Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:20:52 UTC

Tool: LIGHTDART

Names	LIGHTDART
Category	Malware
Type	Downloader
Description	LIGHTDART is a tool used to access a pre-configured web page that hosts an interface to query a database or data set. The tool then downloads the results of a query against that web page to an encrypted RAR file. This RAR file (1.rar) is renamed and uploaded to an attacker controlled FTP server, or uploaded via an HTTP POST with a .jpg extension. The malware will execute this search once a day. The target webpage usually contains information useful to the attacker, which is updated on a regular basis. Examples of targeted information include weather information or ship coordinates.
Information	<http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool LIGHTDART

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

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