Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:17:35 UTC

Tool: FiXS

Names	FiXS
Category	Malware
Type	ATM malware
Description	(Metabase Q) Metabase Q recently identified a new malware that is currently affecting Mexican banks. Due to it's code name in the binary, we dubbed it FiXS. It is not clear yet what the vector for the initial infection is. However, since FiXS utilizes an external keyboard (similar to Ploutus), we anticipate that it follows a similar methodology. In the case of Ploutus, a person with access to these teller machines physically connects an external keyboard to to the ATM for the attack to commence. So far, we have identified some key relevant characteristics of FiXS malware: • It instructs the ATM to dispense money 30 minutes after the last ATM reboot • It is hidden inside another not-malicious-looking program • It is vendor-agnostic targeting any ATM that supports CEN XFS • It interacts with the crooks via external keyboard • It waits for the Cassettes to be loaded to start dispensing • It contains Russian metadata
Information	<https://www.metabaseq.com/fixs-atms-malware/>

Last change to this tool card: 25 April 2023

Download this tool card in JSON format

All groups using tool FiXS

Changed	Name	Country	Observed
Unknown groups			

	[Interesting malware not linked to an actor yet]			

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=7b095e59-1cfa-4d33-9ebe-c6b5df3d8fe9