Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:26:11 UTC

Tool: Ntospy

Names	Ntospy
Category	Malware
Type	Credential stealer
Description	(Palo Alto) To perform credential theft, the threat actor used a custom DLL module implementing a Network Provider. A Network Provider module is a DLL component implementing the interface provided by Microsoft to support additional types of network protocols during the authentication process. This technique is pretty well documented. Sergey Polak demonstrated the technique at BlackHat back in 2004 at his session titled “Capturing Windows Passwords using the Network Provider API.” In 2020, researcher Grzegorz Tworek uploaded his tool NPPSpy to GitHub, which also implements this technique. Due to the file naming patterns of the DLL module, and as a reference to the previous research and tools, Unit 42 researchers named this malware family Ntospy. The threat actor registers the Ntospy DLL module as a Network Provider module to hijack the authentication process, to get access to the user credentials every time the victim attempts to authenticate to the system.
Information	<https://unit42.paloaltonetworks.com/new-toolset-targets-middle-east-africa-usa/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ntospy>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool Ntospy

Changed	Name	Country	Observed
APT groups			

	Operation Diplomatic Specter		2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=674fc53a-c338-4d1f-af34-bd8379acfc2c