Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 01:05:57 UTC

Tool: PocoDown

Names	PocoDown Blitz PocoDownloader
Category	Malware
Type	Tunneling
Description	Uses POCO C++ cross-platform library, XOR-based string obfuscation, SSL library code and string overlap with X-Tunnel, infrastructure overlap with X-Agent, probably in use since mid-2018
Information	<https://threatvector.cylance.com/en_us/home/inside-the-apt28-dll-backdoor-blitz.html> <https://threatvector.cylance.com/en_us/home/flirting-with-ida-and-apt28.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.pocodown>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool PocoDown

Changed	Name	Country	Observed	
APT groups				
	Sofacy, APT 28, Fancy Bear, Sednit		2004-Apr 2025	

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