Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:50:38 UTC

Tool: NeoPocket

Names	NeoPocket
Category	Malware
Type	ATM malware, Keylogger, Info stealer, Credential stealer
Description	(Trend Micro) NeoPocket is an information-stealing malware that targets ATMs manufactured by Diebold. S21sec discovered NeoPocket in April 2014. Unlike the majority of ATM malware, NeoPocket does not steal cash from the ATM as it focuses on data theft only. The malware steals ATM transaction data using a man-in-the-middle (MitM) attack and keylogs user input from specific application windows. This stolen data can be sold in deep web markets for use in creating counterfeit payment cards and carrying out fraudulent fund transfers out of victims' accounts. Because no cash is stolen from the ATM, the compromise tends to remain undetected for prolonged periods and thus allows the criminal group behind NeoPocket to collect large amounts of sensitive data.
Information	<https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf>

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

All groups using tool NeoPocket

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

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