Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:50:37 UTC

Tool: MAPIget

Names	MAPIget
Category	Malware
Type	Info stealer
Description	This malware utility is a set of two files that operate in conjunction to extract email messages and attachments from an Exchange server. In order to operate successfully, these programs require authentication credentials for a user on the Exchange server, and must be run from a machine joined to the domain that has Microsoft Outlook installed (or equivalent software that provides the Microsoft 'Messaging API' (MAPI) service).
Information	<https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf> <http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.mapiget>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool MAPIget

Changed	Name	Country	Observed	
APT groups				
	Comment Crew, APT 1		2006-May 2018	

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