Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:18:23 UTC

Tool: CookieBag

Names	CookieBag TROJAN.COOKIES
Category	Malware
Type	Backdoor
Description	This family of malware is a backdoor capable of file upload and download as well as providing remote interactive shell access to the compromised machine. Communication with the Command & Control (C2) servers uses a combination of single-byte XOR and Base64 encoded data in the Cookie and Set-Cookie HTTP header fields. Communication with the C2 servers is over port 80. Some variants install a registry key as means of a persistence mechanism. The hardcoded strings cited include a string of a command in common with several other APT1 families.
Information	<http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.cookiebag>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool CookieBag

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

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=8df20cec-8073-495f-9c2d-cc6fb70028ec