Advanced Engineering Forum *Online: 2011-09-09*
ISSN: 2234-991X, Vol. 1, pp 310-314
doi:10.4028/www.scientific.net/AEF.1.310

Research on Hiding Technology of Web Malicious Code

Deng-yin ZHANG[1, a], Zhen-xing WANG[2, b], Xiao-qiang ZHAO[3]

[1, 2, 3]Key Lab of Broadband Wireless Communication and Sensor Network Technology (Nanjing University of Posts and Telecommunications), Ministry of Education, Nanjing210003, China

[a]zhangdy@njupt.edu.cn, [b]wzx_1987@163.com

Keywords：Web Malicious Code; Virus; Vulnerabilities

Abstract. In modern network confrontation, it is very important to improve the viability of web malicious code. According to the generation and propagation characteristics, we propose the web malicious code hidden solutions which are based on deformation and encryption. Combining with MS09002 vulnerabilities we give an application example of web Trojan hidden. Test results show that the proposed integrated solution has the better capacity of avoiding virus killing and the stronger hidden performance. The significant improvement of viability of web malicious code is very important of application.

Introductions

Web malicious code spreads [1] relying on the system vulnerabilities. Trojan processes of the web malicious code [2] can be divided into two steps: ① Use the vulnerability of URL format to hide IP address which downloaded by Trojan and convert EXE file into HTML file Trojan, then upload both of them to the FTP space. At last upload the converted HTML file Trojan to the page by using the vulnerability of iframe. ② Attackers send link of exploit web page to customers and entice them clicking. After opening a web page, vulnerability is triggered when the browser analyzes malformation data, whose shellcodes [3] are implemented. Trojan is downloaded to the client and run, so an attacker can easily control the horse [4] client through the Trojan interface. In order to enhance the survival of web malicious code and dissemination capabilities, and avoid the detection of network security defense [5], this paper presents the web malicious code hidden solutions which are based on deformation and encryption, and also combines MS09002 vulnerabilities we give an application example of web Trojan hidden.

Hiding Program of web malicious code

In order to avoid network security defense, web malicious code begins to evolve, and once infected with deformation. Trojan [6] hidden is mainly bypassing the network security scanning and defensive behavior-based detection. Signature-based scanning hidden technologies: Trojan deformation technology and encryption technology. Behavior-based detection of hidden technologies: the host Trojans hiding, hiding files technology and hiding processes technology.

A. Deformation of Hiding Technology

In JavaScript syntax, "\ r" means return, "\ n" means that line, "\ t" represents a tab character, "\ 00" indicates that the string end, "\" " means the double quotes," \ number " followed by the octal representation ASC code of the original character, "\ x" followed by the hexadecimal ASC code of the original character, "\ u-byte number" followed by a double-byte number to represent a double-byte character. Such as that you can change “df.setAttribute ("classid "," clsid:

BD96C556-65A3-11D0-983A-00C04FC2 9E36")" into "df.setAttribute("\143\154\141\163 \163\151\144","\143\154\163\151\144:\x42\x44\x39\x36\x43\x35\x35\x36-65\101\63\u002d\u0031 ……"". After using the transfer character, the web malicious code is beyond recognition.

B. Encryption of Hiding Technology

This is common javaScript encryption and encoding as follows. Make the encryption and decryption processing for the code by using the existing functions or writing your own encryption and decryption functions. In order to prevent signature scanning, web malicious code takes this approach to encrypt. Currently there are some better encryption algorithm, such as MD5 [7] and SHA-1 [8].

C. Process Hiding Technology

Web malicious code needs to run separate processes. Computer users can find processes that are not normal through the simple testing tool. It must be causing alarm. In order to hide them, web malicious code uses Rootkit techniques to hide processes.

Windows operating system traverses the current process through the function of EnumProcesses, CreateToolhelp32Snapshot and so on. Applications break into the kernel mode to call KiSystemService to find the SDT in the NtQuerySystemInformation function address, and then call NtQuerySystemInformation to achieve specific functions. Systems interrupt service routines find its address by querying the SDT (Service Descriptor Table).

SDT table is a function address table, and each of its entry points to a system service routine. Interrupts handling routine call the corresponding system service routine by looking up this table. Through hijacking ZwQuerySystemInformation and NtQuerySystemInformation, hidden process technology modifies its return data or deletes the information of hiding process. Modify the NtQuerySystemInformation table of SDT table to point to the adding NewNtQuerySystemInformation routines of a new hidden program, and then the function call the original function to obtain the process, thread information and filter information that need to be hidden.

D. File Hiding Technology

Web malicious code generates the final results through downloading the Trojan to execute by web malicious code, so if we can hide the Trojan's files, it will be better to protect the web malicious code. Technology of hiding files is mainly inline functions patches, and the main idea is to start replacing some bytes of the kernel function by using jmp xxxxxxxx or call xxxxxxxx command to jump to the well-designed Rootkit code. After making the target file hidden, replace the implement code and jump back to the address of kernel function to excute the normal code.

MS09002 Vulnerability Based Web Trojan Hidden Example

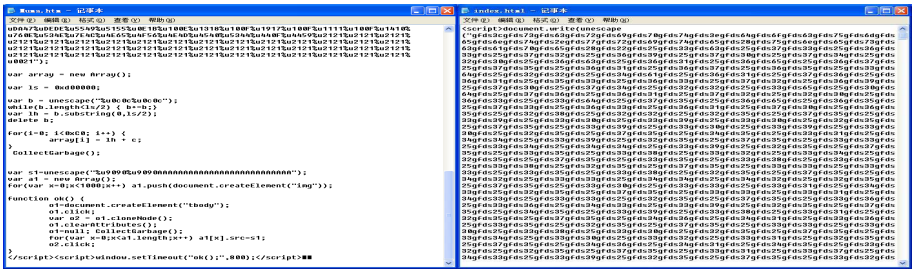
A. MS09002 Vulnerability Analysis

Because of the CFunctionPointer function in Internet Explorer (IE7 and IE8 version) which does not handle document object properly, you can use the special code to trigger the memory broken ring, and then attacker can log on as currently user to execute arbitrary code. MS09002 attack code uses the HEAP SPRAY technical to attack. It causes significant footprint of browser memory, leads normal users not to browse the web and also makes the system on the Trojans.

B. Hidden web malicious codes

We use encryption to evade detection of the Semantics for signature detection and testing. Trojan's signature characteristics are the general web properties functions, such as the document. Write, eval, unescape, fromCharCode, setTimeOut and other functions, and the domain name address downloaded by Trojan. Through the XOR encryption, the feature function sets name

address string disappeared to avoid signature detection. Then we use the escape character deformation method to generate the web malicious code. Change the "\ u-byte number" into all the special symbols to represent the original characters. As follows:



(a) Before encryption (b) After encryption

Fig.1 Shellcode comparison

Before and after the comparison chart from the encryption can be seen, encrypted web malicious code are all garbled which enhance the web malicious code against analysis. So it can avoid network security defense.

Testing and Analysis

Web malicious code modules include the encryption and deformation of web malicious code and files hidden and hidden process of the downloaded Trojan and some other auxiliary hidden. The following will detail the test platform and the three tested modules, and analysis of test results.

A. Testing Platform

Test environment topology is shown in Figure2. In windows XP platform installing different anti-virus software: Kaspersky 6.0, 360 and rising in 2008.

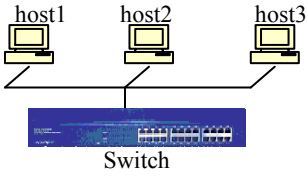
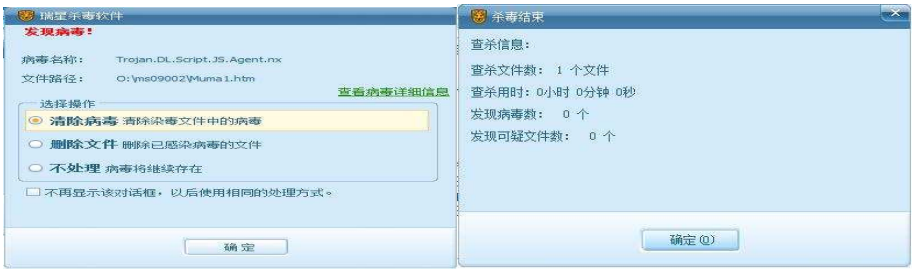


Fig.2 Test topologies

B. Test of Encrypt and Deformation Hiding Technology

Web malicious code uses a simple XOR encryption algorithm. Trojan's signature is usually characteristic properties of web functions, such as document.Write, eval, unescape, fromCharCode, setTimeOut and other functions, and the domain name address downloaded by Trojan. Through the XOR encryption, the feature function sets name address string disappearing to avoid signature detection. The web malicious code escapes character by deformation method. The "\ u-byte number " convert all "\ number " followed by the ASCII code in octal representation of the original characters. Test results charts are as follows.



(a) Before encryption and deformation (b) After encryption and deformation

Fig.3 Rising Antivirus treats web malicious code

(a) Before encryption and deformation (b) After encryption and deformation

Fig.4 360 treats web malicious code

(a) Before encryption and deformation (b) After encryption and deformation

Fig.5 Kaspersky treats web malicious code

From three pictures above we can see that web malicious code can not be detected by the Rising of 2008, Kaspersky and 360 three-detection software after the encrypted and deformation. It indicates that encrypted and reformatted web malicious code has been further improved in viability.

C. Test of Host Trojans Hidden

The web malicious code Trojans HideProcess.exe downloaded through the web runs before the auxiliary hidden. You can find HideProcess.exe in the Task Manager, and it can be found by searching the file HideProcess.exe. After running auxiliary hidden module, process detection software will not detect HideProcess.exe and it can not be found by searching for files. It describes the effect of process hidden and documents hidden as follows:

(a) Before the hidden process (b) After the hidden process

Fig.6 Comparison of the hidden process

In figure6, after process hidden, the Task Manager does not appear HideProcess.exe process. So the supporting hidden module catches the good results. To make the test convenience, we put the running programs of web malicious code into C: \. The test results are as follows:

(a) Before the hidden file (b) After the hidden file

Fig.7 Comparison of the hidden file

After comparing figure7, it can be seen that we can not find hidden files of AddSection.exe in the C: \. So the hidden module catches the hidden effects well.

Conclusions

In this paper, directing the survival and spread for the web malicious code we propose integrated solutions, and we give an application example by using them. Before the web malicious code is running, we use encryption and deformation to avoid network security defense. But after running, Trojan is running after the process hiding and file hiding of host hidden which are used to avoid network security defense. Tests indicate that comprehensive solution reduces the rate of detection of web malicious code greatly. Web malicious code attacks are part of the network security study, we will continue to study the defense program of this web malicious code.

References

[1] Wang Changguang, Bai Xu, Fu Shuai, Ma Jianfeng, Modeling Malicious Code Spread in Scale-Free Networks of Moving Agents, Computer Science and Software Engineering. (2008)546 - 549.

[2] Rabek J C, Roger I, Detection of injected, dynamically generated and obfuscated malicious code, Proceedings of the 2003 ACM Workshop on Rapid Malcode. (2003)76-82.

[3] Gamayunov D, Nguyen Quan, Sakharov F, et al, Racewalk: Fast Instruction Frequency Analysis and classification for shellcode Detection in Network Flow, Computer Network Defense. (2009)4-12.

[4] Madihah S, Nazean J, Knowledge Structure on Virus for User Education, Computational Intelligence and Security. (2006)1515-1518.

[5] Jichiang Tsai, Chung-Hsin Feng, Chuyuan Tsai, A Network Safety-Defense Mechanism with the Linux Security Module, IEEE Region 10 Confedrence. (2006)1-4.

[6] Salmani H, Tehranipoor M, Plusquellic J, A Novel Technique for Improving Hardware Trojan Detection and Reducing Trojan Activation Time, IEEE. (2011)1.

[7] Danyang Cao, Bingru Yang, Design and implementation for MD5-based data integrity checking system. 2010(608-611).

[8] Yongje Choi, Mooseop Kim, Taesung Kim et al, Low power implementation of SHA-1 algorithm for RFID system. (2006)1-5.