# TTP Detail – T1556.008

## TTP Information

Name: Network Provider DLL

Description: Adversaries may register malicious network provider dynamic link libraries (DLLs) to capture cleartext user credentials during the authentication process. Network provider DLLs allow Windows to interface with specific network protocols and can also support add-on credential management functions.(Citation: Network Provider API) During the logon process, Winlogon (the interactive logon module) sends credentials to the local `mpnotify.exe` process via RPC. The `mpnotify.exe` process then shares the credentials in cleartext with registered credential managers when notifying that a logon event is happening.(Citation: NPPSPY - Huntress)(Citation: NPPSPY Video)(Citation: NPLogonNotify)

Adversaries can configure a malicious network provider DLL to receive credentials from `mpnotify.exe`.(Citation: NPPSPY) Once installed as a credential manager (via the Registry), a malicious DLL can receive and save credentials each time a user logs onto a Windows workstation or domain via the `NPLogonNotify()` function.(Citation: NPLogonNotify)

Adversaries may target planting malicious network provider DLLs on systems known to have increased logon activity and/or administrator logon activity, such as servers and domain controllers.(Citation: NPPSPY - Huntress)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: credential-access

**•** mitre-attack: defense-evasion

**•** mitre-attack: persistence