Exploitation of Remote Services, Technique T0866 - ICS

Archived: 2026-04-05 14:11:42 UTC

Adversaries may exploit a software vulnerability to take advantage of a programming error in a program, service, or within the operating system software or kernel itself to enable remote service abuse. A common goal for post-compromise exploitation of remote services is for initial access into and lateral movement throughout the ICS environment to enable access to targeted systems. [1]

ICS asset owners and operators have been affected by ransomware (or disruptive malware masquerading as ransomware) migrating from enterprise IT to ICS environments: WannaCry, NotPetya, and BadRabbit. In each of these cases, self-propagating (wormable) malware initially infected IT networks, but through exploit (particularly the SMBv1-targeting MS17-010 vulnerability) spread to industrial networks, producing significant impacts. [2]

Source: https://attack.mitre.org/techniques/T0866