SOUND-BASED COMMUNICATION IN THE PROCESS OF MALWARE DISTRIBUTION

Ján HURTUK, Branislav MADOŠ, Štefan HALČÍN
Department of Computers and Informatics, Faculty of Electrical Engineering and Informatics,
Technical University of Košice, Letná 9, 042 00 Košice, Slovak Republic, tel. +421 55 602 3023,
e-mail: jan.hurtuk@tuke.sk, branislav.mados@tuke.sk, stefan.halcin@student.tuke.sk

ABSTRACT

This article describes a case study dealing with the analysis of the evolution of malicious software from its beginning to the part. It examines the behaviour and weaknesses and the conclusion of this analysis antics the most important indicators of the effectiveness of its activities, the self is devoted to experimental method of communication by sound waves of frequencies outside the audible spectrum.

Keywords: *Virus, speed, persistence, sound-based, solutions*

1. INTRODUCTION

The issue of malware today is a very hot topic both for the user as to the progress of technology in the world today come increasingly better ways to exploit users. Also, the fight against this type of crime is very difficult, since the attacker just focus on one particular vulnerability, the companies involved in the fight against this crime must manage the security of many components of the various systems and how the software as well as hardware level. Therefore, this work is not only a new study on the possible vulnerability, but also sheds new light on this issue and shows more potential access to abuses of all kinds. The conclusion of this analysis are basis points, which are characteristic and guidance for each malicious software and the fulfilment of which should guarantee high efficiency of its operations. Raised the issue so therefore become the area of communication, then the control and management as a precondition. Drawing conclusions, it is an issue of greatest priority. The purpose of the thesis is therefore to develop a new way of communication software platform, which uses the current user; therefore, this virus is the most widely used Windows as the operating system. In addition to implementing client-server communication form were added to the program drives characterizing viruses to simulate the operation of the behaviour of the virus and spread. These drives have been added to allow for this communication to consider the effectiveness of using it under standard conditions, but the use of the attacker. Also, when analysing topics and audio signal processing were considered other options that domain when used in criminal activities, as reflected in the discovery of low frequency sound as the source of a direct attack on the user.

2. ANALYSIS OF CONDUCT OF MALWARE

Today, the original computer viruses and other malicious software was developed for highly specialized network applications that are constantly changing and influencing the development of a view of computer security. The very issue of harmful applications is very broad and forwards, that the authors of these applications are very motivated and patient in their efforts. It is also possible for many of them to find an organized group. A goal of such attacks is becoming a large amount of information and organizations. In order to understand the work and functioning of the viruses we look into the past, to the development and functioning. Strategy for attacks by malicious software developed and different enough that they can be described as a patient, multi-step process using system vulnerabilities, malware eventually escalating to coordinated attacks on corporate or other networks.

The key elements of modern strategy of attack are therefore

- The ability to infect the target system
- Ability of persistence
- Communication
- Possibility of management and control

3. EVALUATION OF VIRUS DEVELOPMENT AND CURRENT PROBLEMS

From the previous analysis we also show that industry creation and exploitation of viruses, OS groin and software is constantly evolving, moving forward and constantly brings new threats and challenges. You can also see the rule by which viruses using advanced techniques are difficult detectable and traceable. The same also applies to the fight against this threat. The more sophisticated and efficient products and AV software uses the higher the percentage of threats to detect. This dependence us also represents the following figure.

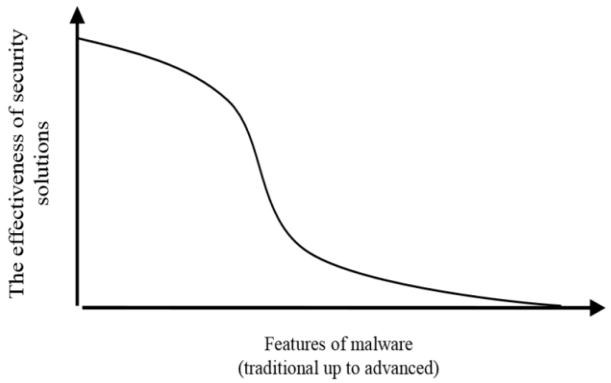

Fig. 1 Dependence of the finding speed based on used technologies

The current state of malware today is vastly different than in the past. Viruses are not used manner as used before. Today, they are instruments of act called cyber-war. They are becoming more sophisticated and advanced and are found in places for them even a few years ago were not available. Therefore for deeper understanding of the need to understand and analyse their development to the state in which we find them today. It also helps us to understand the next generation of viruses and its orientation, analysis of current most widespread threats. After reviewing the selected viruses, we have a question, how to sort and fight viruses nowadays. Unfortunately division threat is not clear as ever and thus the fight against cybercrime this kind is challenging. According the previous chapter provided a solution how to use equipment in a well-secured network, which will (temporarily) averted or limited activity of the virus so that the author can either not be able to drive, the virus will not be able to communicate with their copies in the network, or not can activate or upgrade and thus cease to be active.

4. DEFICITS AND PROPOSED SOLUTION

From previous text we show a number of shortcomings, as well as benefits. If you take a closer look at four main attributes that characterize malware and their activities: Infection, persistence, communication, management and control.

4.1. Pervasiveness

This feature strongly depends on the interaction and activity of the user, today the most powerful tool social engineering. Which uses human interaction and human as the highest risk factor on security.

4.2. Persistence

Defines the ability of malware being seen by the operating system. What used advanced techniques and various exploits allowing direct intervention in the system and its parts.

4.3. Communication

Communication should ensure that information obtained from victims of the attacker were received. In the case where the activity is not performed in most cases the attacker's activity is focused only on the victims of damage or misuse of equipment for further malicious activity on the network.

4.4. Management and control

In my view, it is the most critical point functionality. The reason is that malware to expand successfully hide it in the system, but who cannot drive very quickly becomes uncontrolled and easily guessable. From the perspective of the attacker must have control over their work, especially if it is a more advanced viruses where action can be variable. If, therefore, if there is a loss of control over recurring activities and thus detection, or the undesirable activities which may lead to a waste of resources striker, or in the case of malware aimed at collecting data to complete disablement software. There exists many different options for communication that an attacker can use to their advantage.

From the above we therefore follows that every attribute necessary for correct operation of malware, that malware can in some way deal. Introduce measures to improve persistence, optimize code and implement polymorphism. Alternatively select multiple species distribution and use advanced techniques such as social engineering and social networking. It is necessary, however, to ask what in the event when the user disconnects from the network device.

Or suppose a situation where the device is a multipurpose virus infects a USB device, but its activities will be controlled optionally initialized because the device is closed, or any network. How to ensure a given virus, some basic commands to work. I therefore consider it appropriate to find a new way of communication between devices if they are not available conventional methods.

In this way, a one-way communication via sound broadcasting and its subsequent analysis, which will be described in the following chapters.

5. PROPOSAL OF SOUND-BASED COMMUNICATION

To be able to use sound for communication purposes malware is necessary to determine the key factors affecting communication. These are the:

- What kind of communication we use (centralized / P2P)
- In what sound spectrum communication will take place
- How will the signals decoded and translated the necessary instructions
- What will be the impact and use of the communication, its limitations

The biggest limitation of the communication is that it is a one-way communication, which can only receive instructions and you cannot acknowledge receipt of the instructions, may well confirm its performance. Of course, for this communication would be possible to create a feedback manner similar where sending machine possessed a dictionary of possible responses. But in that case, it would be necessary to work with a precisely timed communication. Possibly find a more appropriate alternative coding and broadcast frequencies.

It also has the communication and hardware limitations, as the host of the major limitations of the communication is that it is a one-way communication, which can only receive instructions and you cannot acknowledge receipt of the instructions, may well confirm its performance. Of course, for this communication would be possible to create a feedback manner similar where sending machine possessed a dictionary of possible responses. But in that case, it would be necessary to work with a precisely timed communication. Possibly find a more appropriate alternative coding and broadcast frequencies. It also has the communication and hardware limitations, since the receiving device must have attached or integrated microphone is necessary to have attached or integrated microphone.

6. DESIGN OF SCHEME OF SPREADING

An attacker could the system, or a specific network infected need to know the topology, systems and equipment that are in it, whether individual vulnerabilities allowing penetration. There are many options of attack and infection of the system or network. In this case, the possibility appears to be the most effective use of social engineering for the initial infection of the system with energy worm characteristics, that is, the spread of a local network.

When doing so it is especially appropriate to infect systems satisfying the condition of homogeneity. And this infiltration, I chose as the main element social Engineering.

According to [1] is a type of social engineering attack exploiting manipulate people in order to perform certain actions (e.g. launch of a file) or to obtain certain information. Social engineering can take place in person, through the means of communication (phone, mail, ...) or by editing environment (such as abandonment media in an accessible place). Defence against all forms of social engineering is almost impossible. As mentioned above, social engineering aims at handling the user to enable the activity needed to carry out infiltration. An example might be induced to launch a fake file means that the user has no knowledge that there was infiltration. When you run a specific set of forged get the right system at the level of what was allocated to the user. To provide the user credible explanation as to why should the file to run, even to ask for the highest possible authorization to access the system and user access is granted to us. The biggest advantage in using this type of infiltration is the existence of web storage, and a trend to share illegal content such as audio, video, software or pornography. Disguise the file as one of the most frequently searched files, ensure him a good assessment of virtual users who also will create only opinion in order to manipulate the target of attack. In the attached table you can find a comparison of individual files and efficiency of downloading users.

Table 1 Types of shared files for the purposes of social engineering

File Type	Description	Downloads for a period of 7 days
Title by a random selection of server	Randomly selected file that was attractive to the average user	5
Title consistent with most downloaded file	The name was choosen according to the most downloaded file	23
Name and type consistent with most downloaded file	To the file name was added extension identical to the original file, too.	149
Filename adapted to the demand	The file name was the same, yet unavailable online	73

7. PROPOSAL FOR IMPLEMENTATION

The point of the operation consists in an infinite loop, which is the first step to verify the existence and thus the instance of malware on your device. Later verify internet connection optionally with C & C server management. Based on the possibility of creating such a link shall be given to the management of that administrator's instructions. The processing instructions that come either from the managing authority, or passively waiting to receive instructions outside the audible range. They translated and performed. Then come the update to the number of different operations, such as the updating source code, etc.

7.1. IRC communication

This type of communication is a fundamental communication with the C & C server management, where the virus attaches to specific IRC channel and thence "read" communication and acts as a regular user. Communication however, apart from reading and translating the key for instruction that controls its activity. Of course, while ensuring that communication is necessary based on official documentation IRC referred to [2] for the proper processing of incoming messages and correct formatting of outgoing messages.

7.2. B. Sound and its translation to the instructions

Basic routine translation of the instructions depends on the aforementioned facts, and a loss of network access and inability to communicate with the management server. To occur this problem starts with a block of code management using sound. He waits for the called. startup phase, which may be a specific time interval of disconnection, time stamp, or incident in the system. Decoding consists of filtering out the sound of the waves, which falls outside the range used by us. Of course, the processing is counted and the noise, dispersion and distortion. So it does not filter only sound directly corresponding to 16KHz, but leaves the sound in the range 15.5 - 16.5 KHz. After filtering unnecessary extent determines the duration of each sequence, appropriate duration of one particular of them and that is based on the length of the code assigned to a specific instruction in the tree. Of course, there are foreseen deviations. And therefore the time for which assigns specific instructions considered only approximate values. The resulting translation instructions also depends on the sound card settings where the user changes the configuration, quality and sampling frequency.

7.3. Audio broadcast

Sound broadcast as follows. Sets the number of iterations broadcasting, ie the number of signals to be transmitted. Sets the frequency at which I will be broadcast. Then adjust the length, ie code instructions for each iteration, ie. signal for each instruction. Then determine whether the available hardware built-in speaker on the motherboard devices when not transmitting on the external speakers. You have not distinguish between speakers connected through connector or speakers built into the laptop. This finding helps nm, If there is an OS from where you use the speaker motherboard prohibited, optionally, where the user does not have sufficient rights to use this speaker.

7.4. Malicious activity

The imitation of malicious activity were selected features command line so as to ensure the best compatibility for Windows, which in our case is an insertable from Windows

2000 to the current version. We also use the function directly access system services to rights as assigned by the user when starting the application or if the user owns the highest administrator privileges and application downloads these privileges. In the event that the application would not be guaranteed the right still following commands have sufficient power to carry out their primary activities.

8. CONCLUSIONS

I propose a solution for communication by sound waves between devices infected by this type of virus, provided that the results of the questionnaire can be taken as a representative sample proved to be very competitive. It can therefore be considered as an alternative to communication via the Internet network.

In the case of real deployment in service, so if I was able to infect a larger area so that it can further spread of it seems to me that such a virus would be successful and could actually survive in the current user environment. An interesting finding in the processing of the issue of using audio frequencies outside the range of human perception was that when using waves at the lower limit of hearing frequencies thus belonging to infrasound can cause physiological changes in the functioning of the human body and mental problems. It is a sound of a wavelength of 20 Hz and below. But even sounds a little above that threshold may bring the same result. In this case it is necessary to long-term effect of such a sound. Specifically, the research addresses this issue prof. Ţiaran and information to which it refers come from work [3], which examines the impact of routine sounds like an open window in the car while driving on the changes in physiology.

The most known sound effects and noise on the human body include the impact of noise on blood pressure and in the long-term effect subsequent formation of hypertension (ie. Increased blood pressure), which may develop into chronic problems. Prof. Ţiaran is based on sound pressure caused by noise, and for each value describes the level of damage so severe that it may be well to heart.

The most important fact is that the noise of the lower frequency has a much greater severity than medium and high frequencies. A powerful low-frequency sound may also be replaced by a weaker sound but a longer time, i.e., the user would be exposed to the sound for a long time.

ACKNOWLEDGMENTS

This work was supported by the Slovak Research and Development Agency under the contract no. APVV-0008-10 and KEGA 008TUKE-4/2013 Microlearning environment for education of information security specialists. The projects are being solved at the Department of Computers and Informatics, Faculty of Electrical Engineering and Informatics, Technical University of Košice.

REFERENCES

[1] Csirt.sk, (2014). [online]. [cit. 2014-12-11]. Available at: <https://www.csirt.gov.sk/osvedcene-postupy/navody-aodporucania/socialne-inzinierstvo-812.html>.

[2] irchelp. [online]. [cit. 2014-12-2.] Available at: <http://www.irchelp.org/irchelp/rfc/chapter4.html>.

[3] ŢIARAN, S.: (2013). Low Frequency Noise and Its Assessment and Evaluation, [online]. [cit. 2015-3-2]. Available at: <http://acoustics.ippt.pan.pl/index.php/aa/article/view/42/41>.

[4] VOKOROKOS, L. – BALÁŽ, A.: Architecture of computer intrusion detection based on partially ordered events / Liberios Vokorokos, Anton Baláž - 2010. In: Petri Nets : Applications. - Vukovar : In-Tech, 2010 P. 13-28 [1,1 AH]. - ISBN 978-953-307-047-6

[5] VOKOROKOS, L. – CHOVANCOVÁ, E. – RADUŠOVSKÝ, J. – CHOVANEC, M.:A Multicore Architecture Focused on Accelerating Computer Vision Computations / Liberios Vokorokos ... [et al.] - 2013. In: Acta Polytechnica Hungarica. Vol. 10, no. 5 (2013), p. 29-43. - ISSN 1785-8860 [online]: http://www.uni-obuda.hu/journal/Issue43.htm...

Received July 20, 2015, accepted August 25, 2015

BIOGRAPHIES

Ján Hurtuk (Ing.) was born on 4th October 1988 in Kežmarok. In 2013 he graduated (MSc.) at the Department of Computers and Informatics at the Faculty of Electrical Engineering and Informatics of the Technical University of Košice. Since 2014 he is studying as a PhD. student at the Department of Computers and Informatics at the Faculty of Electrical Engineering and Informatics of the Technical University of Košice. His scientific research is mainly focused on the computer security.

Branislav Madoš (Ing., PhD.) was born on 20th May 1976 in Trebišov, Slovakia. In 2006 he graduated (Ing.) at the Department of Computers and Informatics at the Faculty of Electrical Engineering and Informatics of the Technical University of Košice. He defended his PhD. in the field of Computers and computer systems in 2009; his thesis title was "Specialized architecture of data flow computer". Since 2010 he is working as an Assistant Professor at the Department of Computers and Informatics. His scientific research is focused on the parallel computer architectures and architectures of computers with data driven computational model.