Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:43:25 UTC

Tool: Dairy

Names	Dairy
Category	Malware
Type	Reconnaissance, Backdoor
Description	Members of this malware family are backdoors that provide file downloading, process listing, process killing, and reverse shell capabilities. This malware may also add itself to the Authorized Applications list for the Windows Firewall.
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.dairy>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Dairy

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

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