Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:07:43 UTC

Tool: Diavol

Names	Diavol
Category	Malware
Type	Ransomware, Big Game Hunting
Description	(Fortinet) As part of a rather unique encryption procedure, Diavol operates using user-mode Asynchronous Procedure Calls (APCs) without a symmetric encryption algorithm. Usually, ransomware authors aim to complete the encryption operation in the shortest amount of time. Asymmetric encryption algorithms are not the obvious choice as they significantly slower than symmetric algorithms.
Information	<https://www.fortinet.com/blog/threat-research/diavol-new-ransomware-used-by-wizard-spider> <https://www.speartip.com/resources/speartip-finds-new-diavol-ransomware-does-steal-data/> <https://securityintelligence.com/posts/analysis-of-diavol-ransomware-link-trickbot-gang/> <https://www.binarydefense.com/threat_watch/new-ransomware-diavol-being-dropped-by-trickbot/> <http://www.ic3.gov/Media/News/2022/220120.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0659/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.diavol>
Playbook	<https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-trickbot-gangs-diavol-ransomware/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Diavol

Changed	Name	Country	Observed

APT groups

	Wizard Spider, Gold Blackburn		2014-May 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f25de7f3-032f-491e-90a0-4f1c5bcc7738