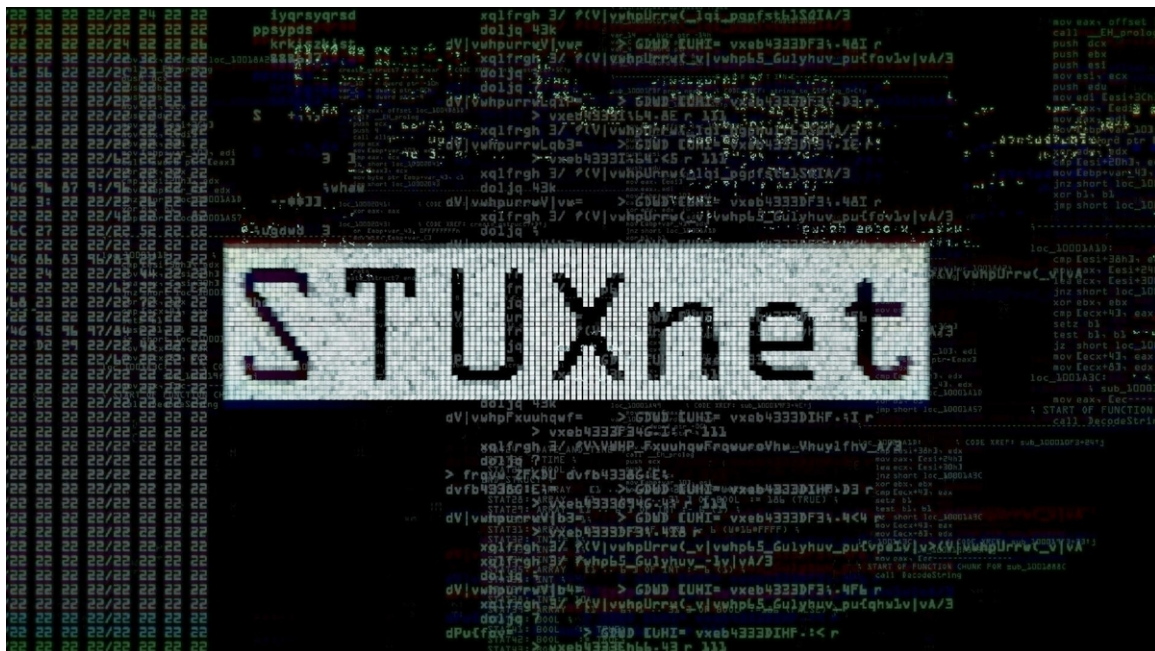


NORTHERN ARIZONA UNIVERSITY

CYBERSECURITY CYB 410 - SOFTWARE SECURITY

Analyzing and Reporting on Stuxnet

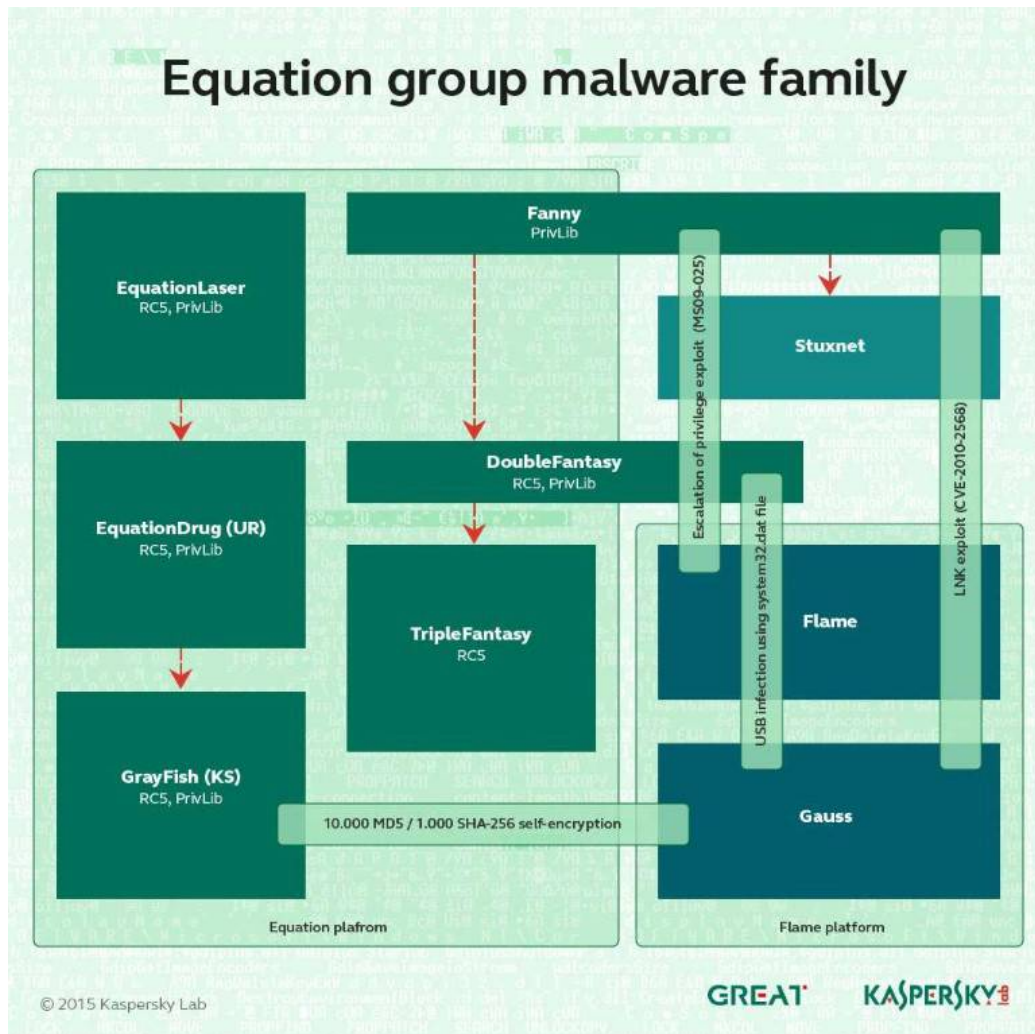


Author:
Akiel Aries

Professor:
Prof. Sareh Assiri

December 7, 2022

1 Overview



Stuxnet is a computer worm first identified in 2010 that was originally implemented to target Iranian governments nuclear facilities. Just like most virus', they mutate and spawn new strains often more dangerous than their predecessor. The original infection succeeded in targeting PLCs (Programmable Logic Controller) which are used in a plethora of manufacturing related processes. For example, PLCs are used in robotic machinery seen in assembly lines at manufacturing plants. The point of these controllers is to be secure, reliable, and useful fault diagnostics.

It is no wonder why Stuxnet was a large threat in the InfoSec industry. It is of popular belief that this is the first computer worm capable of affecting hardware and its peripherals as most computer worms are built as software exploits. The origin of the worm is cloudy however, according to reports from cybersecurity research firms such as Kaspersky Lab, Symantec, and many more, the origin supposedly started as a nation-based collaboration with the United States and Isreal to target the Iranian Nuculear Program. The worm went on to destroy 1/5 of Iran's nuclear centrifuges, an important component in the process of enriching collected uranium, infecting

above 200,000 thousand devices and went on to severely degrade the performance of over 1,000 machines themselves. What lead researchers to believe the bug was nation state sponsored was the lack of infections of other users of the Siemens based software. This was false according to Eugene Kaspersky himself as he said a Russian nuclear power plant was also infected but not affected since it lacked any access to the public-facing internet. The common belief is that the group behind the attack is a nation state sponsored team by the name of Equation Group with reported ties to the USA's National Security Agency (NSA) which is also believed to be a part of over 500 computer infections. When it comes to violation of the CIA triad, this becomes somewhat murky territory as the attack was supposedly carried out the very own United States Government and the infected party was exploited by means of an air gap, meaning the bot's initial attack vector is physical. At a glance, all aspects of the CIA triad were violated as the confidentiality of the attack was not contained per leaked documents along with whistleblowing (allegedly), integrity was not upheld by the nation or said party involved, and availability was not present. The repository that this report will be base the code off of is located here: <https://github.com/research-virus/stuxnet>

2 Source Code

The stuxnet virus makes use of infecting RPC (Remote procedure call) servers based on the different type of call types that are made. The servers are split into two components one managing local RPC calls and the other for managing remote calls. The calls that were sniffed were services.exe for local calls,

Scale

Execution

Reproducible Example

Static Analysis/Debugging

Fuzzing with AFL

Final Notes