THE BRIDGE

CYBER SECURITY

Escalada de Privilegios Windows I

Hijack Execution Flow: Path Interception by Unquoted Path

T1574	Hijack Execution Flow	Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution.

.009	Path Interception by Unquoted Path	Adversaries may execute their own malicious payloads by hijacking vulnerable file path references. Adversaries can take advantage of paths that lack surrounding quotations by placing an executable in a higher level directory within the path, so that Windows will choose the adversary's executable to launch.

C:\Program Files\A Subfolder\B Subfolder\C Subfolder\SomeExecutable.exe

1. C:\Program.exe
2. C:\Program Files\A.exe
3. C:\Program Files\A Subfolder\B.exe
4. C:\Program Files\A Subfolder\B Subfolder\C.exe
5. C:\Program Files\A Subfolder\B Subfolder\C Subfolder\SomeExecutable.exe

- (F) Full Control
- (M) Modify
- (W) Write

- The user we are currently logged in as (%USERNAME%)
- Authenticated Users
- Everyone
- BUILTIN\Users
- NT AUTHORITY\INTERACTIVE


THE
BRIDGE