Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:44:41 UTC

Tool: Barlaiy

Names	Barlaiy POISONPLUG
Category	Malware
Type	Backdoor
Description	(Microsoft) Initial intrusion stages feature the Win32/Barlaiy implant—notable for its use of social network profiles, collaborative document editing sites, and blogs for C&C.
Information	<https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.poisonplug>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Barlaiy

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	
	Barium		2016-Nov 2017	

2 groups listed (2 APT, 0 other, 0 unknown)