Journal of Information Security, **2013, 4, 124-127**
http://dx.doi.org/10.4236/jis.2013.42014 Published Online April 2013 (http://www.scirp.org/journal/jis)

Features of Virus Detection Mechanism in Microsoft Security Essentials (Microsoft Forefront Endpoint Protection)

Dmitry Silnov
Mephi, Moscow, Russia
Email: ds@silnov.pro

Received January 14, 2013; revised February 16, 2013; accepted February 23, 2013

ABSTRACT

In this paper, a signature-based selective mechanism in detecting virus signatures in executable files was found and investigated. A pattern under which the Microsoft Security Essentials antivirus software not detecting a virus signature deliberately placed in files was revealed.

Keywords: Antivirus; Signature-Based Approach; Information Security Software; Digital Signature; Type II Error

1. Introduction

Today, the security of the information systems of public and private organizations is one of the top priorities of developers of information security systems (ISS). ISS isn't only antivirus software, but also firewalls and IDS products. Each ISS developer aspires to create malware detection mechanisms that would more efficiently and promptly detect and neutralize viruses. Despite the fact that virus detection is the main task of any antivirus software, algorithms that lead to this are varied and in some cases, are intellectual property of ISS developers. It is difficult to study these algorithms because of the closed nature of the source code of many antivirusprograms. On the other hand, studying the algorithms will enable to modernize the existing software systems and identify their possible shortcomings.

The author made researches concerning Microsoft Windows kernel. As one of results of that researches some features of virus detection mechanism was found in Microsoft Security Essentials.

2. Approaches to Studying ISS Mechanisms

Source code analysis is the most obvious approach used directly by antivirus software developers. With access to the source code, developers have an undeniable advantage because they know the functioning mechanisms of their software product from within. Provision of funds for payment of staff that would analyze and audit an already created code is not the core costfor an organization since the main task of an antivirus software is to detect virus and not to update the source code. Thus, the problem lies in the fact that from an economic point of view, it is inefficient to invest staff time. Moreover, these are employees with a certain level of access to upgrading of non-core algorithms, though these algorithms are an integral part of the ISS.

Another approach is to interpret the behavior of ISSs based on detection or non-detection of files containing viral parts. Viral parts should be understood to mean either a signature (in the case of studying a signature-based approach to virus-detection), or a separate program elements of viruses that perform operations that can be regarded as suspicious and/or malicious by a heuristic analyzer. This approach is used at least by ISS developers to detect the false positives of their anti-virus products [1].

A third approach proposed in this paper (see the **Figure 1**) is to develop special software programs for analysis and assessment of the effectiveness of antivirus software products.

The software program developed is used to investigate the immunity of antivirus software to false positives. When using this approach in the process of studying Microsoft's antivirus software Microsoft Security Essentials (MSE) [2], it was found that this software behaves abnormally under certain conditions. It should be noted that MSE is a free software product, but Microsoft offers a commercial antivirus software Microsoft Forefront End-

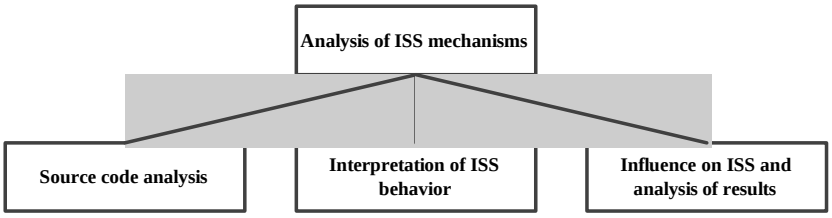

Figure 1. Approaches to the analysis of ISS mechanisms.

point Protection [3] that uses the same anti-malware engine as MSE.

3. Experimental Investigations of Microsoft Security Essentials

The behavioral features observed concern a signature-based approach used by MSE in scanning files for the presence of virus signatures in them. It was found that detection of virus signatures is influenced by the presence or absence of a digital certificate in an executable file. Digital certificates for executable files are used by Microsoft to authenticate software distributed by third-party developers [4]. When there is no digital certificate in an executable file, normal behavior is observed, and virus signatures are rightly detected in the file. When there is a digital certificate in an executable file, the antivirus software shows an unexpected behavior.

With the use of a specially developed software program, an experiment was conducted that revealed a pattern between the presence of a digital certificate and the detection of virus signatures in an executable file. Several executable files located on a test computer running Windows 7 were selected for the experiment. In each of the files selected, a signature was virtually placed so that when reading the given file, the signature replaced a section of the binary code of the file, and when checking the digital certificate, the replacement was not detected. This feature is made possible by a specially designed software program that was created by the author of this paper and will soon be patented. The mechanism of this software program is deliberately not disclosed in details. This software program uses the normal mechanisms of the Windows OS family, and does not break the integrity of the files themselves. The report (see **Table 1**) for this experiment clearly shows that when there is a digital certificate in a binary executable file (exe), the MSE antivirus software does not detect (results Nos. 1 to 11 of the report) the signature placed in the file. When a file is signed with a digital certificate (results Nos. 12 to 16 of the report), virus signature is detected immediately.

An additional experiment was conducted to confirm the behavioral features of the MSE antivirus observed. Let us consider the order of the experiment. A digitally signed file is scanned and the current result recorded. Then, in order to invalidate the certificate, the file is edited and a randomly selected (using HEX editor [5]) character is replaced by another randomly selected one. In doing so, the checksum of the file is broken and as a result, the digital certificate becomes invalid. A repeated scan is carried out and a virus signature is detected. The results of this experiment are presented in the report (see **Table 2**). In the second case, the record "(mod.)" means that the file was modified in accordance with the requirements of the experiment.

4. Analysis of Results Obtained

The results presented reveal a pattern between the presence of a valid digital signature and the detection of virus signature by the MSE antivirus software in executable files. Certainly, an additional and full-scale investigation of this feature is required using legitimately issued digital certificates. Probably, this feature is not observed for all types of digital certificates and for all organizations that have a digital certificate at their disposal. It was found that virus signatures were also not detected in a binary file signed with an expired digital certificate.

Actually, we can talk about expanding the privileges and increasing the trust for signed executable files by MSE, but the limits of such a trust have not been studied thoroughly. An important and relevant question is whether it is possible to spread a digitally signed malware on computers with Microsoft's antivirus software product.

This brings up the question of whether the presence of a digital certificate, from Microsoft's point of view, is a confirmation that the signed software is authentic—at a time when the concept "malware" is often difficult to establish (for example, the so-called "fake antivirus software programs" [6], which offer the user to pay for registration of a product and in exchange his computer will be cleaned of non-existing viruses).

In addition, it should be noted that similar experiments were conducted with the use of other antivirus programs such as Kaspersky Internet Security, Dr. Web, Bitdefender [7], and others. At present, the features described are found only in the antivirus software Microsoft Security Essentials. This is probably because the same organization—Microsoft—develops both the Windows operat-

Table 1. Report No. 1.

No.	File name	Digital certificate	Result
1	HPAuto.exe	Hewlett-Packard Company (expired)	not detected
2	TMExtreme.exe	Arc Soft, Inc. (valid)	not detected
3	mDNSResponder.exe	Apple Inc. (valid)	not detected
4	DTLite.exe	DT Soft Ltd. (valid)	not detected
5	avp.exe	Kaspersky Lab (expired)	not detected
6	opera.exe	Opera Software ASA (valid)	not detected
7	Picasa3.exe	Google Inc. (valid)	not detected
8	uTorrent.exe	Bit Torrent Inc. (valid)	not detected
96	firefox.exe	MozillaCorporation (valid)	not detected
10	iTunes.exe	Apple Inc. (valid)	not detected
11	StarCraft II.exe	Blizzard Entertainment, Inc. (expired)	not detected
12	gyazowin.exe	not signed	detected
13	MegaFon Modem.exe	not signed	detected
14	VKMusic4.exe	not signed	detected
15	xchat.exe	not signed	detected
16	Evernote.exe	not signed	detected

Table 1. Report No. 2.

No.	File name	Certificate	Result
	picasa3.exe	Google Inc. (valid)	not detected
	picasa3.exe (mod.)	Google Inc. (not valid)	detected
	iTunes.exe	Apple Inc. (valid)	not detected
	iTunes.exe (mod.)	Apple Inc. (not valid)	detected
	firefox.exe	Mozilla Corporation (valid)	not detected
	firefox.exe (mod.)	Mozilla Corporation (not valid)	detected

ing system and the MSE antivirus software, and when developing antivirus software, developers are likely to rely on additional knowledge not available to developers of other antivirus software products.

5. Conclusions

The features of the antivirus software Microsoft Security Essentials discovered and investigated show that it is necessary to develop special software tools that could be used for research and analysis of various antivirus software programs. Such research would enable ISS developers improve their own software products and get information about deficiencies in internal mechanisms that could be taken advantage of by malware developers to achieve their interests. On the other hand, it is possible that this MSE antivirus feature is a specially created backdoor that could be used to spread the Stuxnet virus to target computers as this virus was signed with a legitimate digital certificate [8]. Stuxnet virus including sys-file that was signed with a legitimate digital certificate of Realtek Semiconductor Corp., so MSE antivirus didn't notice any illegal activity in signed file because of backdoor described in this article.

Let me specially emphasize that even if it is not connected to the Stuxnet virus, such a feature can be used to spread such viruses.

REFERENCES

[1] D. S. Silnov, "Problems of Antivirus False Positives," Applied Informatics, 2012, pp. 63-66.

[2] “Microsoft Security Essentials—Free Antivirus Software,” 2012. http://windows.microsoft.com/ru-RU/windows/products/security-essentials

[3] “Microsoft Forefront Endpoint Protection, Antivirus Protection against Malware,” 2012. http://www.microsoft.com/ru-ru/server-cloud/forefront/endpoint-protection.aspx

[4] “Introduction to Code Signing,” 2012. http://msdn.microsoft.com/en-us/library/ms537361%28v=vs.85%29.aspx

[5] “WinHEX,” 2012. http://www.winhex.com/winhex/

[6] “Fake Anti-Virus Software and Related Threats, Microsoft Security Center,” 2012. http://www.microsoft.com/ru-ru/security/pc-security/antivirus-rogue.aspx

[7] “Bitdefender Antivirus Software,” 2012. http://www.bitdefender.ru/

[8] “The Stuxnet Sting,” 2012. http://blogs.technet.com/b/mmpc/archive/2010/07/16/the-stuxnet-sting.aspx

