# TTP Detail – T1556.005

## TTP Information

Name: Reversible Encryption

Description: An adversary may abuse Active Directory authentication encryption properties to gain access to credentials on Windows systems. The <code>AllowReversiblePasswordEncryption</code> property specifies whether reversible password encryption for an account is enabled or disabled. By default this property is disabled (instead storing user credentials as the output of one-way hashing functions) and should not be enabled unless legacy or other software require it.(Citation: store\_pwd\_rev\_enc)

If the property is enabled and/or a user changes their password after it is enabled, an adversary may be able to obtain the plaintext of passwords created/changed after the property was enabled. To decrypt the passwords, an adversary needs four components:

1. Encrypted password (<code>G$RADIUSCHAP</code>) from the Active Directory user-structure <code>userParameters</code>
2. 16 byte randomly-generated value (<code>G$RADIUSCHAPKEY</code>) also from <code>userParameters</code>
3. Global LSA secret (<code>G$MSRADIUSCHAPKEY</code>)
4. Static key hardcoded in the Remote Access Subauthentication DLL (<code>RASSFM.DLL</code>)

With this information, an adversary may be able to reproduce the encryption key and subsequently decrypt the encrypted password value.(Citation: how\_pwd\_rev\_enc\_1)(Citation: how\_pwd\_rev\_enc\_2)

An adversary may set this property at various scopes through Local Group Policy Editor, user properties, Fine-Grained Password Policy (FGPP), or via the ActiveDirectory [PowerShell](https://attack.mitre.org/techniques/T1059/001) module. For example, an adversary may implement and apply a FGPP to users or groups if the Domain Functional Level is set to "Windows Server 2008" or higher.(Citation: dump\_pwd\_dcsync) In PowerShell, an adversary may make associated changes to user settings using commands similar to <code>Set-ADUser -AllowReversiblePasswordEncryption $true</code>.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

**•** mitre-attack: defense-evasion

**•** mitre-attack: persistence