Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:56:22 UTC

Tool: FoundCore

Names	FoundCore RainyDay
Category	Malware
Type	Backdoor, Info stealer
Description	(Kaspersky) Communications with the server can take place either over raw TCP sockets encrypted with RC4, or via HTTPS. Commands supported by FoundCore include filesystem manipulation, process manipulation, screenshot captures and arbitrary command execution.
Information	<https://securelist.com/the-leap-of-a-cycldek-related-threat-actor/101243/> <https://www.bitdefender.com/files/News/CaseStudies/study/396/Bitdefender-PR-Whitepaper-NAIKON-creat5397-en-EN.pdf>

Last change to this tool card: 15 May 2021

Download this tool card in JSON format

All groups using tool FoundCore

Changed	Name	Country	Observed	
APT groups				
	Goblin Panda, Cycldek, Conimes		2013-Jun 2020	
	Naikon, Lotus Panda		2010-Apr 2022	

2 groups listed (2 APT, 0 other, 0 unknown)