of Malware [7]

2.1.1 Virus

Virus is one of the types of Malware which is a piece of code that attaches to a programme or a file. When the infected programme is run by a user, the virus executes secretly without users noticing [8]. Ref. [9] indicates that many viruses need four stages to infect and destroy computer systems. Firstly, dormant phase is a stage known as an idle step because the virus is idle and it is activated by date or by another programme. Secondly, the virus tries to copy itself to another programme in the propagation phase. Thirdly, in the triggering phase, in this step the virus is ready to perform its functions. Damaging programmes, erasing files then shutting down or restarting computer systems are done by virus in the execution phase, the fourth stage. These steps are changed from one computer to another and one operating system to another. It also depends on the types of vulnerable points in the system. There many types of Viruses like Macro, Boot, File Infector and Psychological viruses. Macro infects Microsoft office files, Boot targets bios and OS boot sector, File Infector attaches to executable file such exe file and Psychological viruses use social engineering techniques to attract users to do a specific action [10], [11].

2.1.2 Worm

[12] defines worm as "a programme that executes independently of other programmes, replicates itself, and spreads through a network from computer to computer", which means that the worm is a harmful program that infects host to host via a vulnerable and security hole in the systems. The main difference between viruses and worms is that viruses always hide in programmes, however, worms are working independently. Moreover, worms are mostly used by hackers rather than viruses because the worms spread from computer to computer across network connections [13]. Ref. [9] notes that the worm uses some ways for spreading itself. Firstly, it uses email facilities to copy itself from system to system. Secondly, the execution methods help the worm to run itself to other systems. After that, it consumes login facilities in order to duplicate itself from one system to a different system. Ref. [9], [14] mentioned some types of worm such as Morris which was created by Robert Morris in 1998, Code Red and Nimda were released in 2001 and infected 360,000 servers around the world and modified internet documents extensions respectively.

2.1.3 Spyware and Adware

Spyware is placed on a computer, collects users' online and offline activity and back them to the central source, whereas, adware installed on a computer with user permission and it displays ads or popups for marketing purposes [6], [15].

2.1.4 Ransomware

According to [16] and [17], Ransomware is a malicious software that is used by cybercriminals to encrypt and lock computers, smartphones and data devices; it asks the device users to pay the ransom to unlock or decrypt their devices. It spreads via email links and attachments as well as infected websites and USB

Disks. It has many types for example; WannaCry, Ryuk, Troldesh, GoldenEye, Mac and mobile devices ransomware and Sodinokibi. These types have been discovered by Norton and Kaspersky Security Companies. In addition, CovidLock is the most recent types of Ransomware which has been appeared in the mid of March 2020 [18]–[20]. This malware is installed on mobile devices in forms of applications and it is downloaded from a third-party website as shown in Figure 2, not from official GooglePlay and AppleApp stores. This malware poses as Covid-19 and CORONAVIRUS TRACKING APP. Any smartphones with this app installed locks users out from their phone and asks the users to pay $100 dollar using Bitcoin in not less than 48 hours; otherwise, the user will lose all phone's data including photos, contacts, personal information and apps. Despite this, the criminals behind the ransome will outflow user's social media details as shown in Figure 3. Hopefully, any infected smartphones with this malware can be unlocked with 4865083501 [21] pin and in order to avoid un official and illegal apps, Microsoft has announced Covid-19 tracking apps for android and IOS systems it can be downloaded in this https://www.microsoft.com/en-us/bing/search-app-covid?pc_campaign=covid&_branch_match_id=749010479738825604 link

Figure 2. Coronavirus Tracking App [18]

2.1.5 Trojan

Ref. [8], [22]explains that Trojan is a programme, which is put into a system by hackers. It copies information without the user's authorization. Users are aware of the installation processes of Trojans, but they do not know about their hidden processes [5]. Attackers use Trojan in order to spread viruses or other types of malware into systems without the user's attention [10]. Ref. [23], [24] listed Trojan types such as Backdoor, this is used by attackers to control and access a computer. Ransom, SMS, Fake AV, Rootkit, Net-Bus and Sub-Seven which are used by the hackers and the attackers for destroying systems and stealing significant information from the systems.

2.2 Analysis of Countermeasures

There are many ways that can be used for mitigating the impacts of the malware on computer systems. This section will explain the solutions of malware in terms of Firewall, Security Software, Manually Removing Malware and Trainings.

2.2.1 Firewall

Nowadays, it can be seen that both online users and activities have been significantly grown. Whereas, not all users activate are appropriate, as a result, protection mechanisms should be used for protecting electronic systems from unauthorized access. A firewall is one of the protection mechanisms that can be used for controlling and monitoring incoming and outgoing network traffics based on security rules and it has two types of hardware and software [25]–[27]. The firewall scans incoming emails and helps operating system services for distinguishing fake applications and fake users [9], [12], [28]. According to [6], [12], [27], [29] a personal computer can be protected by a software firewall but a large organization can be secured by hardware firewall to allow/deny inside and outside actions that come from the Internet. Moreover, there are several best software firewalls such as Microsoft Windows Firewall, McAfee, Symantec, TrendMicro, Sygare, ZoneAlarm and Sophos as recommended by[6], [27].

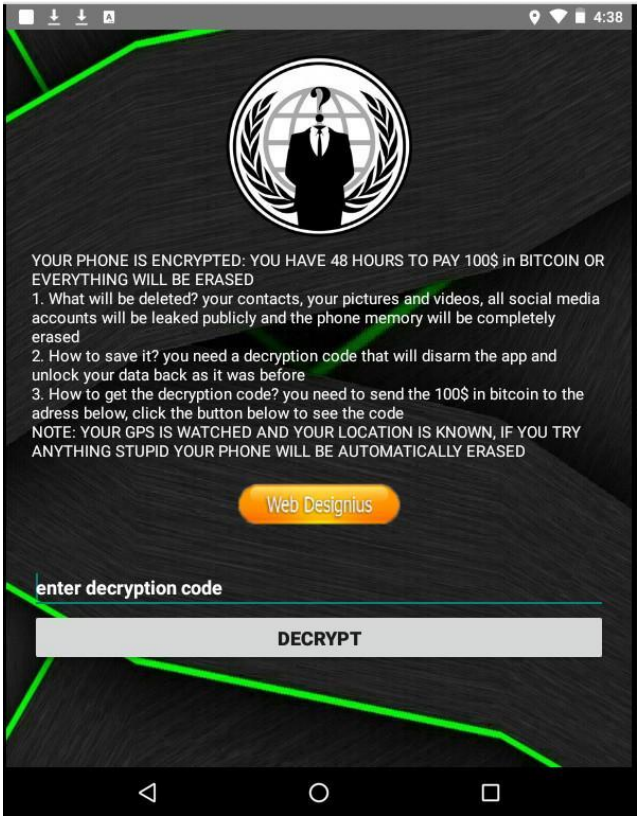

Figure 3. Android Smartphone with CovidLock [18][18]

2.2.2 Security Software

There are many types of security software such as removal tools, antiviruses and internet security software which can be used for protecting computer systems against malware.

1) Malware Removal Tools

Microsoft Safety Scanner, Microsoft Malicious Software Removal Tool and Diagnostics and Recovery Toolset (DaRT) are free malware removal tools that can be used for scanning and removing malware in computer systems [6]. These tools are provided by Microsoft Company and they can repair windows failures. In Table 1, some free removal tools are listed and a download link for each of them has been provided.

Table 1 Malware Removal Tools

Malware Removal Tools	**Download Link**
Microsoft Safety Scanner	https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download
Microsoft Malicious Software Removal Tool	https://www.microsoft.com/en-us/download/details.aspx?id=9905
Microsoft Diagnostics and Recovery Toolset (DaRT)	https://www.microsoft.com/en-us/download/details.aspx?id=35494
Emsisoft Emergency Kit	https://www.emsisoft.com/en/home/emergencykit/
Avast Free Malware Scanner and Removal Tool	https://www.avast.com/c-malware-removal-tool
Malware bytes	https://www.malwarebytes.com/mwb-download/thankyou/

2) Removing Malware Manually

This way is suggested to remove malware without using security software.Also, this way mentioned by [6] too. In this way, the malware file name should be known using Task Manager or Process Explorer programs for example WINWORD.EXE as shown in Figure 4, which is the process file of Microsoft Office Word not malware program. The file detail can be seen in the description column. The Process Explorer program can be downloaded via https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite link.

After identifying the malware file through the task manager or process explorer program, the process file should be killed/end tasked. After that, delete the file in file destination/location. Destination file can be gotten by right clicking on the file then clicking on Open File Location as displayed in Figure 5.

Furthermore, sometimes the malware process file cannot be end-tasked/killed or it is re-enabled after restart because the file might be related/attached to system files. To solve this, the Autoruns program can be used to uncheck the file as shown in Figure 6 “cmd.exe” as an example. The figure shows that the file is running and can be seen in the logon tab. Finally, after unchecking and restarting the computer, the file can be deleted in its location. The Autoruns program can be downloaded via https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite.

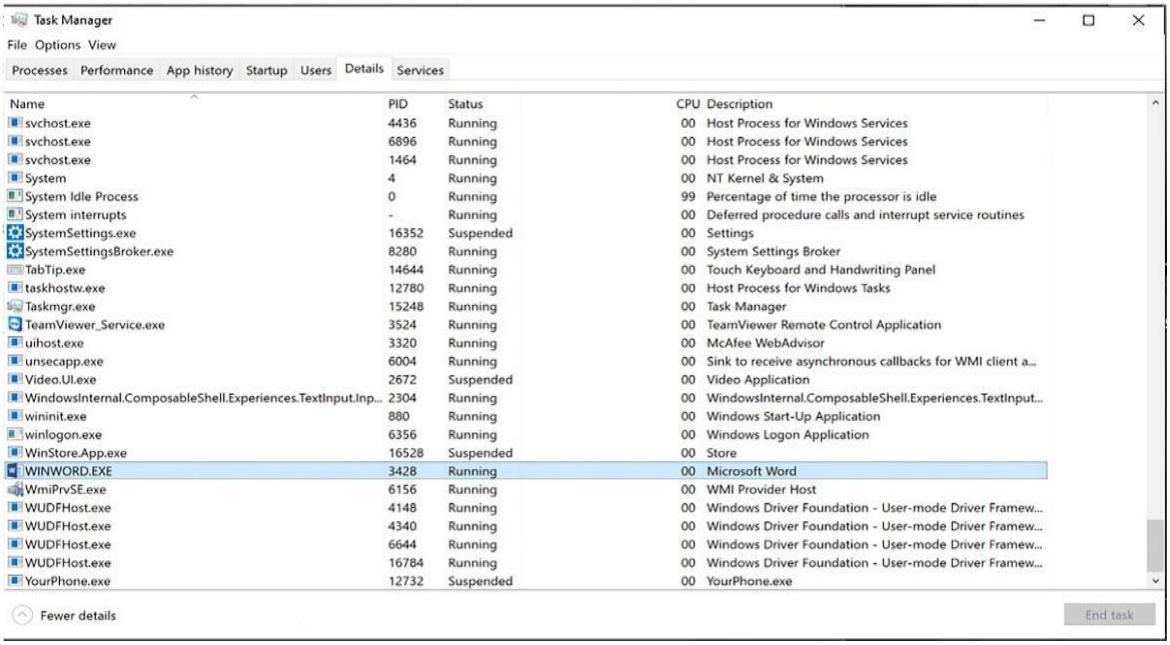

Figure 4. Microsoft Word process (WINWORD.EXE) file.

1) Antiviruses and Internet Security Software

[5] explained the main functions of antivirus programs including scanning start-up files, scanning real-time activities such as downloading files, monitoring application activities such as web browsers, scanning hard disks for known malware, identifying and removing malware. McAfee, Symantec – Norton, Sophos, AVG and Kaspersky antiviruses are endorsed by [6], [27], [30]. Internet Security Software have more features than antiviruses such as; securing online storage, anti-spyware, family and privacy protection, harmful web site blocking, device and platform-independent [6], [31], [32]. They recommended Kaspersky, AVG, Symantec, Trend Micro, McAfee and Sophos Internet Security Software. Some Free and paid Antiviruses and Internet Security Software are listed in Table 2 and a download link for each of them has been provided.

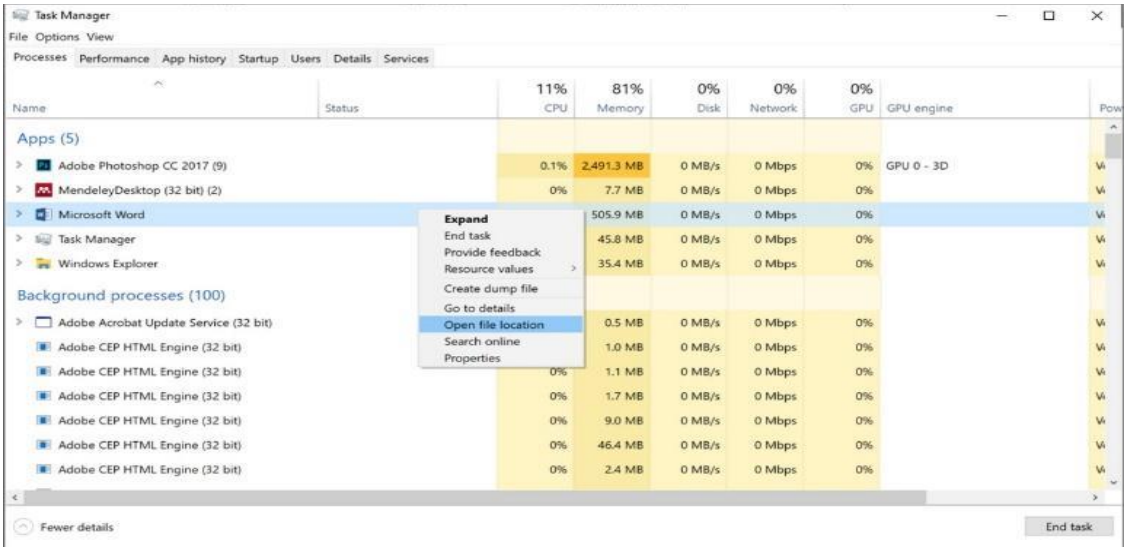

Figure 5. Open file location through Task Manager.

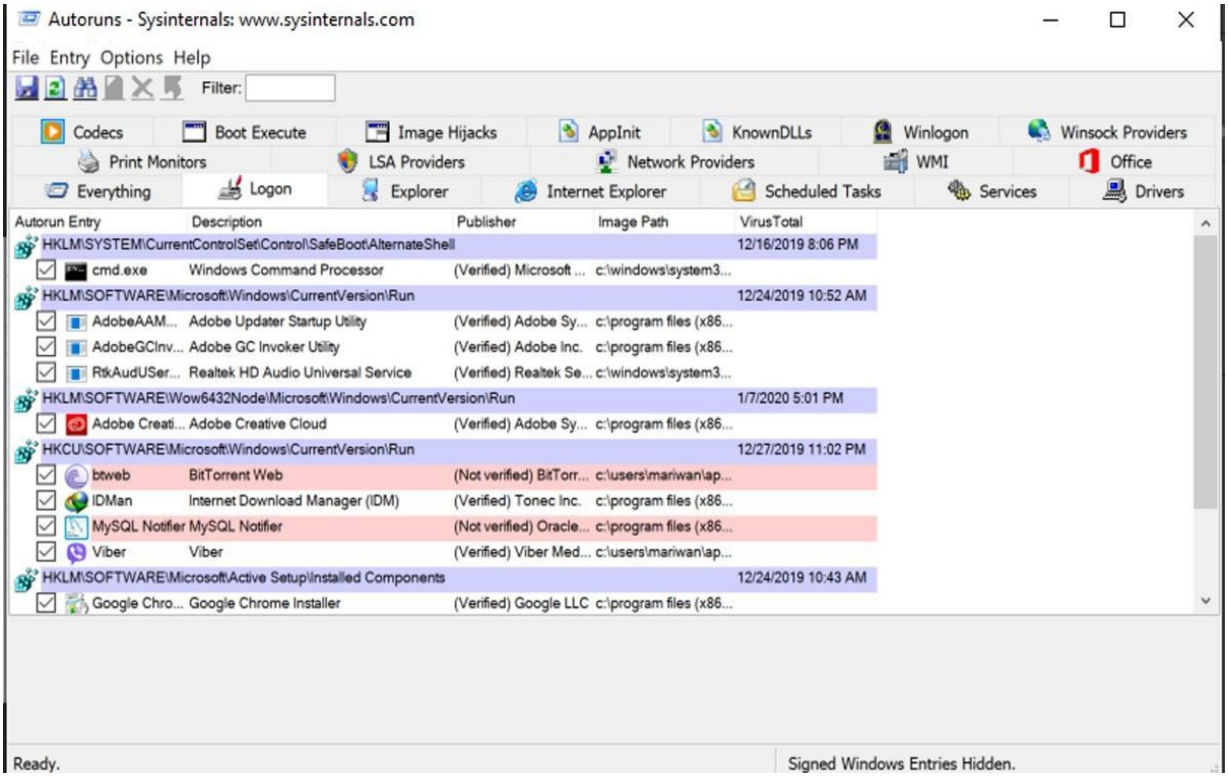

Figure 6. cmd.exe Command Prompt program file is running.

2.2.3 Training

Training is an additional protection way for securing organizations from threats. Malware consciousness and how to use threat mitigation techniques with antiviruses and internet security software are some ways that staff need to work on [8], [10]. Only expected emails should be opened by organization staff because stranger emails might include multimedia docs that are used by hackers and attackers for spreading threats and catching valuable information [28].

Staff should get security awareness by training them to know various types of threats, how they spread and how to find and delete them [6]. Despite that, it is better to use the last version of windows because it includes the latest security features such as windows defender antivirus, firewall, user account control, SmartScreen, trusted secure boot and mandatory security updates. Moreover, organizations should have a security level about how to use electronic devices such as how to transfer data using USB flash drives, portable hard drives, DVD and laptops. Ref. [5] mentioned browser separation, sandboxing technique and server virtualization to decrease the impact of threats. Microsoft "helps protect people against cyberthreats with built-in automation and intelligence" by intelligent security. The intelligent security can be opened by https://www.microsoft.com/en-us/security and it includes comprehensive security techniques and courses about home and business security. Finally, In order to protect data from corruption and loss, staff can use backup data daily, weekly and monthly. This feature can be seen in window setting-update and security-backup, Symantec Norton, Kaspersky Total Security, BullGuard Premium Protection and McAfee LiveSafe security software.

Table 2 Free and paid Antiviruses and Internet Security Software

Name	Type	Pricing	Download Link
AVAST	Antivirus	Free	https://www.avast.com/free-antivirus-download
Kaspersky	Antivirus	Free	https://me.kaspersky.com/free-antivirus
AVG	Antivirus	Free	https://www.avg.com/en-ww/free-antivirus-download
Bitdefender	Antivirus	Free	https://www.bitdefender.com/solutions/free.html
Sophos	Antivirus	Free	https://home.sophos.com/en-us/free-anti-virus-windows.aspx
McAfee Plus	Antivirus	Paid	https://www.mcafee.com/consumer/en-in/store/m0/catalog/mav_512/mcafee-antivirus-plus.html
Bitdefender Plus	Antivirus	Paid	https://www.bitdefender.com/solutions/antivirus.html
Norton Plus	Antivirus	Paid	https://us.norton.com/products/norton-360-antivirus-plus
Webroot	Antivirus	Paid	https://www.webroot.com/in/en/home/products/av
Kaspersky	Antivirus	Paid	https://me.kaspersky.com/antivirus
Norton 360 Deluxe	Internet Security	Paid	https://us.norton.com/products/norton-360-deluxe
McAfee LiveSafe	Internet Security	Paid	https://www.mcafee.com/en-us/antivirus/mcafee-livesafe.html
Bitdefender	Internet Security	Paid	https://www.bitdefender.com/solutions/internet-security.html
Kaspersky	Internet Security	Paid	https://me.kaspersky.com/internet-security

2.3 Methodology

2.3.1 The Questionnaire

A questionnaire has been conducted in order to check whether the University of Halabja is secured or not. The questionnaire is divided into two parts; the first part consists of four yes-no questions while the second part includes 5 statements which should be answered according to 5 scales. A Scale of 5 indicates strongly agree, while a scale of 1 represents strongly disagree. The questionnaire has been distributed among different departments and directorates of Halabja University where employees use computers for daily works. Seventy employees participated in the questionnaire. After they agreed to participate, the items were explained to them and all their questions were answered to make sure that they understood the questions.

3 Results and Discussion

As it can be seen from Table 3, as many as 71% of the participants chose no for the first question which means many of the employees do not use security software. And 60% of them do not use any antiviruses neither free nor paid. 86% of the participants said that the university does not provide any central security for the university computers whereas 13% had no answer. This means that they do not know about central security. For the last question, NO was selected by 91% of the participants and the question is about whether they have participated in any security courses or not.

Table 3 Percentage of the answers of YES-NO Questions

NO.	Questions	Yes (%)	No (%)	N.A (%)
1.	Do you use any internet security software?	26	71	3
2.	Do you use any free or paid antiviruses?	39	60	1
3.	Is there any central security provided by the University?	1	86	13
4.	Have you participated in any security courses?	0	91	9

The results of the data in Table 4, agree with the answers given for the questions in Table 1. For the first statement, "I know what electronic hacks and attacks are", 47% chose strongly disagree, 13% disagree which means the employees of Halabja University despite their profession and different backgrounds and specialties do not know what electronic hacks and attacks are. 21% chose neutral and only 13% know what electronic hacks and attacks are. Only 7% of the participants chose strongly agree to update their software and windows regularly. And, 13% agreed that they update their software and windows regularly. Whereas, 39% strongly disagree that they update their software and windows which is the highest rate. This statement indicates that employees do not update their software and windows regularly. The third statement is about using original software, again 39% strongly disagree that they used original software 17% disagree, 22% neutral, 7% agree and 14% strongly agree. Most of the participants do not feel safe using computers at the university because 29% strongly disagree and 24% disagree with the fourth statement. Whereas 24 were neutral, 10% agree and only 14% feel safe using computers at the university. Concerning the last statement, 80% strongly disagree and 9% disagree that there are courses that teach them computer and web security. Oppositely, only 3% agree and 1% strongly agree that there are security courses at the Halabja University for employees.

Table 4 Percentage of the answers of strongly agree and strongly disagree Questions

NO.	Statements	1(%)	2(%)	3(%)	4(%)	5(%)	N.A (%)
1.	I know what electronic hacks and attacks are.	47	13	21	9	4	6
2.	I update my software and windows regularly.	39	20	20	13	7	1
3.	I use original software like Microsoft windows and Microsoft office products.	39	17	22	7	14	1
4.	I feel safe using computers at my office at the University of Halabja.	29	24	23	10	14	0
5.	There are courses at the University of Halabja that teach us computer and web security.	80	9	4	3	1	3

The results of Table 3 and Table 4 confirm the hypothesis of the paper and they show that the University of Halabja lacks security. Malware can easily attack their computers because most of the employees are not using Internet Security and Antivirus programs. The university staff have not participated in any security courses because the university did not provide IT and security courses previously and they do not use original programs and do not update their programs regularly. To provide an appropriate solution, free and paid Internet Security and Antivirus programs can be used and these have been listed in Table 2. It is recommended for the university administrators to open IT and Security courses for the staff. The courses can include; Malware consciousness, how to use threat mitigation techniques, how to use electronic devices such as how to transfer data using USB flash and how to protect data from corruption and loss by using the backup feature of windows. In the training subsection of this paper extra points have been explained and can be added to the IT and Security courses. The university can contract with Microsoft and other software companies to obtain licenses for windows and Microsoft office products in order to decrease using illegal programs in the university because illegal programs use crack and patch files which are mostly used by hackers and attackers to destroy computer systems.

Lastly, results from Table 1 show that the university is more vulnerable for malware attacks including operating system files and folders corruptions because of low percentage of using internet security, antivirus and original software. Therefore, this paper has considerably suggested and explained how to remove malware manually as well as how to clean and repair corrupted system files and folders from malware through malware removal tools.

4 CONCLUSION

In this paper, Malware and its countermeasures have been briefly analysed. Ransomware which is the most recent type of malicious software has been explained. Firewall, Internet security, software and training as malware countermeasures have been described. CovidLock which is a new malware type has been analysed and its solution has been stated. Through a

questionnaire, the security of computer systems of the University of Halabja has been investigated and it is concluded that the University lacks security. Thereafter in this paper, significant suggestions have been proposed for the University presidency and directorates. Future work might include more research about cloud security as well as compare the University of Halabja in terms of security with other Universities in IRAQ.

FUNDING

This paper was not funded by any organization.

ACKNOWLEDGMENT

The author has no conflict of interest relevant to this article.

REFERENCES

[1] Bitdefender Resource Center, "Real-time Virus Reporting," 2019. .

[2] M. L. teams McAfee® Advanced Threat Research, "McAfee Labs Threats Reports – Threat Research | McAfee," 2019. .

[3] E. Filiol, "Viruses and Malware," in *Handbook of Information and Communication Security*, 2010.

[4] Microsoft Windows Security, "Understanding malware & other threats - Windows security | Microsoft Docs," 2019. .

[5] M. Borrelli, *Malware and Computer Security Incidents: Handling Guides - Nova Science Publishers*. New York: Nova Science Publishers, 2013.

[6] A. Bettany and M. Halsey, *Windows Virus and Malware Troubleshooting*. Berkeley, CA: Apress, 2017.

[7] Avast, "What is Malware & How Does it Work? | Malware Definition | Avast," 2019. .

[8] J. R. Vacca, *Computer and Information Security Handbook*. Elsevier Science, 2017.

[9] W. Stallings, *Cryptography and Network Security: Principles and Practice, Global Edition*. Pearson Education Limited, 2016.

[10] E. Cole, *Network Security Bible*. Wiley, 2011.

[11] P. Stavroulakis and M. Stamp, *Handbook of Information and Communication Security*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

[12] D. Salomon, *Elements of Computer Security*. Springer London, 2010.

[13] J. M. Kizza, *Guide to Computer Network Security*. Springer London, 2013.

[14] J. Aycock, *Computer Viruses and Malware*, vol. 22. Springer US, 2006.

[15] E. Geier and J. Geier, *Simple Computer Security: Disinfect Your PC*. Wiley, 2007.

[16] Norton, "What is ransomware and how to help prevent ransomware attacks," 2019. .

[17] Kaspersky, "Ransomware examples: Types of ransomware attack | Kaspersky," 2019. .

[18] Android-Authority, "New Android ransomware poses as coronavirus tracking app," 2020. .

[19] Digit-NewsDesk, "NEW COVIDLOCK RANSOMWARE POSES AS CORONAVIRUS TRACKING APP TO INFECT ANDROID SMARTPHONES: REPORT," 2020. .

[20] Cybersecurity-Asset-Management, "Coronavirus tracking app locks up Android phones for ransom," 2020. .

[21] Cybersecurity-Asset-Management, "Password found to rescue victims of malicious COVID-19 tracker app," 2020. .

[22] S. Collin, *Dictionary of Computing: Over 10,000 terms clearly defined*. Bloomsbury Publishing, 2009.

[23] Norton, "What is a Trojan? Is it virus or malware? How it works.," 2019. .

[24] W. A. Conklin, G. White, C. Cothren, R. L. Davis, and D. Williams, *Principles of Computer Security, Fourth Edition*. McGraw-Hill Education, 2016.

[25] Comodo, "What is a Firewall? | Explaining How a Firewall Works," 2019. .

[26] R. K. Eds and B. Steffen, *Principles of Security*. 2018.

[27] J. M. Kizza, *Guide to Computer Network Security*, vol. 39, no. 1. 2015.

[28] E. Cole *et al.*, *Wiley Pathways Network Security Fundamentals*. Wiley, 2007.

[29] Cisco, "What Is a Firewall? - Cisco," 2019. .

[30] W. Stallings and L. Brown, *Computer Security: Principles and Practice, Global Edition*. Pearson, 2017.

[31] AVG, "Compare All AVG Products | Find the Perfect Software," 2019. .

[32] Kaspersky, "Kaspersky Anti-Virus vs. Kaspersky Internet Security: what's the difference?," 2019.