Detection of Encrypted Channel, Detection Strategy DET0641

Archived: 2026-04-05 16:20:43 UTC

AN1716

Since data encryption is a common practice in many legitimate applications and uses standard programming language-specific APIs, encrypting data for command and control communication is regarded as undetectable to the user.

AN1717

Since data encryption is a common practice in many legitimate applications and uses standard programming language-specific APIs, encrypting data for command and control communication is regarded as undetectable to the user.

Source: https://attack.mitre.org/detectionstrategies/DET0641#AN1717