Riddle Spider - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:42:33 UTC

APT group: Riddle Spider

Names	Riddle Spider *(CrowdStrike)* Avaddon Team *(self given)*	
Country	[Unknown]	
Motivation	Financial gain	
First seen	2020	
Description	(Cornell University) 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.	
Observed	Countries: Australia, Belgium, Brazil, Canada, China, Costa Rica, Czech, France, Germany, India, Indonesia, Italy, Japan, Jordan, Peru, Poland, Portugal, Russia, South Korea, Spain, Switzerland, Thailand, UAE, UK, USA and Worldwide.	
Tools used	Avaddon.	
Operations performed	Jun 2020	New Avaddon Ransomware launches in massive smiley spam campaign <https://www.bleepingcomputer.com/news/security/new-avaddon-ransomware-launches-in-massive-smiley-spam-campaign/>
	Jul 2020	Avaddon ransomware shows that Excel 4.0 macros are still effective <https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shows-that-excel-40-macros-are-still-effective/>

	Aug 2020	Avaddon ransomware launches data leak site to extort victims <https://www.bleepingcomputer.com/news/security/avaddon-ransomware-launches-data-leak-site-to-extort-victims/>
	Jan 2021	Another ransomware now uses DDoS attacks to force victims to pay <https://www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/>
	Feb 2021	Avaddon ransomware fixes flaw allowing free decryption <https://www.bleepingcomputer.com/news/security/avaddon-ransomware-fixes-flaw-allowing-free-decryption/>
	Apr 2021	Cyber-attackers hold PN to ransom with major data leak threat <https://timesofmalta.com/articles/view/cyber-attackers-hold-pn-to-ransom-with-major-data-leak-threat.865968>
	May 2021	Insurer AXA hit by ransomware after dropping support for ransom payments <https://www.bleepingcomputer.com/news/security/insurer-axa-hit-by-ransomware-after-dropping-support-for-ransom-payments/>
	Jun 2021	Avaddon ransomware shuts down and releases decryption keys <https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/>
Information	<https://arxiv.org/abs/2102.04796>	

Last change to this card: 15 June 2021

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=b41f0843-fe80-4005-bb32-38336f92b80a