ISSN: 2688-8645

Analysis and Discussion of Huigezi Trojan Horse

Yuxin Feng[1, a]

[1]Department of Computer Science, North China Electric Power University, Baoding 071000, China.

[a]389378797@qq.com

Abstract

Trojan horses are very common on the Internet. As a representative of Trojan horses, Huigezi has been rampant for a period of time. Now let us interpret Huigezi Trojan horse, explore its operating principle, and learn its detection and elimination methods.

Keywords

Trojan Horse, Network Security, Trojan Horse Prevention and Control, Huigezi Trojan.

1. Introduction

Huigezi is a very complex and fully functional remote control program. Since 2001, when Huigezi was born, it has been judged by anti-virus professionals as the most dangerous backdoor program, and it has attracted great attention in the security field. In 2004, 2005, and 2006, Huigezi was selected as one of the top ten viruses of the year by major domestic anti-virus manufacturers for three consecutive years. As a result, Huigezi became famous and gradually the focus of media and netizen.

Huigezi was written in Delphi and was not released as a finished product at the earliest. It appeared on the Internet in the form of technology research and adopted source code sharing. The source code of the early version of Huigezi can still be searched on the Internet. When Huigezi appeared, the most discussed "rebound port" connection method was used to avoid the interception of most personal network firewalls. Huigezi was not as famous as Glacier Trojan at the time, so there were only a small number of infections, but its open source method also allowed it to gradually increase its spread and there are many different versions appeared. The variation of Huigezi appeared in 2011. It can evade the detection of mainstream administrators and is highly concealed. Since the servers are all started in a hidden way, it has established its status as a malicious Trojan.

2. Principle of Operation

Huigezi consists of two parts: client and server. The client is a program used by hackers to remotely control the machine implanted with a Trojan horse, and the server program is a Trojan horse. Huigezi uses the connection method based on the rebound port principle. And the client remotely controls the server. The hacker uses the client program to configure the server program. The configurable information mainly includes the online type, the public network IP address used when actively connecting, the connection password, port used, start-up item name, service name, process hiding method, shell used, proxy, icon, etc. The default file name of the server file configured by the client is G_Server.exe, the file name can also be changed, and hackers can trick users into running it through various methods.

When G_Server.exe runs for the first time, it copies itself to the Windows directory and registers it as a service, then releases two files: G_Server.dll and G_Server_Hook.dll. And then injects G_Server.dll and G_Server_Hook.dll through remote thread injection into Explorer.exe and IExplorer.exe to make it execute. After G_Server.exe exits, these two dynamic libraries continue

ISSN: 2688-8645

to run. Since there is no independent process, the virus achieves the purpose of hiding itself. G_Server.dll will release the file G_ServerKey.dll, set the properties of G_ServerKey.dll to hidden, system and read-only, and then initialize the network, enter the network command loop, wait for the client to connect, and then parse the command sent by the client, then execute the corresponding command. G_ServerKey.dll will actually be loaded by all ring3 processes that have a message loop. The working principle is that after starting a hidden window IE process through the G_Server.exe service process, inject a remote thread into this IE process, and then the IE process will load G_ServerKey. dll, call the export function CreateObject of G_ServerKey.dll and set up two message hooks, so that all processes with a message loop will load G_ServerKey.dll and perform APIHOOK operations in DllMain of G_ServerKey.dll. The keyboard operation is performed inside the hook function. After that, each time the computer turn on, G_Server.exe in the Windows directory will automatically run and exit after activating the dynamic library to ensure concealment. G_Server.dll implements the backdoor function and creates a shared memory for communication with the client. The client can perform many operations on the server. Another dynamic library, G_Server_Hook.dll, hides the files of Huigezi , service registry keys, and even module names in the process by intercepting the API calls of the process. The intercepted functions are mainly used to traverse files, registry keys and some functions of process modules. Therefore, it is difficult to traverse the files and modules of Huigezi in normal mode.

3. Simple Analysis of Part of the Source Code

From the source code of Huigezi v1.2, we can see it first defines a project file named H_Client, and then lists the units that need to be used in the project.

The project execution part includes various forms generated when Huigezi runs, and finally releases the logo form and displays the main form.

Next part is the unit file Splash.pas of the logo form, where FormKeyDown represents an event triggered by pressing the keyboard.

The last part is AboutUnit, the unit file related to the form. The procedure of the two tab click processes is to open IE, and the last FormKeyDown process is used by the original author to hide the mark.

The each unit file of program achieves corresponding functions, and the main form calls each program module when user performs an operation. Fig. 1 shows the model of the Huigezi program.

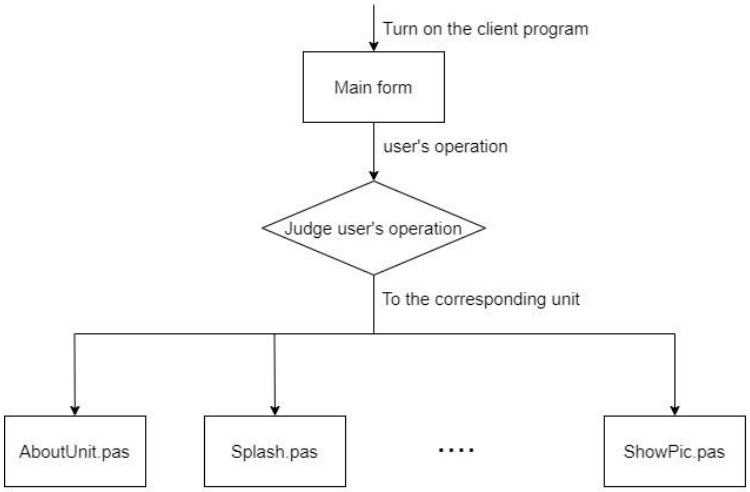

Fig 1. The model of the program

ISSN: 2688-8645

4. Manual Detection Method

In the normal mode, Huigezi will hide itself, so the operation of detecting this Trojan must be performed in safe mode. From the operating principle, it can be seen that the server of Huigezi will generate a "_hook.dll" ending file in the system directory. Then set Windows directory to display all files, and then search for files ending with "_hook.dll" in the Windows installation directory. If a file is found as xx_hook.dll, there are also xx.exe, xx.dll and xxKey .dll in the same directory.

5. Manual Elimination Method

Manual elimination of Huigezi is divided into two steps. You still have to operate in safe mode. The first step is to remove the service and delete the entire G_Server item in the registry editor. The second step is to delete the program files (G_server.exe, G_Server.dll, G_Server_Hook.dll and G_ServerKey.dll), which are in the Windows directory. After restarting the computer, the goal of eliminating Huigezi has been achieved.

6. Conclusions

Huigezi itself does not have the ability to propagate, and it's usually spread by bundling software via web-pages, emails, chat tools, and illegal software. Therefore, in order to avoid such viruses, it is very necessary to develop good Internet surfing habits. At the same time, pay attention to the security configuration of your own system, and timely turn off some unnecessary services and sharing, which will improve our computer's ability to resist malicious code.

References

[1] Xiaoqing Han. Computer virus analysis and prevention[M]. Beijing:Electronic Industry Press, 2006

[2] Lixin Chen. Computer virus prevention know-all[M] .Beijing:Tsinghua University Press, 2001.

[3] Hui Li. Hacker attack and defense and computer virus analysis and detection and security solutions[M].Beijing: Electronic Information Technology Press, 2006.

[4] HUANG Xiao -ke. Princples and Prevention of the "Hack. Huigezi"[N]. Journal of Anhui Metallurgical Science and Technology Vocation.