Report
On
“Batata3 Trojan”

Introduction:

- The **“Batata3 Trojan”** is a malware in a form of a trojan horse made for Microsoft windows.

Date of production:

- Started on 1st February 2021
- Ended on 7th February 2021

Production:

Language used:

- C++
- Command line

What does it do:

- The main purpose of **“Batata3 Trojan”** is to destroy the operating system by deleting one of the system files, in our case it deletes a file from CatRoot folder. After deleting the file, the first thing the malware does is making the mouse moves randomly, then it starts searching random stuff on google like:

  - BATATA3
  - Hakuna Matata
  - Resident evil 8
  - MY PC GOT CRAZY

- Also, it opens some YouTube Videos like:

  - La3riba - العربية | Erkez Hip Hop de Debo
  - Shaggy - Boombastic (Official Music Video)
  - أغنية اسمي فلفول - سبيس تون | Spacetoon

- After that the trojan starts annoying noises while playing with themes, it starts jumping from black theme to the white theme with pausing for 3 seconds each time. The noises go on and Batata3 kill the explorer.exe processes and starts popping up bat files containing ASCII ART such as a “skull”, “I’m BATMAN”, “BATATA3” and “I LOVE LASAGNA”. The annoying noise stops and everything backs to normal, nothing will happen for 10 seconds, then an ASCII ART bat file will appear with “ BYE BYE ” written on it with an evil laugh in the background. Then the PC will force a restart and the system won’t boot up because of a missing file and force a BSod.

Release:

Features:

- The features of this malware are some of the processes cannot be stopped because it will be mixed with system processes, because after all it’s all command lines.
- Once the program is executed there is no going back, the Operating system is dead.

Bugs:

- The themes and google popups sometimes do not work

Why is it marked as a failure:

- It demands admin privilege
- The noise needs visual c++ redistributable / Direct X to work in the background

Conclusion

- The malware needs to ask less from the system and everything needs to work properly
- It’s a good malware but it doesn't make a HUGE Disaster