Analyzing WhisperGate - destructive malware targeting Ukraine - part 1

Published: 2022-02-03 · Archived: 2026-04-05 14:10:11 UTC

In this video, we look at "Whisper Gate" - an infamous destructive malware targeting Ukrainian organizations, that has been discovered and described by Microsoft. We will deep dive into malware code and find out how it works, what it does, and if data is destroyed beyond recovery. Malware sample: MD5: 5d5c99a08a7d927346ca2dafa7973fc1 SHA-1: 189166d382c73c242ba45889d57980548d4ba37e SHA-256: a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92 Malware Baazar: https://bazaar.abuse.ch/sample/a196c6... VirusTotal: https://www.virustotal.com/gui/file/a... Video parts: 00:00 Intro 01:04 Triage 03:58 Static analysis 09:42 MBR code 10:19 Renaming 23:13 Dynamic analysis 29:32 Recovery 31:42 Outro Follow me on social media: My blog: https://malfind.com/ My Twitter: _/ lasq88_ My GitHub: https://github.com/lasq88 #malwareanalysis #malware #cybersecurity #whispergate #technology

---

Source: https://www.youtube.com/watch?v=Ek3URIaC5O8