Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:47:20 UTC

Tool: Sibot

Names	Sibot
Category	Malware
Type	Backdoor
Description	(Microsoft) Sibot is a dual-purpose malware implemented in VBScript. It is designed to achieve persistence on the infected machine then download and execute a payload from a remote C2 server. The VBScript file is given a name that impersonates legitimate Windows tasks and is either stored in the registry of the compromised system or in an obfuscated format on disk. The VBScript is then run via a scheduled task.
Information	<https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0589/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Sibot

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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