

Detection of Symmetric Cryptography, Detection Strategy

DET0650

Archived: 2026-04-05 12:36:35 UTC

AN1731

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.

AN1732

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/DET0650#AN1731>