Template Injection Attacks - Bypassing Security Controls by Living off the Land

By Created by:Brian Wiltse

Archived: 2026-04-05 15:41:49 UTC

As adversary tactics continue to adapt and embrace the concept of living off the land by using legitimate company software instead of a virus or other malwareRut15, their tactics techniques and procedures (TTPs) often leverage programs and features in target environments that are normal and expected. The adversaries leverage these features in a way that enables them to bypass security controls to complete their objective. In May of 2017, a suspected APT group began to leverage one such feature in Microsoft Office, utilizing a Template Injection attack to harvest credentials, or gain access to end users computers at a US power plant operator, Wolf Creek Nuclear Operating Corp. In this Gold Paper, we will review in detail what the Template Injection attacks may have looked like against this target, and assess their ability to bypass security controls.
