

APPLICATION SHIMMING

The attackers use the Application Compatibility Toolkit to trick applications into not seeing the ports, directories, files, and services the attackers want to hide.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

Windows Assessment and Deployment Kit (ADK)



*These are not
the ports you're
looking for.*

[https://docs.microsoft.com/en-us/windows-hardware/
get-started/adk-install](https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install)

<https://attack.mitre.org/techniques/T1546/011/>



Backdoors™ & Breaches

PERSISTENCE

Created by: **BLACK HILLS** | Information Security