Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:59:15 UTC

Tool: Ploutus

Names	Ploutus Ploutus ATM Plotus
Category	Malware
Type	ATM malware
Description	(Symantec) According to external sources, the malware is transferred to the ATM by physically inserting a new boot disk into the CD-ROM drive. The boot disk then transfers malware. The criminals created an interface to interact with the ATM software on a compromised ATM, and are therefore able to withdraw all the available money from the containers holding the cash, also known as cassettes. One interesting part to note is that the criminals are also able to read all the information typed by cardholders through the ATM keypad, enabling them to steal the sensitive information without using any external device.
Information	<https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=4274cb7f-d65d-4928-bdf4-0275eedc80d2&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments> <https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=54602160-07ea-4dbb-8794-14725ea4c8ba&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments> <https://www.fireeye.com/blog/threat-research/2017/01/new_ploutus_variant.html> <http://antonioparata.blogspot.co.uk/2018/02/analyzing-nasty-net-protection-of.html> <https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ploutus_atm>

AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:ploutus>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool Ploutus

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=fdf897ad-2431-44a2-b3da-b9a3d55d0387