Threat Group Cards: A Threat Actor Encyclopedia

Tool: CookieTime

Names	CookieTime
Category	Malware
Type	Backdoor
Description	(Kaspersky) Compared to the already known malware clusters of the Lazarus group, CookieTime shows a different structure and functionality. This malware communicates with the C2 server using the HTTP protocol. In order to deliver the request type to the C2 server, it uses encoded cookie values and fetches command files from the C2 server. The C2 communication takes advantage of steganography techniques, delivered in files exchanged between infected clients and the C2 server. The contents are disguised as GIF image files, but contain encrypted commands from the C2 server and command execution results.
Information	<https://securelist.com/apt-trends-report-q1-2021/101967/>

Last change to this tool card: 16 May 2021

Download this tool card in JSON format

All groups using tool CookieTime

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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