Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:12:57 UTC

Tool: EKANS

Names	EKANS Snake SNAKEHOSE
Category	Malware
Type	ICS malware, Ransomware, Big Game Hunting
Description	(Dragos) EKANS ransomware emerged in mid-December 2019, and Dragos published a private report to Dragos WorldView Threat Intelligence customers early January 2020. While relatively straightforward as a ransomware sample in terms of encrypting files and displaying a ransom note, EKANS featured additional functionality to forcibly stop a number of processes, including multiple items related to ICS operations. While all indications at present show a relatively primitive attack mechanism on control system networks, the specificity of processes listed in a static “kill list” shows a level of intentionality previously absent from ransomware targeting the industrial space. ICS asset owners and operators are therefore strongly encouraged to review their attack surface and determine mechanisms to deliver and distribute disruptive malware, such as ransomware, with ICS-specific characteristics.
Information	<https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/> <https://blog.malwarebytes.com/threat-analysis/2020/06/honda-and-enel-impacted-by-cyber-attack-suspected-to-be-ransomware/> <https://unit42.paloaltonetworks.com/threat-assessment-ekans-ransomware/> <https://www.deepinstinct.com/2020/06/29/the-snake-attacks-holding-the-industrial-sector-ransom/> <https://www.fortinet.com/blog/threat-research/ekans-ransomware-targeting-ot-ics-systems>
MITRE ATT&CK	<https://attack.mitre.org/software/S0605/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.snake>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:ekans>
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=ekans-ransomware>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool EKANS

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=8236a50f-f937-4e6e-b935-8dea58971dfa