Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:14:59 UTC

Tool: Cinobi

Names	Cinobi
Category	Malware
Type	Banking trojan, Backdoor, Info stealer
Description	(Trend Micro) The Cinobi banking trojan is split into four stages, with each stage downloading additional components and possibly p environment or anti-virtual machine (VM) checks. There are two command-and-control (C&C) servers, with one of them returning s the other one returns the configuration files.
Information	<https://www.trendmicro.com/en_us/research/21/h/cinobi-banking-trojan-targets-users-of-cryptocurrency-exchanges-.html> <https://documents.trendmicro.com/assets/pdf/Tech%20Brief_Operation%20Overtrap%20Targets%20Japanese%20Online%20Bank <https://blog.trendmicro.com/trendlabs-security-intelligence/operation-overtrap-targets-japanese-online-banking-users-via-bottle-ex brand-new-cinobi-banking-trojan/> <http://www.pwncode.io/2019/12/unpacking-payload-used-in-bottle-ek.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.cinobi>

Last change to this tool card: 28 December 2021

Download this tool card in JSON format

All groups using tool Cinobi

Changed	Name	Country	Observed	
Unknown groups				
	【Interesting malware not linked to an actor yet】			

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