Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:44:25 UTC

Tool: Mechanical

Names	Mechanical GoldStamp
Category	Malware
Type	Keylogger, Banking trojan
Description	(Arbor) Logs keystrokes to %userprofile%\appdata\roaming\apach.{txt,log} and also functions as a “cryptojacker” that replaces Ethereum wallet addresses with 0x33883E87807d6e71fDc24968cefc9b0d10aC214E. This Ethereum wallet address currently has a zero balance and no transactions.
Information	<https://www.netscout.com/blog/asert/stolen-pencil-campaign-targets-academia>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.mechanical>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool Mechanical

Changed	Name	Country	Observed	
APT groups				
	Kimsuky, Velvet Chollima		2012-Aug 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=0828b2b4-e78b-4162-b0b6-d86c697e9240