Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:00:03 UTC

Tool: BLUELIGHT

Names	BLUELIGHT
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Credential stealer, Downloader, Exfiltration
Description	(Volexity) The BLUELIGHT malware family uses different cloud providers to facilitate C2. This specific sample leveraged the Microsoft Graph API for its C2 operations. Upon start-up, BLUELIGHT performs an oauth2 token authentication using hard-coded parameters. Once the client is authenticated, BLUELIGHT creates a new subdirectory in the OneDrive appfolder and populates it with several subdirectories used by the C2 protocol.
Information	<https://www.volexity.com/blog/2021/08/17/north-korean-apt-inkysquid-infects-victims-using-browser-exploits/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0657/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.bluelight>

Last change to this tool card: 13 October 2023

Download this tool card in JSON format

All groups using tool BLUELIGHT

Changed	Name	Country	Observed	
APT groups				
	Reaper, APT 37, Ricochet Chollima, ScarCruft		2012-Mar 2025	

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