Avaddon ransomware: an in-depth analysis and decryption of infected systems

By [Submitted on 9 Feb 2021]

Archived: 2026-04-29 07:49:41 UTC

View PDF

Abstract:The commoditization of Malware-as-a-Service (MaaS) allows criminals to obtain financial benefits at a low risk and with little technical background. One such popular product in the underground economy is ransomware. In ransomware attacks, data from infected systems is held hostage (encrypted) until a fee is paid to the criminals. This modus operandi disrupts legitimate businesses, which may become unavailable until the data is restored. A recent blackmailing strategy adopted by criminals is to leak data online from the infected systems if the ransom is not paid. Besides reputational damage, data leakage might produce further economical losses due to fines imposed by data protection laws. Thus, research on prevention and recovery measures to mitigate the impact of such attacks is needed to adapt existing countermeasures to new strains.

In this work, we perform an in-depth analysis of Avaddon, a ransomware offered in the underground economy as an affiliate program business. This has infected and leaked data from at least 23 organizations. Additionally, it runs Distributed Denial-of-Service (DDoS) attacks against victims that do not pay the ransom. We first provide an analysis of the criminal business model from the underground economy. Then, we identify and describe its technical capabilities. We provide empirical evidence of links between this variant and a previous family, suggesting that the same group was behind the development and, possibly, the operation of both campaigns.

Finally, we describe a method to decrypt files encrypted with Avaddon in real time. We implement and test the decryptor in a tool that can recover the encrypted data from an infected system, thus mitigating the damage caused by the ransomware. The tool is released open-source so it can be incorporated in existing Antivirus engines.

Subjects:	Cryptography and Security (cs.CR)
Cite as:	arXiv:2102.04796 [cs.CR]
	(or arXiv:2102.04796v1 [cs.CR] for this version)
	https://doi.org/10.48550/arXiv.2102.04796 arXiv-issued DOI via DataCite
Journal reference:	Computers & Security 109 (2021) 102388
Related DOI:	https://doi.org/10.1016/j.cose.2021.102388

	DOI(s) linking to related resources

Submission history

From: Javier Yuste [view email]
[v1] Tue, 9 Feb 2021 12:31:49 UTC (66 KB)