Spring 5-4-2017

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

Mengze Li
Valparaiso University, mengze.li@valpo.edu

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

Mengze Li

Abstract: The Trojan Virus, or Trojan, is a malicious computer program that is used to compromise a computer by fooling users about its real intent[1]. Although, unlike computer viruses, or worms, the Trojan does not directly attack operating systems[2], many modern forms act as a backdoor, which can grant access without authorization[3]. This kind of infection helps attackers to break the confidentiality, integrity and availability of the data, and 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). Recent Trojans have been engineered to cause bigger destruction and yet remain less obvious than their ancestors. For example, several cheap android phones come preinstalled with Trojan viruses, which, for example, show advertisements on top of running apps and prevent users from removing the pictures[4]. In a desktop-based example, the BackDoor.TeamViewer.49 can remove its icon from the Windows notification area and disable error reporting and implement a special mechanism meant to prevent it from being restarted on an infected computer once the TeamViewer is launched[5], which means that its malicious behavior is too hard to identify.

---

[1] *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.*

[2] *"What is the difference between viruses, worms, and Trojans?". Symantec Corporation. Retrieved 2009-01-10.*

[3] *"VIRUS-L/comp.virus Frequently Asked Questions (FAQ) v2.00 (Question B3: What is a Trojan Horse?)". 9 October 1995. Retrieved 2012-09-13.*

[4] *ValueWalk: Several cheap android phones come preinstalled with trojan viruses (2016). . Chatham: Newstex. Retrieved from http://ezproxy.valpo.edu/login?url=http://search.proquest.com/docview/1848915535?accountid=14811*

[5] *https://www.scmagazine.com/knock-knock-unique-new-backdoor-trojan-infecting-computers/article/528205/*

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. Take the example below:

```
{
    "timestamp": 12345,
    "account_id": "abc@gmail.com",
    "location": {
        "lat": 200,
        "lon": 1
    },
    "audio_url": "abc@gmail.com/12345/audio.aac",
    "image_url": "abc@gmail.com/12345/image.jpg"
}
```
[6]

These lines of code can help the hackers collect images, 10-second sound clips, and location information from users' phones every 3 seconds, and upload them via Wi-Fi. We are furthermore comparing the modern Trojan with the old Trojan to see the improvement of the modern Trojan, and how the Trojan hide itself from the anti-malware software, and the IPS system. Both, code analysis and historical comparison are critical in developing patches to prevent the process of such unauthorized data theft.

Although many Trojan viruses are armored, which means that the attackers have used advanced methods, such as encrypting the code, or added useless code to confuse the cybersecurity professional, we will be using hackers' actual code stubs, obtained from public sources such as GitHub, in order to get around this obstacle. This analysis will support our theory that most of modern Trojan viruses are intending to act as a backdoor for granting unauthorized accesses, thereby causing bigger destruction while more skillfully attempting to evade detection by common countermeasures.

[6] *https://github.com/project-columbus/trojan*

Keywords: Trojan Virus, Security, Impaction, Code