Threat Group Cards: A Threat Actor Encyclopedia

Tool: WINNKIT

Names	WINNKIT
Category	Malware
Type	Rootkit
Description	(Cybereason) The final payload deployed by Winnti is also the most evasive and sophisticated: a driver acting as a rootkit, dubbed WINNKIT. WINNKIT's previous version was researched in the past, and its purpose is to act as a kernel-mode agent, interacting with the user-mode agent and intercepting TCP/IP requests, by talking directly to the network card. The almost zero detection rate in VirusTotal, together with the compilation timestamp from 2019, illustrates just how evasive this rootkit really is, staying in the shadows for 3 years.
Information	<https://www.cybereason.com/blog/operation-cuckoobees-a-winnti-malware-arsenal-deep-dive>

Last change to this tool card: 19 July 2022

Download this tool card in JSON format

All groups using tool WINNKIT

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	

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