The Wars in Your Machine: New Developments in Trojan Virus Engineering

Author: Mengze Li · Advisor: Sonja Streuber

INTRODUCTION

Definition:
The Trojan Virus is a malicious computer program that is used to compromise a computer by fooling users about its real intent.

- Unlike computer viruses, or worms, the Trojan does not directly attack operating systems
- Modern forms act as a backdoor to grant access without authorization.
- Help attackers to break the confidentiality, integrity and availability of data
- Can cause a huge impact to both, private users and public organizations, such as exposing the user's credit card information, or other personal identity information (PII).

Method:
- In this study, we are reviewing and analyzing the actual code of three famous modern Trojans in order to learn their most common functions and goals.
- We use hackers' actual code stubs, obtained from public sources such as GitHub.

HISTORY OF TROJAN FUNCTIONALITY

Most common functionalities of old Trojan viruses:
- Large number of pop-ups to make users download software programs containing multiple harmful viruses.
- Upload and download software and data sharing.
- Reinstall the Trojan virus itself from the hidden infected files after removal.

Other typical functionalities:
- Modification or deletion of files.
- Data corruption.
- Spreading malware across the network.
- Infecting other connected devices on the network.

EXAMPLE: Spy Sheriff (1980)
- Ca. one million computer systems worldwide
- Appearance of a huge number of pop-ups, which warned users about the risks of their computer systems and the necessity to install the applications for solving the problem.
- Reinstalled itself from the hidden infected files.

EXAMPLE: Vundo (2010)
- Occupied a large number of memory of computer, so that it could generate lots of pop-ups to warn users the necessity of installing software programs which contained multiple harmful computer viruses.

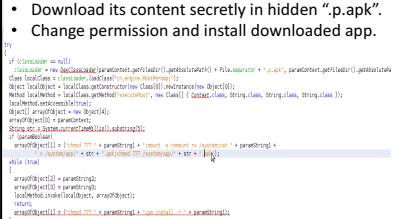
THREE NEW TROJANS

Shedun: Android Trojan

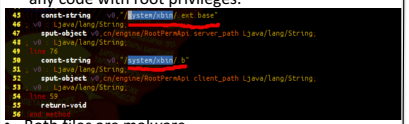
- Runs on Android mobile devices; has been seen pre-installed on cellphones and tablets from China.
- Downloads and installs adware; launches popup advertisements
- Roughly 20,000 popular Android applications infected (Twitter, Facebook, Snapchat, etc.)

Analysis

com.qq package:
- Download its content secretly in hidden ".p.apk".
- Change permission and install downloaded app.



- Change the permissions of application to grant whole authorizations to allow attackers to execute any code with root privileges.



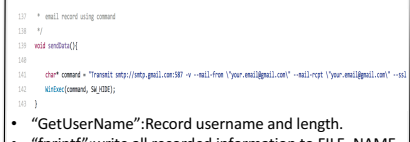
- Both files are malware.
- The .ext.base files require root permissions.

Cockroach Trojan

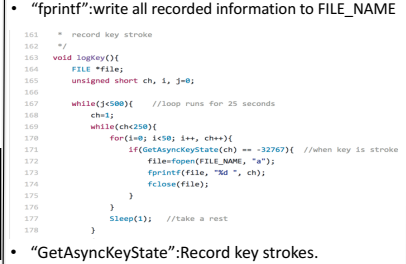
- Steals the sensitive data, such as user name, password, time, date, email, and every key stroke and emails the data back to the host.
- Spread among Windows PCs through USB drives.
- Very hard to detect with anti-virus software.

Analysis

- Transmit target email with Transmit.exe file.
- your.email@gmail.com is the attack email.
- Use SSL protocol to encrypt traffic.



- "GetUserName":Record username and length.
- "fprintf":write all recorded information to FILE_NAME

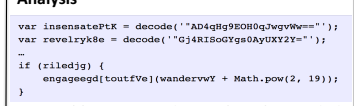


- "GetAsyncKeyState":Record key strokes.
- Attacker can get the password when user is typing.

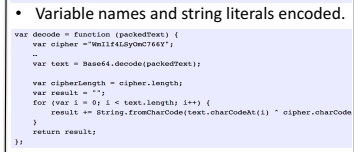
Polymorphic JavaScript Trojan

- Spread as email attachments
- In different emails, the cipher, string literals and variable names are different which makes itself less detectable.
- Meant to be run from disk, which gives it permissions to attack system globally.

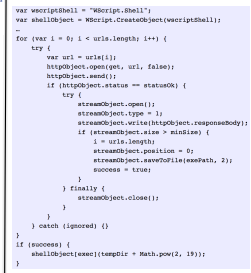
Analysis



- Variable names and string literals encoded.



- "decode" function defined.



- EXE file is malicious & will attack user system secretly.

CONCLUSION

- Compared to the old Trojan viruses, the new Trojan viruses are more armored, undetectable and sophisticated.
- Also, the new Trojan viruses can change the permission of the application and execute as the root to cause more damage than old Trojan viruses.
- Finally, the new Trojan virus can spy on the user's computer systems, and record sensitive data, such as user name, password, and email contents, to break the confidentiality of sensitive data.

REFERENCES

- *Landwehr, C. E; A. R Bull; J. P McDermott; W. S Choi (1993). A taxonomy of computer program security flaws, with examples. DTIC Document. Retrieved 2012-04-05. . Last accessed 04/23/2017.*
- *"What is the difference between viruses, worms, and Trojans?". Symantec Corporation. Retrieved 2009-01-10. . Last accessed 04/23/2017.*
- *"VIRUS-L/comp.virus Frequently Asked Questions (FAQ) v2.00 (Question B3: What is a Trojan Horse?)". 9 October 1995. Retrieved 2012-09-13.*
- *https://www.scmagazine.com/knock-knock-unique-new-backdoor-trojan-infecting-computers/article/528205/. Last accessed 04/23/2017.*
- *http://www.infoniac.com/hi-tech/the-history-and-description-of-trojan-horse-virus.html. Last accessed 04/23/2017.*
- *https://en.wikipedia.org/wiki/Trojan_horse_(computing) . Last accessed 04/23/2017.*
- *shedun: adware/malware family threatening your Android device. https://blog.avira.com/shedun/ . Last accessed 04/23/2017.*
- *https://github.com/MinhasKamal/TrojanCockroach/blob/master/com/minhaskamal/trojanCockroach/TrojanCockroach.cpp . Last accessed 04/23/2017.*
- *https://github.com/MinhasKamal/TrojanCockroach . Last accessed 04/23/2017.*
- *http://www.sjoerdlangkemper.nl/2016/02/18/polymorphic-javascript-malware/ . Last accessed 04/23/2017.*

VALPARAISO UNIVERSITY