Snatch (Malware Family)

By Fraunhofer FKIE

Snatch is a ransomware which infects victims by rebooting the PC into Safe Mode. Most of the existing security protections do not run in Safe Mode so that it the malware can act without expected countermeasures and it can encrypt as many files as it finds. It uses common packers such as UPX to hide its payload.

▶ [TLP:WHITE] win_snatch_auto (20201014 | autogenerated rule brought to you by yara-signator)
