Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:21:25 UTC

Tool: Prilex

Names	Prilex
Category	Malware
Type	ATM malware, POS malware, Credential stealer
Description	(Kaspersky) While researching malware for ATM jackpotting used by a Brazilian group called Prilex, our researchers stumbled upon a modified version of this malware with some additional features that was used to infect point-of-service (POS) terminals and collect card data. This malware was capable of modifying POS software to allow a third party to capture the data transmitted by a POS to a bank. That's how the crooks obtained the card data. Basically, when you pay at a local shop whose POS terminal is infected, your card data is transferred right away to the criminals. However, having the card data is just half the battle; to steal money, they also needed to be able to clone cards, a process made more complicated by the chips and their multiple authentications. The Prilex group developed a whole infrastructure that lets its "customers" create cloned cards — which in theory shouldn't be possible.
Information	<https://www.kaspersky.com/blog/chip-n-pin-cloning/21502/> <https://threatpost.com/latin-american-atm-thieves-turning-to-hacking/128289/> <https://blog.trendmicro.com/trendlabs-security-intelligence/dissecting-prilex-cutlet-maker-atm-malware-families/> <https://securelist.com/prilex-modification-now-targeting-contactless-credit-card-transactions/108569/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.prilex>

Last change to this tool card: 17 February 2023

Download this tool card in JSON format

All groups using tool Prilex

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

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