THE GHOST IN THE SYSTEM: TECHNICAL ANALYSIS OF REMOTE ACCESS TROJAN

İlker Kara, Murat Aydos

Dept. of Computer Engineering, Hacettepe University, Ankara
e-mails: karaikab@gmail.com, maydos@hacettepe.edu.tr
Turkey

Abstract: Although the cyberattacks in the past have been planned to block access and to destroy information, these now have turned into attacks that demand ransom or steal user's information. Malware designed for these purposes cause losses of reputation, customer and market loss problems in addition to user's financial losses. Attackers' new favorite, the Remote Access Trojan (RAT), allows viewing and modifying user's files and functions in the system, monitoring and recording user activity, and using the victim's system to attack other systems. RATs can easily hide in the system with their advanced methods of infection and can be present as ghost entities in the system without getting caught by the security software. Although new methods have been developed to solve the damage caused by RATs, a definite solution still has not been found since it's difficult to detect RAT's presence. In order to solve this problem, the identification of the threat and its consequences as well as the RAT's infectious activities in the target system and its manufacturer are of importance. This study discusses a detailed analysis of RAT detection on a real victim's computer, targeted by a real RAT attack. Behavior of the malware was analyzed in detail using static and dynamic analysis, and it was shown that the server connected through RAT was traceable through its whois information.

Key words: Remote Access Trojan (RAT), Trojan, Malware Analysis

1. INTRODUCTION

The concept of espionage is not a new phenomenon for today's world. Throughout the history of humankind, espionage has been a common tactic used by malevolent people, from the First World War to the present. Today, the attackers started to implement this tactic in the cyber world. Attackers can use their deceiving tactics effectively and easily for profit or for attacks to steal user's information. These malicious software can easily infect users' systems by various methods such as custom-designed e-mails, visits to unsafe websites, cookies and social engineering attacks that deceivingly look like advertisements [1-3].

Spyware, unlike viruses and worms, create their copies once infected with the target system and spread more [4,5]. The purpose of spyware is to collect the requested information by hiding in the target system. This information may cover a wide area ranging from the user's social media account password to credit card information. Other than that, commercial companies can spread adware over the Internet to detect user habits. Spyware, infiltrating systems without the knowledge of users, is one of the most important attacks against personal privacy [6]. Infectious techniques of spyware are not well-known by users [7]. One of the most important measures to ensure the information and computer security is to keep the operating system up-to-date through patches and updates constantly, and measures such as not to download and execute unsolicited programs from unsafe websites are also effective in providing a protection against spyware [8]. Like the antivirus software widely used by users against viruses, recently developed anti-spyware products should also be installed and updated on the systems as an indispensable tool for the users. One of the common misconceptions is that a computer system with an antivirus program will protect against all malware and spyware. Of course, virus protection programs are very important, but numerous malware and spyware are released every day [9].

2. TROJAN SOFTWARE

Trojans, which named after the Trojan horse in mythology, are malicious software that deceive users by appearing something beneficial for them [10-12]. Trojan horses are often infect the target system when the user opens a program that is considered to be originated from a legitimate source. In this method, the victim's system is infected through updates free of charge or through free downloads. The trojan itself is not a virus (trojan may contain viruses, but it is not a virus itself). Trojan does not replicate itself, it only performs its intended purpose (stealing passwords, information copy, etc.). Trojans appear as a harmless program (e.g. a game or utility) to the user. The user sees the trojan as a harmless program at first run. However, the trojan can perform many operations (erase or corrupt data) upon its execution at the system. Trojans are modified for giving maximum damage to victims or for performing specifically intended actions [13]. The Trojan sends the password of every e-mail address opened after infecting the victim computer. The username and passwords of social media accounts such as Facebook, Twitter, Instagram and the username and passwords you have used for all other websites can be captured and changed at any time. This feature is enabled by the activation of the "keylogger" feature in Trojan [14]. Even if the attacker is not online, the trojan sends all the keyboard entries to the attacker using the user's e-mail address periodically, with intervals set by the trojan's keylogger settings [15].

Social media-based malware, which is frequently seen all over the world recently, causes many victims to experience harmful consequences [16-20]. Social media-based malwares are often used for financial benefits (such as ransomware),

stealing user's personal information, intelligence gathering activities, blackmail, and espionage [21, 22]. After encrypting the files in the target system, the ransomware also encrypts the private files of the user. In order to access these files again, the victim must pay the ransom to the attacker. Payment is made with virtual currency, called Bitcoin [23, 24].

◆ **What is RAT?**

RATs are the programs that allow malicious attackers to control the system and access the victim's information by opening a backdoor in the user's system [25-27]. It is a class of malware, which is developed constantly with new methods, enabling the attacker to connect to the victim's system remotely and interactively [28]. They are not only simple attacks, intelligence agencies and activist groups also use RATs for specific purposes, such as blackmailing and spying [29].

The RAT infection to the target system takes place primarily by directing the user to install a modified file [30]. This file can be sent to the system via social media platforms (MSN, Facebook, Instagram, etc.) over the RAT's server or through a program that will be downloaded by the user. Another method of infection is Java Downloader. When the victim visits a specific website, the Java codes are uploaded to victim's computer and activated, without the user's knowledge. The simplest attack that RATs can perform is the ability to turn on webcam and microphone devices at any time. If the user's system is open and connected to the Internet, even if the user is not using the system, the attacker can connect to the webcam to view, record or listen to the entire conversations in the room. In addition, the attacker can use the remote access feature to visit any website and download any file into the user's system. In short, RATs transmit information about all applications, application passwords, account passwords, hardware, system structure and features installed in the system to attackers upon execution of the trojan. This constitutes a quite risk and very dangerous vulnerability if you use online banking or keep company information on the system.

Spyware and its derivatives, which have become a serious source of income for the attackers in the cyberworld, are being released every passing day. When the trojan attacks, which have unintentionally caused great harm to users and commercial institutions, were examined, it was revealed that there were not enough measures taken against these attacks and that the threat identification and detailed analysis were insufficient. In this study, a real attack example was examined for the detection and detailed analysis of the trojan threat and it was attempted to make contributions for more effective measures against such malicious software. In the analysis, trojan software were evaluated in detail step-by-step and possible measures to combat these malware were proposed.

3. METHOD

There is no standard method for malware analysis. However, we performed a static analysis first, without running the malware, secondly, a dynamic analysis was performed, in which its actions (file-directory movements) were examined by running the malware in a controlled environment, and finally the code analysis was performed for architectural analysis of the malware. In principle; no analysis is performed in the victim computer due to the difficulty in controlling the victim computer (live system) and the potential of further damage. For this reason, the copy of the victim computer was taken, and analysis was performed in a different environment (business computer). The FTK Imager (free version) program was used to copy the computer attacked by the RAT malware. Since the RAT software would attack user data quickly upon running it, it was executed in virtual machine mode of the workstation. Analysis for the characteristic behavior of TeslaCrypt ransomware were performed through "AccessData Forensic Toolkit v6.2.1.10 (FTK)", "Process Explorer", "Wireshark" and "Cuckoo". Although there is no standard method for malware analysis, the general trend is moving from simple to complex. It is a good way to obtain all the information that can be get without executing the malware first, then to analyze its actions in a controlled environment, and finally to examine the code architecture on the malware. In this study, a model was proposed for the analysis steps and the proposed model algorithm was applied (Fig.1).

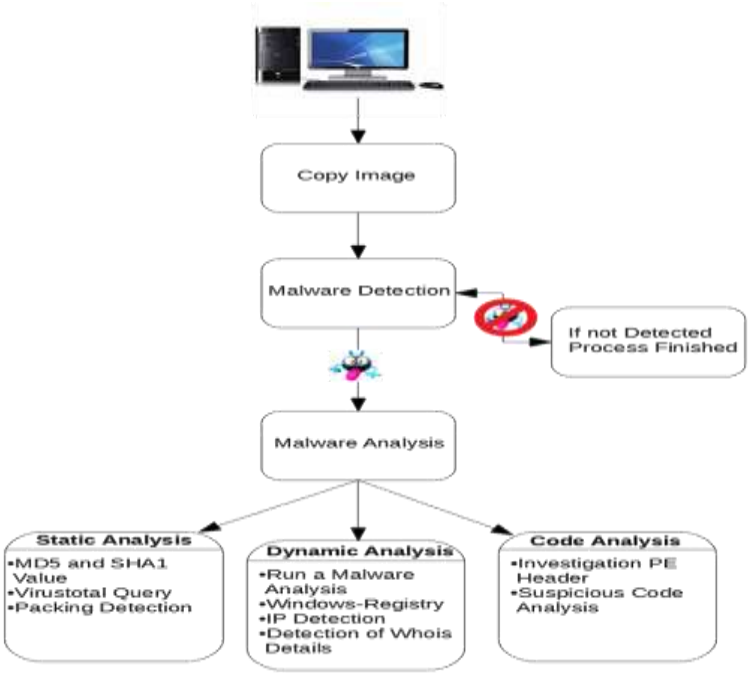

Fig. 1. Proposed model algorithm for malware analysis.

4. ANALYSIS

In the first examinations on the copy, it was seen that there was a suspicious file on the victim's desktop. Malicious software process was initiated considering that this file may be a malware. When looking at the last operations performed by the user on the computer, it was seen that the file in question was downloaded. It is known that social media accounts (Facebook and Instagram accounts) of the victim cannot be accessed after the download. As a result of the analysis, "Locker BLUE (Marvel Avengers Alliance) 15-05-26.exe" file was found in the "IMAGE__.001/Partition 2/NONAME [NTFS]/[root]/Users/ByLoressima/Downloads/" folder.

Fig. 2. The appearance of the suspicious file on the victim's computer

In the direction of the proposed model algorithm, static analysis was performed first. The file information was obtained using the FTK and Cuckoo programs (Table 1). As a result of the static analysis, information on the victim computer that has the RAT software were obtained by using FTK and Process Explorer programs, and presented in Table 1.

Table 1. Suspect file information (LOCKER BLUE (MARVEL AVENGERS ALLIANCE) 15-05-26.EXE)[1]

Process Name	File Information
File name	Locker BLUE (Marvel Avengers Alliance) 15-05-26.exe
Creating Time	02.06.2015 16:20:45 (2015-06-02 13:20:45 UTC)
Access Time	02.06.2015 16:20:45 (2015-06-02 13:20:45 UTC)
Replacement Time	02.06.2015 16:09:01 (2015-06-02 13:09:01 UTC)
File Size (Byte)	1.389.807 bytes (1357 KB)

The file "Locker BLUE (Marvel Avengers Alliance) 15-05-26.exe", detailed information is given in Table 1 as a result of the static analysis, was queried online via the www.virustotal.com website, which contains databases of numerous antivirus companies, and it was understood that the subject file is a malware (Fig. 2).

[1] link access: "http://dosya.co/hu2vk3xy37x4/LockerBlue_(64_BIT)_17-03-29.EXE.html"

Fig. 3. Screenshot of the result of the query performed on www.virustotal.com website.

As a result of the query of the file "Locker BLUE (Marvel Avengers Alliance) 15-05-26.exe", which is shown in detail in Figure 3, on the www.virustotal.com website, it was found that the file was detected as malware by 17 antivirus programs. In accordance with the proposed model algorithm, dynamic analysis was performed as the second stage analysis. The "Locker BLUE (Marvel Avengers Alliance) 15-05-26.exe" malware was found to be designed to capture personal information and FTK and Process Explorer programs were used to analyze its file-directory and registry actions (Table 2 and Table 3).

Table 2 and Table 3 show the dynamic analysis results of the "Locker BLUE (Marvel Avengers Alliance) 15-05-26.exe" malware. As a result of the examinations of the file-directory movements of the malware, it was seen that its activities were related to the Internet locations. As shown in Table 2, the malware creates a password named "lockerbluepassword" by issuing the "Write to: C:\Users\Admin\AppData\Local\Microsoft\Windows\TemporaryInternetFiles\Content.IE5\BX3UL1GO\lockerbluepassword[1].html" command under Internet Files. In addition, it was found that it performs operations with the "C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@fbugs[1].txt" command. This command may be important, because it may contain information about the attacker. It was observed that the attacker performs write operations with the "Write to" command, and then performs a delete by issuing the "Delete" command.

Table 2. Locker Blue (Marvel Avengers Alliance) 15-05-26.exe file-directory actions.

File Operation	**File Information**
Creates:	C:\Users\Admin
Creates:	C:\Users\Admin\AppData\Local
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Writes to	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@fbugs[1].txt
Writes to	C:\Users\Admin\AppData\Local\Temp\~DFF6F47C4D6E39EA3F.TMP
Writes to	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ BX3UL1GO\lockerbluepassword[1].html
Deletes:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@fbugs[1].txt
Deletes:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@fbugs[2].txt
Deletes:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ X3IPB3Z1\favicon[1].ico

Table 3. Locker Blue (Marvel Avengers Alliance) 15-05-26.exe windows registry actions.

File Operation	**File Information**
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\connections
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\connections
Creates key:	HKCU\software\microsoft\internet explorer\main
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\passport\lowdamap
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\wpad
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[proxybypass]
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet settings[proxyserver]
Value changes:	HKCU\software\microsoft\windows\currentversion\internet settings\zones[securitysafe]
Value changes:	HKCU\software\microsoft\windows\currentversion\internet settings\connections[defaultconnectionsettings]
Value changes:	HKLM\software\microsoft\directdraw\mostrecentapplication[name]
Value changes:	HKLM\software\microsoft\directdraw\mostrecentapplication[id]

As shown in Table 3, it creates key by the "Create key: HKCU\software\microsoft\windows\currentversion\Internetsettings\passport\lowdamap" command under the Internet setting in the system. After these commands were processed, it was observed that these values were changed with "Value change: HKLM\software\microsoft\directdraw\mostrecentapplication[name]", and "Valuechange:HKLM\software\microsoft\directdraw\mostrecentapplication[id]" commands.

After examining the file-directory and registry actions of the malicious software named "Locker BLUE (Marvel Avengers Alliance) 15-05-26.exe", the "Wireshark" program was used to examine the network actions of the malware. In the Wireshark analysis of network activities of the "Locker BLUE (Marvel Avengers Alliance) 15-05-26.exe" malware, the Whois information of the attacker was found to be accessible (Fig.3).

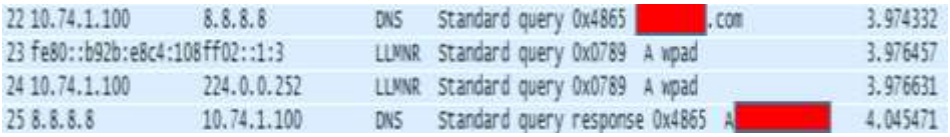

Fig. 4. Network actions of the "Locker BLUE (Marvel Avengers Alliance) 15-05-26.exe" malware as listed by the Wireshark program.

The “Whois” command contains the information for the domain (such as google.com or the IP of the person or the institution). In terms of the battle for malware, acquiring the Whois info of the attacker is very important first step to impose sanctions on the attacker.

5. DISCUSSION AND CONCLUSION

All individuals and institutions using the Internet can be exposed to different attacks every day in today's informatics world. Many of these attacks to the systems, websites and software, such as denial of service, temporary or permanent blocking of service, information theft, attacks for changing information and so on have become popular through "Social Engineering", which is performed to determine the tendencies of the individuals. Trojans are divided into different classes according to their intended use. The most common known trojans are malicious software that provides remote access to the victim system and hands over its control to the attacker. RAT allows attacker to perform many operations such as file import-send-delete, data display, and so on.

The "Locker BLUE (Marvel Avengers Alliance) 15-05-26.exe" malware, analyzed in this study, is one of the most widespread RATs. This malware designed to steal user's personal information can perform many operations (file download-send-delete, data display) in the victim system (Table 2 and Table 3). With the technical analysis of the malware, the characteristics of the malware can be identified and the attacker's Whois information can be found as a result of the analysis. In this

study, a real RAT attack ("Locker Blue (Marvel Avengers Alliance) 15-05-26.exe") was investigated in detail. Behavior of the malware was analyzed in detail using static and dynamic analysis. In addition, it was shown as a result of the study that the server connected through RAT was traceable through its whois information. There is a need for a comprehensive solution that eliminates security threats and vulnerabilities against malicious attacks that become increasingly more dangerous for companies and people. Various products developed for this purpose provide temporary protection against periodic threats. Known antivirus software and sandbox solutions fail to a large extent to combat new generation RATs in practice. The attackers can easily overcome the intuitive and behavior based automatic analysis mechanisms by the methods they have developed. In order to prevent this, an effective fight plan is proposed that include three stages to be aware of the threat and stop it before it becomes a problem. These are: i) Awareness, ii) Preventive action and iii) Restore to normal.

i) Awareness: The best defense against the attacks begins with awareness of the threat. It should be noted that human is the first line of defense against attacks. A conscious human resource is the basis for the security of the systems in any institution or organization.

ii) Preventive action: Malware developers can often reach their goals by making use of out-of-date software with known vulnerabilities and by silently infecting users' systems. If the user frequently updates his/her software in the system, it can be said that the system is more protected against the malware infection. Regularly updated, highly customized antispam protection is an effective measure against malware attacks. Attackers often target machines that use Remote Desktop Protocol (RDP) to remotely connect to systems. Attackers are known to log on to the target system with RDP and disable security software. Some security software has tools to defend against disabling, but it is best to disable RDP if it is not used. The most typical infection method of malware is the sending of e-mails and messages that seem to be harmless at first glance. They should get training to ensure that they do not click on links in e-mails and messages from unknown addresses and their awareness should be increased in this regard.

iii) Restore to normal: One of the most valid defenses against malware attacks is backup and data recovery. It would be useful to take regular backups in another medium against the attempts of the attackers to harm and delete valuable files of the users.

Not using the "save password" option in systems and changing passwords at regular intervals are good measures against password thefts. Users should always take the measures for the "Worst-Case Scenario".

REFERENCES

[1] Luo, Xin, and Qinyu Liao. Awareness Education as the Key to Ransomware Prevention, Information Systems Security, Volume 16, No 4, Pp.195-202, 2007.

[2] Xiao, K., Forte, D., Jin, Y., Karri, R., Bhunia, S., & Tehranipoor, M. Hardware Trojans: Lessons learned after one decade of research. ACM Transactions on Design Automation of Electronic Systems (TODAES), Volume 22, No. 1, Pp. 6, 2016.

[3] Kadir, Andi Fitriah Abdul, Natalia Stakhanova, and Ali A. Ghorbani. Understanding Android Financial Malware Attacks: Taxonomy, Characterization, and Challenges. Journal of Cyber Security and Mobility, Volume 7, No. 3, Pp.1-52, 2018.

[4] Saracino, A., Sgandurra, D., Dini, G., & Martinelli, F: Effective and efficient behavior-based android malware detection and prevention. IEEE Transactions on Dependable and Secure Computing, Volume 15, No.1, Pp. 83-97, 2018.

[5] Javaheri, Danial, Mehdi Hosseinzadeh, and Amir Masoud Rahmani. Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-Level System Routines. IEEE Access, No. 6, Pp.78321-78332, 2018.

[6] Gupta, B. B., Tewari, A., Jain, A. K., Agrawal, D. P. Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications, Volume 28, No12, Pp. 3629-3654, 2017.

[7] Shahzad, Raja Khurram, Syed Imran Haider, and Niklas Lavesson. In Availability, Reliability, and Security, 2010. ARES'10 International Conference on IEEE, Pp. 295-302, 2010.

[8] Wu, Ming-Wei, and Sy-Yen Kuo. Examining Web-based spyware invasion with stateful behavior monitoring. In prdc. IEEE, Pp. 275-281, 2017.

[9] Petkovic, G. M., Basicevic, I., Kukolj,D., Miroslav Popovic, M. Evaluation of Takagi-Sugeno-Kang Fuzzy Method in Entropy-based Detection of DDoS attacks. Computer Science and Information Systems, Volume 5, No 1, Pp.139-162, 2017.

[10] Froomkin, A. Michael. Article 2B as Legal Software for Electronic Contracting-Operating System or Trojan Horse? Berkeley Technology Law Journal, Pp.1023-1062, 1998.

[11] Provos, N., McNamee, D., Mavrommatis, P., Wang, K., Modadugu, N. The Ghost in the Browser: Analysis of Web-based Malware. HotBots, Volume 7, No 4, Pp. 4, 2007.

[12] Liang, Y., Peng, G., Zhang, H.,Wang, Y. An unknown trojan detection method based on software network behavior. Wuhan University Journal of Natural Sciences, Volume 18, No 5, 2013, Pp.369-376, 2013.

[13] Spalka, Adrian, Armin B. Cremers, and Hanno Langweg. The fairy tale of'what you see is what you sign'-trojan horse attacks on software for digital signatures. In Proceedings of the IFIP WG, Volume 9, No 11.7, Pp. 75-86, 2011.

[14] Al-Gburi, Qusay A., and Mohd Aifaa Mohd Ariff. Dynamic Security Assessment for Power System Under Cyber-Attack. Journal of Electrical Engineering & Technology, Pp.1-11, 2019.

[15] Gadhiya, Savan, and Kaushal Bhavsar. Techniques for malware analysis. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Pp.4, 2013.

[16] Zhang, Zhiyong, and Brij B. Gupta. Social media security and trustworthiness: overview and new direction. Future Generation Computer Systems 86, 2018), Pp. 914-925, 2018.

[17] Alwagait, Esam, Basit Shahzad, and Sophia Alim. Impact of social media usage on students academic performance in Saudi Arabia. Computers in Human Behavior, 51, 2015, pp.1092-1097.

[18] Chakraborty, Rajarshi, Claire Vishik, and H. Raghav Rao. Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. Decision Support Systems, Volume 55, Pp. 948-956, 2013.

[19] Khan, Gohar Feroz. Social media-based systems: an emerging area of information systems research and practice. Scientometrics, Volume, 95, Pp. 159-180, 2013.

[20] Jurek, Anna, Maurice D. Mulvenna, and Yaxin Bi. Improved lexicon-based sentiment analysis for social media analytics. Security Informatics, Volume 4, Pp. 9, 2015.

[21] Zolait, A. H. S., Al-Anizi, R. R., Ababneh, S., BuAsalli, F., Butaiba, N. User awareness of social media security: the public sector framework. International Journal of Business Information Systems, Volume 17, Pp.261-282, 2014.

[22] Sowriraghavan, Abinaya, and Pete Burnap. Prediction of Malware Propagation and Links within Communities in Social Media Based Events. In Proceedings of the ACM Web Science Conference, Pp. 59, 2015.

[23] Ali, Syed Taha. Bitcoin: Perils of an Unregulated Global P2P Currency (Transcript of Discussion). In Cambridge International Workshop on Security Protocols, Pp. 294-306, 2015.

[24] Krombholz, K., Judmayer, A., Gusenbauer, M., & Weippl, E. The other side of the coin: User experiences with bitcoin security and privacy. In International Conference on Financial Cryptography and Data Security, Pp. 555-580, 2016.

[25] Stafford, Thomas F., and Andrew Urbaczewski. Spyware: The ghost in the machine. The Communications of the Association for Information Systems, Volume14, No1, Pp. 49, 2004.

[26] Jiang, Dan, and Kazumasa Omote. An approach to detect remote access Trojan in the early stage of communication. In Advanced Information Networking and Applications (AINA), IEEE 29th International Conference on IEEE, Pp.706-713, 2015.

[27] Chen, Zhongqiang, Peter Wei, and Alex Delis. Catching remote administration trojans (RATs). Software: Practice and Experience, Volume 38, No.7. Pp. 667-703, 2008.

[28] Adachi, Daichi, and Kazumasa Omote. A host-based detection method of remote access trojan in the early stage. In International Conference on Information Security Practice and Experience, Pp.110-121, 2016.

[29] Marchetti, M., Pierazzi, F., Colajanni, M.,Guido, A. Analysis of high volumes of network traffic for Advanced Persistent Threat detection. Computer Networks, Volume 109, Pp.127-141, 2016.

[30] Brewer, Ross. Advanced persistent threats: minimising the damage. Network security, Volume 4, No 4, Pp.5-9. 2014.

Information about the authors:

Dr. İlker KARA - Dr. İlker KARA is a Lecturer in the Department of Computer Engineering at the University of Hacettepe, where he has been a faculty member since 2017. Dr. Kara completed his Ph.D. at Gazi University, 2015. His research interests lie in the area of digital investigation, forensics and internet security. He has collaborated actively with researchers in several other disciplines of computer science, particularly forensic security.

Dr. Murat AYDOS – Dr. Murat Aydos received the B.Sc. degree from Yildiz Technical University (Turkey) in 1991, and M.S. degree from Electrical and Computer Engineering Department, Oklahoma State University (USA), in 1996. He completed his Ph.D. study in Oregon State University, Electrical Engineering and Computer Science Department in June 2001. Dr. Aydos joined Informatics Institute @ Hacettepe University in April 2013. He is the Head of Information Security Division at the Informatics Institute. Dr. Aydos is the author/co-author of more than 30 technical publications focusing on the applications of Cryptographic Primitives, Information & Data Security Mechanisms.

Manuscript received on 25 January 2019