

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:39:53 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool ATMRipper


Tool: ATMRipper

Names	ATMRipper Ripper Ripper ATM
Category	Malware
Type	ATM malware
Description	<p>(Trend Micro) Last August , security researchers released a blog discussing a new ATM malware family called Ripper which they believe was involved in the recent ATM attacks in Thailand. Large numbers of ATMs were also temporarily shut down as a precautionary measure.</p> <p>That analysis gave an overview of the techniques used by the malware, the fact that it targets three major ATM vendors, and compared Ripper to previous ATM malware families. Their analysis was based on the file with MD5 hash 15632224b7e5ca0ccb0a042daf2adc13. This file was uploaded to Virustotal by a user in Thailand on August 23.</p>
Information	<p><https://blog.trendmicro.com/trendlabs-security-intelligence/untangling-ripper-atm-malware/></p> <p><https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf></p> <p><https://www.dropbox.com/s/1xvhee0s7o12i61/Whitepaper ATM Heist GSB August 2016.pdf?dl=0></p>
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.ripper_atm >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:ATMRIPPER >

Last change to this tool card: 25 May 2020

Download this tool card in [JSON](#) format

All groups using tool ATMRipper

Changed	Name	Country	Observed	
APT groups				
	Cobalt Group		2016-Oct 2019	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=c80d3d14-4c5d-47e8-a960-fb9f4d13d05a