Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:33:33 UTC

Tool: ATMitch

Names	ATMitch
Category	Malware
Type	ATM malware, Backdoor
Description	(Kaspersky) The malware, which we have dubbed ATMitch, is fairly straightforward. Once remotely installed and executed via Remote Desktop Connection (RDP) access to the ATM from within the bank, the malware looks for the “command.txt” file that should be located in the same directory as the malware and created by the attacker. After execution, ATMitch writes the results of this command to the log file and removes “command.txt” from the ATM’s hard drive. The malware uses the standard XFS library to control the ATM. It should be noted that it works on every ATM that supports the XFS library (which is the vast majority).
Information	<https://securelist.com/atmitch-remote-administration-of-atms/77918/> <https://blog.yoroi.company/research/atmitch-new-evidence-spotted-in-the-wild/> <https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.atmitch>

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

All groups using tool ATMitch

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

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