ANALYSIS OF MODERN ATTACKS ON ANTIVIRUSES

[1]SILNOV DMITRY SERGEEVICH, [2]TARAKANOV OLEG VLADIMIROVICH
Department of Information Systems and Technologies, National Research Nuclear University MEPhI
(Moscow Engineering Physics Institute), Moscow, Russia
E-mail: [1]ds@silnov.pro , [2]o-tar@yandex.ru

ABSTRACT

Modern malware (viruses, worms, and Trojan horses) are increasingly applying integrated approach inherently and combining multiple technologies to counter the actions of antivirus software and information security tools. Lack of specific classification of directions of counteraction and their approaches creates no clear idea of the degree of threat. This leads to solutions that cannot fully eliminate a threat. This article considers the first ever case of classifying counteraction methods to antivirus actions. The classification presented identified two main approaches of influencing antivirus actions: targeted and non-targeted attack. After analysing the methods, we classified false positive virus alarms based on which it is shown that false positives are systemic in nature.

Keywords: *Antivirus, False Positive, Viruses, Retroviruses, False Negative*

1. INTRODUCTION

As antivirus tools get more sophisticated, viruses are following two directions: either to avoid interaction with the antivirus software or to counter it. Avoiding interaction or, in other words, ensuring co-existence between the virus and antivirus software is quite an extensive and elaborated issue. Malware developers often follow this path, based on the fact that each individual computer system is just a single element and loosing it, in particular, due to successful detection by the antivirus software, is a matter of time and the loss of that computer system is not that critical. The situation is different when each individual computer system is of vital importance to the hacker, meaning that active measures need to be taken, i.e. to counter the antivirus software in order to ensure that the virus runs in the system on its own as long as possible. One of such directions is to generate false positive.

To analyze the existing problem of false positives, one needs to consider earlier-occurred cases of false positives and their causes, as well as classify the possible methods of attacking antivirus tools.

2. CLASSIFICATION OF METHODS OF COUNTERING ANTIVIRUS ACTIONS

Thanks to the technological efficiency of antivirus systems in fighting viruses, the latter are increasingly using multiple technologies simultaneously to counter antivirus tools. Counteraction methods can be divided into two main areas, each of which is well represented. Since attacks on antivirus tools are usually direct and indirect in nature, you can classify two basic approaches depending on the methods of influencing the antivirus tools: targeted and non-targeted attack.

The essence of non-targeted attack boils down to the fact that one can classify such approaches by identifying separate areas of counteraction (Figure 1).

Non-targeted attacks are such attacks, whose targets are not antivirus files or processes. In fact, they attempt to secure passive resistance by trying to hide their own presence in one form or another, and not compromising antivirus processes. The following are some non-targeted attacks:

• Generation of files with virus signatures. The aim of such behavior by viruses is to attempt to conceal their own files among other specially generated virus files. This technique can be successful in cases where it is impossible to hide own presence from antivirus, but it is possible to prevent detection of that type of virus among a host of other signatures.

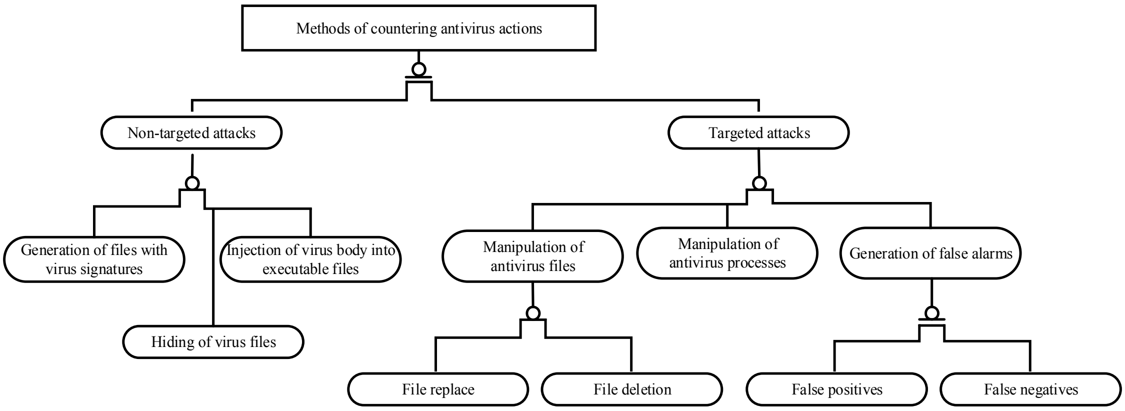
Methods of countering antivirus actions
Non-targeted attacks
Targeted attacks
Generation of files with virus signatures
Injection of virus body into executable files
Hiding of virus files
Manipulation of antivirus files
Manipulation of antivirus processes
Generation of false alarms
File replace
File deletion
False positives
False negatives

Figure 1: Classification Of Methods Of Countering Antivirus Actions

• Hiding of virus files. Another approach is an attempt by the virus to conceal its own files or the files of its own modules or additional files that need to be hidden from the antivirus tool. Modern developers of rootkit virus are moving in this direction. These developers inject third-party software (which is not part of the rootkit virus) for a fee. The purpose of this software is often to obtain money from the user under various pretexts. Along with simple "injection", the developers can also for a fee help hide individual files.

• Injection of a virus body into executable files. A virus body is injected into executable files to execute a certain code purportedly by that process in order to hide suspicious activity. It is quite possible to inject a virus into the iexplore.exe process of the Internet Explorer browser to execute network requests and receive responses, such as those containing control commands from the control center. The main objective of this approach again is not to counter the antivirus tool, but to ensure that the virus functions and avoids being blocked by a firewall or antivirus tool.

The second counteraction area involves targeted impact methods – the virus directly acts on antivirus files or processes. The purpose here is not only to hide the existence of the virus in the system, but in some cases, to inactivate the antivirus system or compromise it in the eyes of the user. This could make the user disable the antivirus tool by himself. We will consider targeted impact methods in detail. Such methods include:

• Modification of the configuration and system files of an operating system and antivirus tool, such as the hosts file with the aim of blocking communication with antivirus sites [1]. This approach is used not only against antivirus tools, but also to block requests for license activation of other software products. Regardless of target, the purpose is to prevent network interaction via false DNS server permissions. This approach is ineffective if IP address rather than symbolic name is used for network communication. Virus developers themselves often use this technique, although it has certain limitations and inconveniences.

• Removal of antivirus files [2]. This approach is one of the most targeted attacks, whose purpose is to completely remove the antivirus tool from the system. However, practical implementation is often not possible, either because of self-defense by antivirus programs or because of lack of necessary access rights (for example, right to remove operating system kernel drivers/modules.

• Termination of antivirus processes. This approach is possible only if the necessary access exists to enable terminate third-party processes currently running under the operating system. Most often, this involves a simple comparison of the list of running processes in a predetermined pattern of their names and termination of processes if necessary [3].

• Generation of false alarms – false positives and false negatives.

Modern antivirus tools can efficiently deal with most classified methods of attack – both targeted and non-targeted.

The situation is different with false positives. Antivirus software developers regard part of false positives as random events, without considering the possibility of intentional targeted manipulation aimed at creating false positives. Therefore, research in the field of generation of false positives as one of counteraction methods to antivirus tools is relevant and necessary.

3. ANALYSIS OF FALSE POSITIVE VIRUS ALARMS

Intermittent errors in signature databases, in the code of the antivirus tool or in file compression and encryption algorithms used frequently used by antivirus tools are the main cause of false positive virus alarms. Depending on the virus detection technology – heuristic method using certain patterns of virus behavior or signature-based analysis using the signature database – the problem of false positives is inherent in both approaches. This is due to the features of these methods. Eliminating false positives completely is impossible. However, if a heuristic method is based on the elements of a scoring system regarding the patterns of behavior of the analysed processes that are not clearly and rigidly predetermined, while the final decision is determined by summing up a number of parameters, then the signature-based method is completely deterministic, and a clear comparison based on the signature database is used.

In this regard, it is expedient to analyze the signature method, identify the direction of false positives that arise in the course of applying this method and determine to what extent are false positives considered as a virus threat during an attack on the antivirus tool. Signature-based false positives should be classified in two main ways – deliberate or accidental (Figure 2). Let us consider each of the options in more detail.

2.1 Signature-Based Type I And Type II Errors

False positives (type I errors) are common. The variety of application software makes the probability of signatures coinciding during a failed signature allocation procedure by the employee of the antivirus company very high.

The situation is different for false negatives (type II errors). Signature-based method is elaborated in terms of the algorithm, and if the antivirus in the test lab sees a virus signature in the file, then in the same file the antivirus tool will see that signature in any other conditions. If such specialized technologies as, for example, obfuscation or polymorphism, are applied, then it is not entirely correct to talk about type II error in such a situation for the reason that the algorithm is working correctly, and another file in fact needs to be analysed.

2.2 Random False Positives

Analysis of cases of false positives has found that antivirus software developers consider bugs in signature databases or in antivirus algorithms as the cause of such errors. As for bugs in signature databases, it is usually the fault of that employee whose duty includes identifying signatures from a virus file. This procedure is not clearly formalized – cannot be performed automatically – meaning that errors may occur due to human factor. The consequences are different:

- Removal of harmless software seen by the antivirus tool as malicious due to a bug in the signature database [4]

- Malfunctioning of the operating system due to removal of its critical system files [5].

- Deactivation of the antivirus tool due to removal of its own files [6]

As can be seen, the consequences of such errors are serious and in some cases fatal. When it comes to critical information, such errors are inadmissible.

Even a more serious situation and, consequently, more serious consequences is when such false positives are not accidental, not caused by a one-off human error or bugs in algorithms, but are created intentionally.

2.3 Deliberate False Positives

Antivirus software developer, evaluating possible virus threats, do not pay due attention to deliberate generation of false positives. There are several reasons for this. First, this is due to the fact that modern antivirus tools monitor disk operations in real time, which means, in the opinion of antivirus developers, these tools have complete control over the contents of the disk. Secondly, if virus developers set themselves the goal of

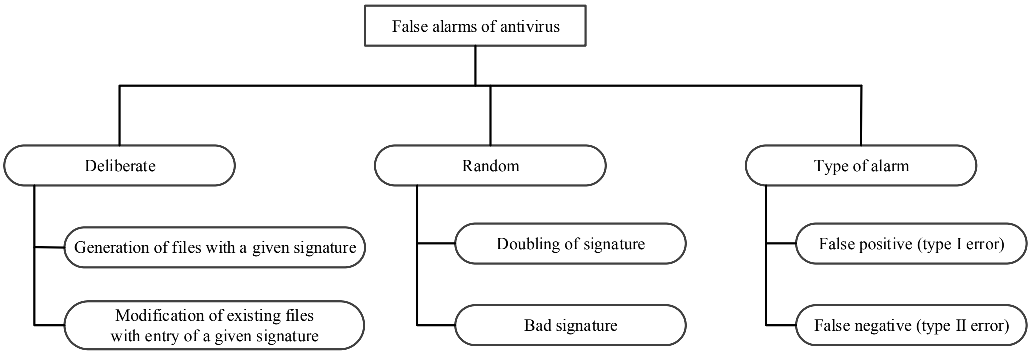
False alarms of antivirus
Deliberate
Generation of files with a given signature
Modification of existing files with entry of a given signature
Random
Doubling of signature
Bad signature
Type of alarm
False positive (type I error)
False negative (type II error)

Figure 2: Classification Of Signature-Based False Positive Virus Alarms

countering antivirus tools, the methods to be used to solve this task boils down to deactivating the antivirus tool as a whole, and not distorting its operations. However, deactivating the antivirus tool is not that productive because if the tool stops working, it will be easily noticeable not only by the technical personnel but also by the ordinary user. Relatively successful antivirus countering technologies through generation of false positives existed just before real-time disk control features were introduced in antivirus tools. Let’s consider the approaches that have been used both previously and in the present time, but only approaches to those antivirus tools that do not have disk control features.

Generation of files with a given signature. This approach involves a one-off or systematic (at specified intervals) creation of files with virus signatures within an existing file system. The generated files are placed usually in an arbitrary manner, but the purpose of such action is to ensure maximum coverage of the file system. For example, if an antivirus program performs only periodic scanning of the file system for malicious objects, this approach can be successful since the antivirus program will each time detect more and more new viruses, which will thus attract the user’s attention. In this case, the source of the files will most likely be found either by the user or by a third-party expert. However, this maximum distribution approach may be effective only if the antivirus program has no real-time disk subsystem control features. If there is such control, attempts to write the file to the file system with a known virus signature will fail because such attempts will be blocked by the antivirus system.

Modification of existing files with entry of a given signature. Various file viruses use this approach, when their bodies are integrated in legal executed files. If you are using antivirus software that have real-time disk control features, this type of virus is also not effective because distribution, i.e, introduction in new files will be blocked if the designated signature is already known to the antivirus program. If the antivirus tool lacks real-time disk subsystem control, then this approach is acceptable. But even in this case, not all executable files can be integrated. Software programs with prior launching self-control features will stop functioning after injection of a third-party code in their files.

Thus, within the framework of the analysis conducted, two main conclusions can be formulated:

1. Generation of false positives is not considered as a possible way of manipulating antivirus tools.

2. Cases of false positives described in open literature are related to only random errors in antivirus software, including errors in signature databases. For this reason, creation of destructive impacts under the guise of signature-based false positives reduces the probability of these impacts being detected.

Information security tools are often commercial products with closed source code. This complicates the ability to analyze protection mechanisms against false positives. Nevertheless, to protect intellectual property, some antivirus product developers patent their approaches to reduce the number of false positives, thus allowing to explore contemporary approaches to solving this problem. In the process of patent search in the databases of Rospatent, WIPO, USPTO, a number of patents (RU107615, EP2278516, EP2441025, WO2007087141, US8028338, US7757292) were analysed, which revealed the essence of modern approaches towards reduction of the number of false positives. All of these approaches come down to identifying and processing facts of false positives, when these facts have already occurred, or in special circumstances, during pre-testing (for example, on a dedicated stand for testing new antivirus databases) or when using an information security system on the client hardware. Therefore, research on methods of countering antivirus tools, including generation of false positives, is relevant and necessary.

REFRENCES:

[1] Net-Worm.Win32.Kido.dv. Retrieved February 7 ,2015, from http://www.securitylab.ru/virus/366642.php.

[2] Trojan.BAT.AnitV.a. Retrieved February 12, 2015, from http://www.securitylab.ru/virus/306301.php.

[3] Trojan-Downloader.Win32.Bagle.z. Retrieved February 12, 2015, from http://www.securelist.com/ru/descriptions/147249/Trojan-Downloader.Win32.Bagle.z

[4] Symantec identifies a NASA program as adware. (2007). Retrieved February 7, 2015, from http://www.cnews.ru/news/line/index.shtml?2007/07/17/259193

[5] Symantec paralizes millions of PCs. (2007). Retrieved February 7, 2015, from http://www.cnews.ru/news/top/index.shtml?2007/05/25/252011

[6] The Avira antivirus identified itself as a virus, Retrieved February 7, 2015, from http://lenta.ru/news/2011/10/27/avira/