Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:22:35 UTC

Tool: HighNoon

Names	HighNoon
Category	Malware
Type	Backdoor, Rootkit
Description	(FireEye) HIGHNOON is a backdoor that consists of multiple components, including a loader, dynamic-link library (DLL), and a rootkit. When loaded, the DLL may deploy one of two embedded drivers to conceal network traffic and communicate with its command and control server to download and launch memory-resident DLL plugins. HighNoon seems to be a variant of Winnti.
Information	<https://www.fireeye.com/blog/threat-research/2019/08/game-over-detecting-and-stopping-an-apt41-operation.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.highnoon> <https://malpedia.caad.fkie.fraunhofer.de/details/win.highnoon_bin>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:HIGHNOON>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool HighNoon

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	
	Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon		2010-Oct 2024	

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