Registry Keys for Persistence

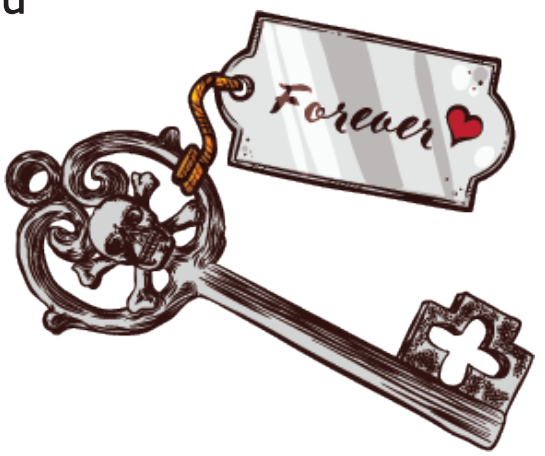
The attackers add/modify registry commands to cause their malware to run on system startup and/or user login. This has been around forever. Almost every piece of solid malware in existence can do this.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

reg command



https://attack.mitre.org/techniques/T1112

EXPV1_0421

Backdoors™ & Breaches

PERSISTENCE

Created by: BLACK HILLS | Information Security