Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:38:01 UTC

Tool: GetMail

Names	GetMail
Category	Malware
Type	Info stealer
Description	Members of this family of malware are utilities designed to extract email messages and attachments from Outlook PST files. One part of this utility set is an executable, one is a dll. The malware may create a registry artifact related to the executable.
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.getmail>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool GetMail

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

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