Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 24, S. 125-129, Nisan 2021
© Telif hakkı EJOSAT'a aittir
Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 24, pp. 125-129, April 2021
Copyright © 2021 EJOSAT
Research Article

The Spy Next Door: A Digital Computer Analysis Approach for Backdoor Trojan Attack

Ilker Kara[1*]

[1*] Cankırı Karatekin University, Departmant of Medical Services and Techniques, Eldivan Medical Services Vocational School, Cankırı, Turkey, (ORCID: 0000-0003-3700-4825), karaikab@gmail.com

(2nd International Conference on Access to Recent Advances in Engineering and Digitalization (ARACONF)-10–12 March 2021)

(**DOI:** 10.31590/ejosat.897799)

ATIF/REFERENCE: Kara, I. (2021). The Spy Next Door: A Digital Computer Analysis Approach for Backdoor Trojan Attack. *Avrupa Bilim ve Teknoloji Dergisi*, (24), 125-129.

Abstract

Developments in internet-based technologies have some risks as well as their convenience. Attackers use the information they obtain by taking advantage of the user vulnerabilities and vulnerabilities in the information system for their interests. Although measures have been taken to prevent the number of victims of crimes committed in a cyber environment in recent years, the adequacy of the measures taken is still controversial. The attackers organize malware attacks especially to obtain users' secret information (social media password, banking information). Backdoor trojan malware is a type of cyber attack that tries to obtain unlimited authorization to obtain all user permissions in the system in which they infiltrate and delivers this information to the attacker. This study focused on the detection and analysis of the backdoor trojan malware. For this purpose real backdoor trojan malware case has been investigated in detail. The analysis results show that the information about the attacker is accessible.

Keywords: Digital forensic, Backdoor trojen, Malware analysis method.

Kapımdaki Düşman: Arka Kapı Trojen Saldırıları için Adli Bilişim Analizi Yaklaşımı

Öz

İnternet tabanlı teknolojilerinde yaşanan gelişmeler getirdiği kolaylıklarının yanı sıra bazı risklerinde barındırmaktadır. Saldırganlar bilişim sisteminde bulunan açıkları ve kullanıcı zafiyetlerinden faydalanarak ele geçirdikleri bilgileri kendi çıkarları için kullanmaktadır. Son yıllarda siber ortamda işlenen suç maruz kalan mağdur sayısını önlemek için tedbirler alınsa da alınan tedbirlerin yeterliliği halen tartışmalıdır. Saldırganlar, özellikle kullanıcıların gizli bilgilerini (Sosyal hesap parola, bankacılık bilgileri gibi) ele geçirmek için zararlı yazılımlar saldırıları düzenlemektedir. Arka kapı trojen zararlı yazılım saldırıları saldırıları son zamanlarda daha popüler hale getirmiştir. Arka kapı trojen zararlı yazılımları sızdıkları sistemde kullanıcıya fark ettirmeden tüm kullanıcı izinlerini almaya yönelik sınırsız yetki almaya çalışan ve ele geçirdiği bu bilgileri saldırgana ulaştıran siber saldırı türüdür. Bu çalışmada arka kapı trojen zararlı yazılım saldırı tespiti ve analizi üzerine odaklanmıştır. Bu amaçla gerçek bir arka kapı trojen zararlı yazılım vakası detaylı olarak incelenmiştir. Analiz sonuçlarından saldırganın ait bilgilerin ulaşılabilir olduğu göstermektedir.

Anahtar Kelimeler: Adli bilişim, Arka kapı trojeni, Zararlı yazılım analiz metotu.

[*] Corresponding Author: karaikab@gmail.com

1. Introduction

Malware is malicious software designed to damage the system they target (such as slowing or disrupting their functions, collecting critical information) [1]. Viruses, Worms, Trojans, Spywares, Ransomware are evaluated within this scope [2]. Spyware has recently come to the fore as the types of malicious software that attackers frequently resort to. Concrete action is required to fight against this cyber threat [3]. In this fight, the necessary besides defining the thread, analyze detail the attack steps, methods, and activities in spyware during the attack. In the literature, it is seen that (1) static analysis and (2) dynamic analysis, and (3) Sandbox approaches are widely used for malware (Figure 1).

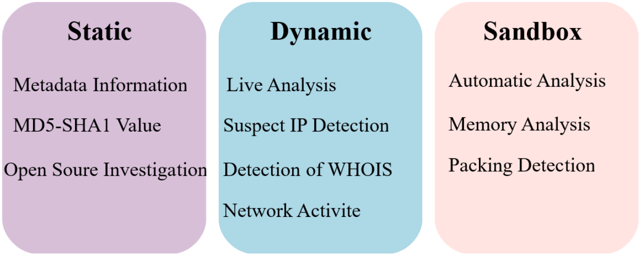


Figure 1. Commonly employed malicious software detection and analysis methods in the literatüre.

The static analysis includes the information that can be collected about the malware without executing it [4]. The information to be obtained by the static analysis method is extremely important and is relatively easier than other analysis types. By obtaining meta-data information, MD5 and SHA1 values of the malware, open-source research can be done about the malware. Web addresses specially designed for malicious software such as www.virustotal.com can be searched from the library of many malware types that have been previously detected and analyzed. Static analysis results are also guiding in the analysis to be made in the future.

Dynamic analysis is the analysis approach that is usually done by running malware in a safe environment [5]. With the execution of malicious software codes, it enables the movement capability of the malware and code analysis in detail. Approaches such as Windows-Registry, memory dump analysis are used to understand the working principle of malware.

Sandbox analysis is software that can automatically perform static and dynamic analysis of malware and provide analysis reports. This approach includes weaknesses. After the attackers design the malicious software, they test them in the sandbox environment and develop many anti-sandbox techniques to prevent them from being caught [6]. This approach can be easily circumvented in current malware.

Backdoor Trojan attacks are one of the most threatening malware attacks in recent years. This malware, also called spyware, can be defined as malicious software designed by the attacker to capture the information that is considered confidential or confidential without the user's knowledge or permission. Spyware can be for the service of a government or a company, or it can be designed for ordinary users to gain benefits.

New methods are developing to fight against spyware. Moser ve ark. [7], investigated the disadvantages of the static analysis methodology used in the analysis of malware. In studies, showed that static analysis alone is not enough to detect or classify malware. He/She also has claimed to be a necessary complement to static analysis in dynamic analysis of malware in a virtual machine environment, as it is less vulnerable to code cloaking transformation [8].

Engele et al., [9] suggested analysis programs to prevent trojan attacks and suspicious operations. The applicability of this method for trojan attacks is controversial, as it involves human factors and includes the possibility that malicious people can reach it. Gandotra et al., [10] has shown that machine learning techniques can be used to detect and classify new types of malware in behavior patterns obtained by static or dynamic analysis for trojans.

With all these in mind, in this study, we present an approach to contribute to the detection and analysis of backdoor Trojan malware attacks. This study mainly offers two contributions:

- The study focuses specifically on backdoor Trojan malware attacks and offers an approach that can be used in the detection and analysis of these attacks.

- The approach suggested in the study was selected as a real backdoor Trojan malware attack case and the results were evaluated by performing the attack detection and analysis.

This article has designed as described below: In section 2, we have reviewed some of the related studies. Section 3, (material and method), we have performed analysis and detection of real backdoor trojan malware. In the following section 4 evaluated the approach in the case. Lastly, section 5 completes the study and explains possible solution recommendations to fight against backdoor Trojan malware attack in the possible future.

2. Related Work

Although there is a work in the field of backdoor trojan malware detection and analysis in the literature, this section is briefly reviewed focusing on some of the important ones.

Moser et al [11] prepared a malware data set and examined the limits of analysis in order to prevent malware from infiltrating the victim system and preventing the activities of the user without being noticed. As a result of this study that more robust analysis techniques should be developed. Wang et al., worked on the mechanisms in the system that allow programs to be called automatically during the boot process of the operating system or when an application is started, by detecting and analyzing malicious software and tracing the malware.

Inoue et al., focused on providing internet access with malicious software with attackers and emphasized that controlling and blocking the traffic of this communication will contribute to the struggle [12]. Bayer et al. [13] showed that the detection and analysis of the malware can be done with analysis tools. Similarly, Bellard [14] examined using Windows Native API system service calls analysis tools besides Windows API functions.

3. Material and Method

In this section, backdoor trojan malware samples and introducing Workstation and analysis tools used in the analysis.

3.1. Case Study Dataset

In the case studies, it is extremely important that the chosen case includes the subject exactly and, if possible, it is a real example that we encounter in daily life.

We collaborate with an information security company operating in accordance with Turkey as an example of such a case. This company has special employees and equipment that collects and analyzes different types of malware samples, and they shared a true backdoor Trojan malware case with us.

3.2. Preparation of Analysis Environment

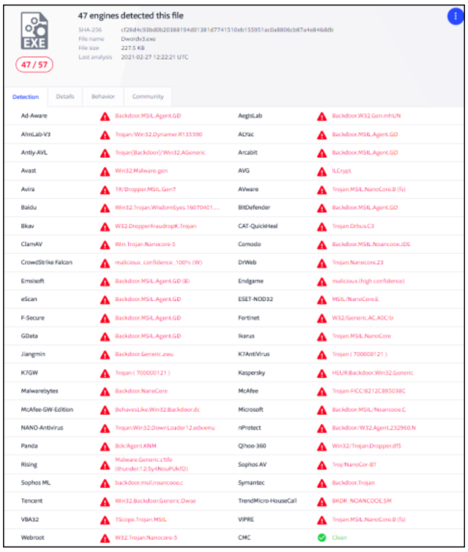
All analyses were performed on a Lenovo V530 Intel Core i7 8700 32GB 1TB + 512GB SSD brand workstation with Windows 10 Pro software. Analyses performed using “Process Monitor 3. 60 (Free Version)”, “Autopsy 4.17.0 (Free Version)” and “Wireshark 3.5.0” tools. An example is a real cyberattack and forensic case because for this reason some of the information is hidden.

3.3. Case Study

In the example examined, it was seen that a message was sent from the victim's social media accounts to request money from groups of victim’s friends without the victim’s knowledge, and the banking applications stored on his computer were blocked due to incorrect attempts. Therefore, the victim made a legal application to have the victim’s computer examined

For this purpose, the image copy of the victim’s computer in E01 format has been investigated in the workstation with the program Autopsy 4.17.0 (Free Version). Internet records belonging to the date of 27.02.2021, which is the date of suspicious transactions, were examined from the statements of the victim. As a result of this examination, it showed suspicious file which name is “Dwordv3.exe” has been downloaded.

Examinations have been focused on the file named “Dwordv3.exe”, from www.virustotal.com (Figure 2).



47 engines detected this file

SHA-256 cf28d4c93bd0b20388194d01381d7741510eb155951ac0a8806cb87a4e846ddb
File name Dwordv3.exe
File size 227.5 KB
Last analysis 2021-02-27 12:22:21 UTC

47 / 57

Ad-Aware	Backdoor.MSIL.Agent.GD	AegisLab	Backdoor.W32.Gen.mhUN
AhnLab-V3	Trojan/Win32.Dynamer.R135590	ALYac	Backdoor.MSIL.Agent.GD
Antiy-AVL	Trojan[Backdoor]/Win32.AGeneric	Arcabit	Backdoor.MSIL.Agent.GD
Avast	Win32:Malware-gen	AVG	ILCrypt
Avira	TR/Dropper.MSIL.Gen7	AVware	Trojan.MSIL.NanoCore.B (fs)
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Backdoor.MSIL.Agent.GD
Bkav	W32.DropperFraudropK.Trojan	CAT-QuickHeal	Trojan.Orbus.C3
ClamAV	Win.Trojan.Nanocore-5	Comodo	Backdoor.MSIL.Noancooe.JDE
CrowdStrike Falcon	malicious_confidence_100% (W)	DrWeb	Trojan.Nanocore.23
Emsisoft	Backdoor.MSIL.Agent.GD (B)	Endgame	malicious (high confidence)
eScan	Backdoor.MSIL.Agent.GD	ESET-NOD32	MSIL/NanoCore.E
F-Secure	Backdoor.MSIL.Agent.GD	Fortinet	W32/Generic.AC.A0C!tr
GData	Backdoor.MSIL.Agent.GD	Ikarus	Trojan.MSIL.NanoCore
Jiangmin	Backdoor.Generic.zwu	K7AntiVirus	Trojan (700000121)
K7GW	Trojan (700000121)	Kaspersky	HEUR:Backdoor.Win32.Generic
Malwarebytes	Backdoor.NanoCore	McAfee	Trojan-FICC!8212C885038C
McAfee-GW-Edition	BehavesLike.Win32.Backdoor.dc	Microsoft	Backdoor:MSIL/Noancooe.C
NANO-Antivirus	Trojan.Win32.DownLoader12.edxemu	nProtect	Backdoor/W32.Agent.232960.N
Panda	Bck/Agent.KNM	Qihoo-360	Win32/Trojan.Dropper.df5
Rising	Malware.Generic.c!tfe (thunder:1:2:Sy4NouPUkfD)	Sophos AV	Troj/NanoCor-BT
Sophos ML	backdoor.msil.noancooe.c	Symantec	Backdoor.Trojan
Tencent	Win32.Backdoor.Generic.Dwso	TrendMicro-HouseCall	BKDR_NOANCOOE.SM
VBA32	TScope.Trojan.MSIL	VIPRE	Trojan.MSIL.NanoCore.B (fs)
Webroot	W32.Trojan.Nanocore-5	CMC	✓ Clean

Figure 2. Screen capture of the suspicious file named “Dwordv3.exe” showing www.virustotal.com query.

“File-Directory”, “Windows Registry”, Autopsy and “Process” tools used for the static analysis and the tool named Process Monitor used for the actions were performed of the suspicious file named “Dwordv3.exe”.

Table 1. File-directory and registry logs of "Dwordv3.exe" malware.

Process	**Process Process Activity**
Creates	C:\Users\Admin
Creates	C:\Users\Admin\AppData\Roaming
Creates	C:\Users\Admin\AppData\Roaming\run.dat
Creates	C:\Users\Admin\AppData\Local\Temp\tmp6F5.tmp
Creates	C:\Users\Admin\AppData\Roaming\Password\Logon
Creates	C:\Users\Admin\AppData\Roaming\Logon\Admin
Writes	C:\Users\Admin\AppData\Roaming\run.dat

Table 2. Windows and registry activity of "Dwordv3.exe" malware.

Process	**Process Process Activity**
Creates key	HKLM\software\microsoft\fusion\gacchangenotification\default
Creates key	HKLM\system\currentcontrolset\services\tcpip\parameters
Creates key	HKLM\software\microsoft\windows\currentversion\run[dhcp service
Sets/Creates value	HKLM\software\microsoft\fusion\gacchangenotification\default

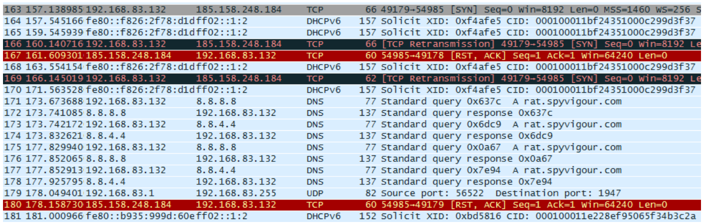
Table 3. Process activity of "Dwordv3.exe" malware.

Process	**Process Process Activity**
Creates process	C:\Windows\temp\Dwordv3.exe ["C:\windows\temp\Dwordv3.exe"]
Creates process	C:\Windows\system32\schtasks.exe["schtasks.exe"/create/f/tn"DHCPService"/xml "C:\Users\Admin\AppData\Local\Temp\tmp55A.tmp"]
Creates process	C:\Windows\system32\schtasks.exe"schtasks.exe"/create/f/tn"DHCPServiceTask"/xml "C:\Users\Admin\AppData\Local\Temp\tmp6F5.tmp"]
Creates process	C:\Windows\System32\schtasks.exe
Creates process	C:\Windows\temp\Dwordv3.exe ["C:\windows\temp\Dwordv3.exe"]
Terminates process:	C:\Windows\system32\schtasks.exe["schtasks.exe"/create/f/tn"DHCPService"/xml "C:\Users\Admin\AppData\Local\Temp\tmp55A.tmp"]

As can be seen in Table 1, when the "Dwordv3.exe" file-directory movements are examined, the malware first creates itself in the temp folder under Windows. Then it logon the registered accounts in the system with “Password” and executes the malware with the “run” command. After the examination of the Windows Registry actions, it was seen the DHCP service command has run. DHCP service is designed for providing an IP address to computers that do not have a disc. When Process

Actions are examined, it is seen that the malware created and executed a file as "schtasks.exe" under the Windows \ system32 folder after creating itself in the temp file. This result is showing that “Dwordv3.exe” backdoor trojan malware is structured as packaged. Malware packaging is made to add malicious software codes to a file that seems harmless at first glance to circumvent existing security systems. “schtasks.exe” file accessed to DHCP service has been observed.

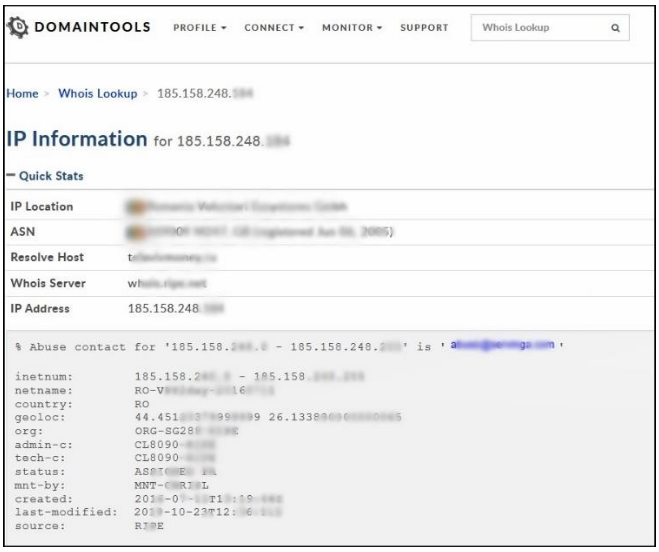
After the detection of process actions, file folder, and Windows-registry, “Wireshark” tool has been used for dynamic analysis. Wireshark tools have analyzed the network traffic in order to detect the IP address of the system that belongs to this malware (Figure 3).



```
163 157.138985 192.168.83.132     185.158.248.184     TCP       66 49179→54985 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 S
164 157.545166 fe80::f826:2f78:d1dff02::1:2           DHCPv6   157 Solicit XID: 0xf4afe5 CID: 000100011bf24351000c299d3f37
165 159.545939 fe80::f826:2f78:d1dff02::1:2           DHCPv6   157 Solicit XID: 0xf4afe5 CID: 000100011bf24351000c299d3f37
166 160.140716 192.168.83.132     185.158.248.184     TCP       66 [TCP Retransmission] 49179→54985 [SYN] Seq=0 Win=8192 Le
167 161.609301 185.158.248.184    192.168.83.132      TCP       60 54985→49178 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
168 163.554154 fe80::f826:2f78:d1dff02::1:2           DHCPv6   157 Solicit XID: 0xf4afe5 CID: 000100011bf24351000c299d3f37
169 166.145019 192.168.83.132     185.158.248.184     TCP       62 [TCP Retransmission] 49179→54985 [SYN] Seq=0 Win=8192 Le
170 171.563528 fe80::f826:2f78:d1dff02::1:2           DHCPv6   157 Solicit XID: 0xf4afe5 CID: 000100011bf24351000c299d3f37
171 173.673688 192.168.83.132     8.8.8.8             DNS       77 Standard query 0x637c  A rat.spyvigour.com
172 173.741085 8.8.8.8            192.168.83.132      DNS      137 Standard query response 0x637c
173 173.742172 192.168.83.132     8.8.4.4             DNS       77 Standard query 0x6dc9  A rat.spyvigour.com
174 173.832621 8.8.4.4            192.168.83.132      DNS      137 Standard query response 0x6dc9
175 177.829940 192.168.83.132     8.8.8.8             DNS       77 Standard query 0x0a67  A rat.spyvigour.com
176 177.852065 8.8.8.8            192.168.83.132      DNS      137 Standard query response 0x0a67
177 177.852913 192.168.83.132     8.8.4.4             DNS       77 Standard query 0x7e94  A rat.spyvigour.com
178 177.925795 8.8.4.4            192.168.83.132      DNS      137 Standard query response 0x7e94
179 178.049401 192.168.83.1       192.168.83.255      UDP       82 Source port: 56522  Destination port: 1947
180 178.158730 185.158.248.184    192.168.83.132      TCP       60 54985→49179 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
181 181.000966 fe80::b935:999d:60eff02::1:2           DHCPv6   152 Solicit XID: 0xbd5816 CID: 000100011e228ef95065f34b3c2a
```

Figure 3. screenshot of the network actions belong to the malware named “Dwordv3.exe”.

After detecting that the malware communicated with the IP address "185.158.248.XXX" and the domain name "rat.spyxxxxxx.com", the WHOIS queries for the relevant domain name and IP address were made on the www.domaintools.com web page, and the screenshot of the query It can be seen in Figure 4.



Home > Whois Lookup > 185.158.248.[redacted]

IP Information for 185.158.248.[redacted]

− Quick Stats

IP Location	[redacted]
ASN	[redacted]
Resolve Host	t[redacted]
Whois Server	wh[redacted]
IP Address	185.158.248[redacted]

```
% Abuse contact for '185.158.[redacted] - 185.158.248.[redacted]' is '[redacted]'

inetnum:        185.158.2[redacted] - 185.158[redacted]
netname:        RO-V[redacted]
country:        RO
geoloc:         44.451[redacted] 26.1338[redacted]
org:            ORG-SG28[redacted]
admin-c:        CL8090[redacted]
tech-c:         CL8090[redacted]
status:         AS[redacted]
mnt-by:         MNT-[redacted]
created:        201[redacted]
last-modified:  201[redacted]
source:         RI[redacted]
```

Figure 4. Screenshot of WHOIS query for IP address “185.158.248.XXX”.

As the result of the query, it was seen that the information about the attacker could be reached.

4. Discussion

The case that we consider as a take backdoor trojan malware case in this study is named as a real case study analysis. The example of the backdoor Trojan malware case under investigation is called the popular type of cyberattacks designed to capture confidential information stored in the victim system.

From the analysis results, (1) this used example of backdoor trojan malware case detection and analysis (2) offers two important advantages, such as accessing information about the attacker. On the other hand, backdoor trojan malware case analysis has some difficulties. Since it can use different designs in each attack, it is similar to other attack examples, but the detection and analysis approach may vary according to the case. For this reason, case studies contribute greatly to the fight against this crime.

We believe that the approach proposed in this study needs to be reinforced and repeated with more current examples to support it.

5. Conclusion

In this study, we conducted a study involving a real case study for backdoor trojan malware attack detection and analysis. Moreover, it showed that information about the attacker could be reached from the analysis results. With the approach used in the study, it has been seen that it can be a suitable method that can be used especially in backdoor Trojan malware attack detection and analysis.

Finally, we believe the study will raise awareness in the fight against malware. As a future study, we plan to investigate backdoor trojan malware attack detection and analysis with different sample data sets.

References

[1] Kara, I. (2019). A basic malware analysis method. Computer Fraud & Security, 2019(6), 11-19.

[2] Kara, I. (2020). Security Risks and Safeguard Measures in Social Media Usage. Avrupa Bilim ve Teknoloji Dergisi, 10-15.

[3] Anderson, B., Quist, D., Neil, J., Storlie, C., & Lane, T. (2011). Graph-based malware detection using dynamic analysis. Journal in computer Virology, 7(4), 247-258.

[4] Kara, I. (2015). Türkiye De Zararli Yazilimlarla Mücadelenin Uygulama Ve Hukuki Boyutunun Değerlendirilmesi. Akademik Bakış Uluslararası Hakemli Sosyal Bilimler Dergisi, (52), 87-98.

[5] Talukder, S., & Talukder, Z. (2020). A survey on malware detection and analysis tools. International Journal of Network Security & Its Applications, 12(2).

[6] Pandey, A., Tripathi, A., Alenezi, M., & Khan, A. K. (2020). Framework for producing effective efficient secure code through malware analysis. International Journal of Advanced Computer Science and Applications, 11(2), 497-503.

[7] Paul, K. I., & Moser, K. (2009). Unemployment impairs mental health: Meta-analyses. Journal of Vocational behavior, 74(3), 264-282.

[8] Bermejo Higuera, J., Abad Aramburu, C., Bermejo Higuera, J. R., Sicilia Urban, M. A., & Sicilia Montalvo, J. A. (2020). Systematic Approach to Malware Analysis (SAMA). Applied Sciences, 10(4), 1360.

[9] Egele, M., Scholte, T., Kirda, E., & Kruegel, C. (2008). A survey on automated dynamic malware-analysis techniques and tools. ACM computing surveys (CSUR), 44(2), 1-42.

[10] Gandotra, E., Bansal, D., & Sofat, S. (2014). Malware analysis and classification: A survey. Journal of Information Security, 2014.

[11] Moser, A., Kruegel, C., & Kirda, E. (2007, December). Limits of static analysis for malware detection. In Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007) (pp. 421-430). IEEE.

[12] Inoue, D., Yoshioka, K., Eto, M., Hoshizawa, Y., & Nakao, K. (2008, May). Malware behavior analysis in isolated miniature network for revealing malware's network activity. In 2008 IEEE International Conference on Communications (pp. 1715-1721). IEEE.

[13] Bayer, U., Moser, A., Kruegel, C., & Kirda, E. (2006). Dynamic analysis of malicious code. Journal in Computer Virology, 2(1), 67-77.

[14] Fabrice, B. (2005, June). Qemu, a fast and portable dynamic translator. In USENIX2005Annual Technical Conference, FREENIX Track.