Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:08:00 UTC

Tool: Deadglyph

Names	Deadglyph
Category	Malware
Type	Backdoor
Description	(ESET) Deadglyph's loading chain consists of multiple components, as illustrated in Figure 3. The initial component is a registry shellcode loader, which loads shellcode from the registry. This extracted shellcode, in turn, loads the native x64 part of the backdoor – the Executor. The Executor subsequently loads the .NET part of the backdoor – the Orchestrator. Notably, the only component on system's disk as a file is the initial component, which is in the form of a Dynamic Link Library (DLL). The remaining components are encrypted and stored within a binary registry value.
Information	<https://www.welivesecurity.com/en/eset-research/stealth-falcon-preying-middle-eastern-skies-deadglyph/>

Last change to this tool card: 12 October 2023

Download this tool card in JSON format

All groups using tool Deadglyph

Changed	Name	Country	Observed	
APT groups				
	Stealth Falcon, FruityArmor		2012-Mar 2025	

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