Mavinject on LOLBAS

Archived: 2026-04-02 12:40:53 UTC

Used by App-v in Windows

Paths:

- C:\Windows\System32\mavinject.exe
- C:\Windows\SysWOW64\mavinject.exe

Resources:

- https://twitter.com/gN3mes1s/status/941315826107510784
- https://twitter.com/Hexcorn/status/776122138063409152
- https://oddvar.moe/2018/01/14/putting-data-in-alternate-data-streams-and-how-to-execute-it/

Acknowledgements:

- Giuseppe N3mes1s (@gN3mes1s)
- Oddvar Moe (@oddvarmoe)

Detections:

- Sigma: proc_creation_win_lolbin_mavinject_process_injection.yml
- IOC: mavinject.exe should not run unless APP-v is in use on the workstation

Execute

1. Inject evil.dll into a process with PID 3110.

   ```
   MavInject.exe 3110 /INJECTRUNNING C:\Windows\Temp\file.dll
   ```

   Use case

   Inject dll file into running process

   Privileges required

   User

   Operating systems

   Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

   ATT&CK® technique

   T1218.013: Mavinject

   Tags

Execute: DLL

Alternate data streams

1. Inject file.dll stored as an Alternate Data Stream (ADS) into a process with PID 4172

   ```
   Mavinject.exe 4172 /INJECTRUNNING C:\Windows\Temp\file.ext:file.dll
   ```

   Use case

   Inject dll file into running process

   Privileges required

   User

   Operating systems

   Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

   ATT&CK® technique

   T1564.004: NTFS File Attributes

   Tags

   Execute: DLL
