Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:21:21 UTC

Tool: BarbWire

Names	BarbWire
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Credential stealer, Keylogger, Downloader, Exfiltration
Description	(Cybereason) The backdoor component of APT-C-23's operation is a very capable piece of malware, and it is obvious that a lot of effort was put into hiding its capabilities using a custom base64 algorithm. Its main goal is to fully compromise the victim machine, gaining access to their most sensitive data. The backdoor's main capabilities include: • Persistence • OS Reconnaissance • Data encryption • Keylogging • Screen capturing • Audio recording • Download additional malware • Local/external drives and directory enumeration • Steal specific file types and exfiltrate data
Information	<https://www.cybereason.com/blog/operation-bearded-barbie-apt-c-23-campaign-targeting-israeli-officials>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.barbwire>

Last change to this tool card: 27 December 2022

Download this tool card in JSON format

All groups using tool BarbWire

Changed	Name	Country	Observed

APT groups

	Desert Falcons	[Gaza]	2011-Oct 2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=97f960d1-4a27-4432-ad27-a21a572ef9ce