Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:54:48 UTC

Tool: Andaratm

Names	Andaratm
Category	Malware
Type	Backdoor, Exfiltration
Description	(AhnLab) Andaratm malware was used in attacks on military agencies in 2016, on ATMs and financial institutions in 201 on cryptocurrencyexchanges in 2018. 18 variants have been identified as of May 2018.The codesof Andaratm include str such as '%s\cmd.exe /c echo | %s > %s'and '%s*****%s.' When Andaratm is executed, it acquires information, such as the computer name and username, attempts to connect to th designated C2 server, and receives and executes the command. The encryption method of Andaratm is similar to the methods generally used by malware. Andaratm only executes simple commands, such as downloading files, uploading files, and running cmd.exe files.
Information	<https://global.ahnlab.com/global/upload/download/techreport/%5BAhnLab%5DAndariel_a_Subgroup_of_Lazarus%20

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Andaratm

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=e10666f4-2aa9-4405-bfcf-20ea4827fef2