Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:58:20 UTC

Tool: Avaddon

Names	Avaddon
Category	Malware
Type	Ransomware, Big Game Hunting
Description	(Awake Security) Avaddon is a cryptolocker ransomware written in C++ that is best known for encrypting files and changing the file extension to .avdn. The ransomware also deletes the volume shadow copies and other system backups and typically demands a ransom ranging between $150 and $900. Since the ransomware uses strong encryption algorithms like AES256 and RSA2048, no decryptor is available and it is impossible to decrypt the file without the key that was used to encrypt it. This ransomware is sold similar to other Ransomware-as-a-service(RaaS) like REvil. Thus, even someone with limited technical background can become an “affiliate” to spread the malware. In return, the profit gets shared between the threat actor and the affiliate. In this blog post we dissect this malware and discuss methods to perform threat hunting for the Avaddon ransomware family.
Information	<https://awakesecurity.com/blog/threat-hunting-for-avaddon-ransomware/> <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-report-avaddon-and-new-techniques-emerge-industrial-sector-targeted> <https://www.subexsecure.com/pdf/malware-reports/June-2020/Avaddon_Ransomware.pdf> <https://arxiv.org/pdf/2102.04796.pdf> <https://labs.sentinelone.com/avaddon-raas-breaks-public-decryptor-continues-on-rampage/> <https://www.domaintools.com/resources/blog/avaddon-the-latest-raas-to-jump-on-the-extortion-bandwagon> <https://www.offensive-hackers.com/2020/06/this-new-avaddon-ransomware-targeting-worldwide-users.html> <https://www.proofpoint.com/us/blog/security-briefs/ransomware-initial-payload-reemerges-avaddon-philadelphia-mr-robot-and-more> <https://asec.ahnlab.com/en/17411/> <https://www.cybereason.com/blog/cybereason-vs.-avaddon-ransomware> <https://www.cyber.gov.au/sites/default/files/2021-05/2021-

	003%20Ongoing%20campaign%20using%20Avaddon%20Ransomware%20-%2020210508.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0640/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.avaddon>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:avaddon>
Playbook	<https://www.nomoreransom.org/uploads/Avaddon_documentation.pdf> <https://www.nomoreransom.org/uploads/Avaddon_documentation_new.pdf>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Avaddon

Changed	Name	Country	Observed	
APT groups				
	Riddle Spider	[Unknown]	2020-Jun 2021	

1 group listed (1 APT, 0 other, 0 unknown)

↑
