Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:22:59 UTC

Tool: Mekotio

Names	Mekotio Metamorfo Casbaneiro
Category	Malware
Type	Banking trojan, Reconnaissance, Backdoor, Keylogger, Info stealer, Credential stealer
Description	(ESET) As is common for most Latin American banking trojans, Mekotio has several typical backdoor capabilities. It can take screenshots, manipulate windows, simulate mouse and keyboard actions, restart the machine, restrict access to various banking websites and update itself. Some variants are also able to steal bitcoins by replacing a bitcoin wallet in the clipboard and to exfiltrate credentials stored by the Google Chrome browser. Interestingly, one command is apparently intended to cripple the victim's machine by trying to remove all files and folders in C:\Windows tree.
Information	<https://www.welivesecurity.com/2020/08/13/mekotio-these-arent-the-security-updates-youre-looking-for/> <https://cofense.com/blog/autohotkey-banking-trojan/> <https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/rooty-dolphin-uses-mekotio-to-target-bank-clients-in-south-america-and-europe/> <https://www.welivesecurity.com/2019/10/03/casbaneiro-trojan-dangerous-cooking/> <https://research.checkpoint.com/2021/mekotio-banker-returns-with-improved-stealth-and-ancient-encryption/> <https://www.sygnia.co/blog/breaking-down-casbaneiro-infection-chain/> <https://www.sygnia.co/blog/breaking-down-casbaneiro-infection-chain-part2/> <https://www.forcepoint.com/blog/x-labs/exploring-metamorfo-banking-malware> <https://www.trendmicro.com/en_us/research/24/g/mekotio-banking-trojan.html> <https://www.trendmicro.com/en_us/research/24/i/banking-trojans-mekotio-looks-to-expand-targets--bbtok-abuses-ut.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.mekotio>

Last change to this tool card: 23 October 2024

Download this tool card in JSON format

All groups using tool Mekotio

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=a5c752a8-eefc-4ed1-9520-0e0ae67fa892