Ntospy (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 12:57:17 UTC

Ntospy is a credential stealer leveraging a well-established technique of abusing the Windows Network Provider interface, a method documented as early as 2004 and exemplified by tools like NPPSpy. Posing as a legitimate Network Provider DLL, Ntospy injects itself into the Windows authentication process, hijacking login attempts to harvest user credentials. It achieves this by registering a malicious Network Provider, typically named "credman," which intercepts authentication requests and redirects them to it malicious DLL.

Instead of immediately exfiltrating the stolen data, Ntospy employs a form of local storage, writing the captured credentials in cleartext to files disguised as harmless Microsoft Update packages using the .msu file extension. These files are often planted in system directories with believable names like "c:/programdata/package cache/windows10.0-kb5009543-x64.msu," further masking their malicious purpose.

Adding to its stealth, Ntospy incorporates obfuscation techniques to evade detection. This includes using seemingly innocuous filenames for its DLL, often mimicking critical system files like "ntoskrnl.dll" to blend in. Some variants even go a step further by encrypting the credential storage file path within the DLL, requiring analysis and decryption to uncover its full functionality.

▶ [TLP:WHITE] win_ntospy_auto (20251219 | Detects win.ntospy.)
