Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:27:39 UTC

Tool: DmaUp3.exe

Names	DmaUp3.exe
Category	Malware
Type	Reconnaissance, Credential stealer
Description	(Kaspersky) The module collects information about current system which includes the following: • Network adapter MAC address • CPU Name and Identifier • System default codepage • Windows OS and Service Pack versions • Hostname and IP address • Local user name • Cached passwords for Internet Explorer 6/7/8/9 (Protected Storage and IntelliForms) • Mozilla Firefox stored secrets (<12.0) • Chrome stored secrets • MS Outlook Express accounts • MS Windows Mail accounts • MS Windows Live Mail accounts • MS Outlook accounts (SMTP/IMAP/POP3/HTTP) • MSN Messenger • Gmail Nofifier credentials • Google Desktop accounts • Google Talk accounts If the module reveals that current System default codepage is 0412 (Korean) it terminates.
Information	<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08070901/darkhotelappendixindicators_kl.pdf>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool DmaUp3.exe

Changed	Name	Country	Observed	
APT groups				
	DarkHotel		2007-2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=c4e969d2-f993-4a23-8cc9-7b117f14182e