Sauron

- Project sauron compromises a top of the top modular cyberespionage platform in terms of technical sophistication designed to enable long term campaigns through stealthy survival mechanisms coupled with multiple exfiltration methods.

- Technical details show how attackers learned from other extremely advanced actors in order to avoid repeating their mistakes.

  Ex:- All artifacts are customized per given target, reducing their values as indicators of compromise for anyother victim.

some other key features of project Sauron:-

- It is a modular platform designed to enable long term cyberespionage campaigns
- All modules and network protocols use strong encryption algorithms such as RC6, RC5, RC4, AES, Salsa 20 etc.
- It uses a modified lua scripting engine to implement the core platform and its plugins.
- there are upwards of 50 different plugin types
- The actor behind project Sauron has high interest in communication encryption software widely used by targeted governmental organizations. It steals encryption keys, configuration files & IP addresses of the key infrastructure servece related to the encryption software
- It is able to exfiltrate data from air gapped networks by using specially prepared USB storage drivers where data is stored in an area invisible to the operation system.
- The platform makes extensive use of the DNS protocol for data exfiltration and realtime status reporting.

- The APT was operational as early as June 2011 and remained active until April 2016
- The initial infection vector used to penetrate victim networks remain unknown
- The attackers utilize legitimate software distribution channels for lateral movement with in infected networks.

The attacked organization are key entities in state functions:

- Government
- Scientific reasearch centers
- Military
- Telecommunication providers
- Finance.