Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:35:40 UTC

Tool: OpGhoul

Names	OpGhoul
Category	Malware
Type	Reconnaissance, Backdoor, Keylogger, Credential stealer, Info stealer
Description	(Kaspersky) The malware is based on the Hawkeye commercial spyware, which provides a variety of tools for the attackers, in addition to malware anonymity from attribution. It initiates by self-deploying and configuring persistence, while using anti-debugging and timeout techniques, then starts collecting interesting data from the victim's device, including: • Keystrokes • Clipboard data • FileZilla ftp server credentials • Account data from local browsers • Account data from local messaging clients (Paltalk, Google talk, AIM…) • Account data from local email clients (Outlook, Windows Live mail…) • License information of some installed applications
Information	<https://securelist.com/operation-ghoul-targeted-attacks-on-industrial-and-engineering-organizations/75718/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.opghoul>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool OpGhoul

Changed	Name	Country	Observed	
APT groups				
	Operation Ghoul	[Unknown]	2016	

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