Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:38:14 UTC

Tool: Nightdoor

Names	Nightdoor NetMM Suzafk
Category	Malware
Type	Backdoor
Description	(ESET) The backdoor that we have named Nightdoor (and is named NetMM by the malware authors according to PDB paths) is a late addition to Evasive Panda's toolset. Our earliest knowledge of Nightdoor goes back to 2020, when Evasive Panda deployed it onto a machine of a high-profile target in Vietnam. The backdoor communicates with its C&C server via UDP or the Google Drive API. The Nightdoor implant from this campaign used the latter. It encrypts a Google API OAuth 2.0 token within the data section and uses the token to access the attacker's Google Drive. We have requested that the Google account associated with this token be taken down.
Information	<https://www.welivesecurity.com/en/eset-research/evasive-panda-leverages-monlam-festival-target-tibetans/> <https://symantec-enterprise-blogs.security.com/threat-intelligence/daggerfly-espionage-updated-toolset>
MITRE ATT&CK	<https://attack.mitre.org/software/S1147>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.nightdoor>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool Nightdoor

Changed	Name	Country	Observed

APT groups

	Bronze Highland		2012-Jul 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=43a3efa0-ab8e-4404-8416-f2629a7026e3