SAURON

**Overview:**

Sauron is a computer virus, kind of a targeted attack platform designed for long-term cyber-espionages. It was used to exfiltrated data from air-gapped networks (networks isolated from the public internet) through legitimate channels of software distribution.

**Operation:**

The modules and network protocols in the malware used very strong encryption algorithms such ass RC5, AES, Salsa20 etc. It was written in a modified Lua scripting engine which was used to implement its core platform as well as up to 50 different plugin types. It was able to exfiltrate data through even air-gapped networks using specially prepared USB devices which would store data in a place invisible to the OS. It was operational from 2011 to 2016. The malware was disguised as files from legitimate software such as kavupd.exe (Kaspersky) and KB2931368.exe (Microsoft).

**Victims:**

Countries targeted included Russia, Iran and Rwanda amongst many others. Key government organizations were prime targets such as Scientific research centers, telecom and finance providers and even the military. It was able to collect high value intelligence compromising mot entities within its reach.

**Discovery:**

Kaspersky Lab’s Anti Targeted Attack Platform discovered the virus in September 2015 when it found irregular network traffic in government organization networks.