Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:02:15 UTC

Tool: 3AM

Names	3AM
Category	Malware
Type	Ransomware, Big Game Hunting
Description	(Symantec) A new ransomware family calling itself 3AM has emerged. To date, the ransomware has only been used in a limited fashion. Symantec's Threat Hunter Team, part of Broadcom, has seen it used in a single attack by a ransomware affiliate that attempted to deploy LockBit on a target's network and then switched to 3AM when LockBit was blocked. 3AM is written in Rust and appears to be a completely new malware family. The ransomware attempts to stop multiple services on the infected computer before it begins encrypting files. Once encryption is complete, it attempts to delete Volume Shadow (VSS) copies. It is still unclear whether its authors have any links to known cybercrime organizations.
Information	<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/3am-ransomware-lockbit>

Last change to this tool card: 12 October 2023

Download this tool card in JSON format

All groups using tool 3AM

Changed	Name	Country	Observed	
APT groups				
	LockBit Gang	[Unknown]	2019-May 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=edd78e6e-9ac3-4a71-a2fc-5e47c8aa3fd8