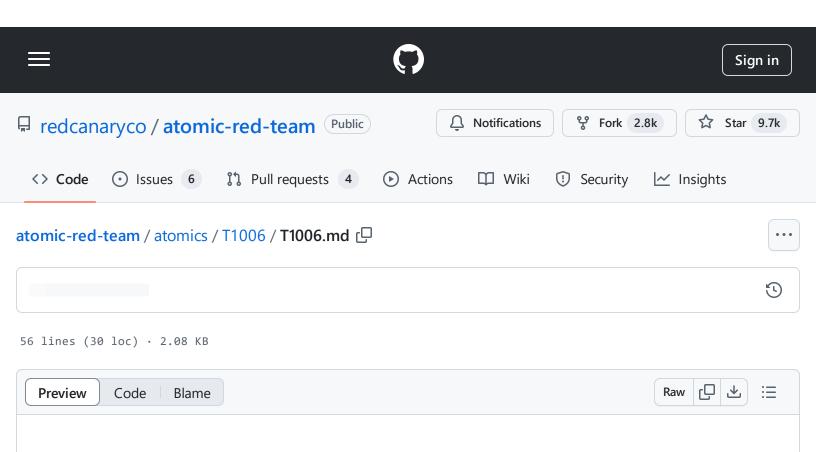
atomic-red-team/atomics/T1006/T1006.md at f339e7da7d05f6057fdfcdd3742bfcf365fee2a9 · redcanaryco/atomic-red-team · GitHub - 31/10/2024 17:29 https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1006/T1006.md



T1006 - Direct Volume Access

Description from ATT&CK

Adversaries may directly access a volume to bypass file access controls and file system monitoring. Windows allows programs to have direct access to logical volumes. Programs with direct access may read and write files directly from the drive by analyzing file system data structures. This technique bypasses Windows file access controls as well as file system monitoring tools. (Citation: Hakobyan 2009)

Utilities, such as NinjaCopy, exist to perform these actions in PowerShell. (Citation: Github PowerSploit Ninjacopy)

Atomic Tests

Atomic Test #1 - Read volume boot sector via DOS device path (PowerShell)

Atomic Test #1 - Read volume boot sector via DOS device path (PowerShell)

For a NTFS volume, it should correspond to the following sequence (NTFS partition boot sector):

Supported Platforms: Windows

auto_generated_guid: 88f6327e-51ec-4bbf-b2e8-3fea534eab8b

Inputs:

Name	Description	Туре	Default Value
volume	Drive letter of the volume to access	String	C:

Attack Commands: Run with powershell! Elevation Required (e.g. root or admin)

```
$buffer = New-Object byte[] 11
$handle = New-Object IO.FileStream "\\.\#{volume}", 'Open', 'Read', 'ReadWrite'
$handle.Read($buffer, 0, $buffer.Length)
$handle.Close()
Format-Hex -InputObject $buffer
```