

## EDR/XDR/MDR

EDR/XDR/MDR Windows Defender AV/EDR AV/EDR

AMSI 'Invoke-Mimikatz' PowerShell

```
PS C:\> 'Invoke-Mimikatz'
At line:1 char:1
+ 'Invoke-Mimikatz'
+ ~~~~~
This script contains malicious content and has been blocked by your antivirus software.
+ CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent
```

## UAC

UAC (Get-ItemProperty PowerShell

HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System).EnableLUA

```
(Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System).EnableLUA
```

```
PS C:\> (Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System).EnableLUA
1
PS C:\>
```

## AppLocker

AppLocker Get-ChildItem -Path Powershell

HKLM:\SOFTWARE\Policies\Microsoft\Windows\SrpV2\Exe\

```
Get-ChildItem -Path HKLM:\SOFTWARE\Policies\Microsoft\Windows\SrpV2\Exe\
```

```
PS C:\Users\john> Get-ChildItem -Path HKLM:\SOFTWARE\Policies\Microsoft\Windows\SrpV2\Exe\

Hive: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\SrpV2\Exe

Name      Property
----      -
921cc481-6e17-4653-8f75-050b80acca20 Value : <FilePathRule Id="921cc481-6e17-4653-8f75-050b80acca20" Name="(Default Rule)
acca20    All files located in the Program
          Files folder" Description="Allows members of the Everyone group to run
          applications that are located in the
          Program Files folder." UserOrGroupSid="S-1-1-0"
          Action="Allow"><Conditions><FilePathCondition
          Path="%PROGRAMFILES%\*" /></Conditions></FilePathRule>
a61c8b2c-a319-4cd0-9690-d2177cad7b51 Value : <FilePathRule Id="a61c8b2c-a319-4cd0-9690-d2177cad7b51" Name="(Default Rule)
ad7b51    All files located in the Windows
          folder" Description="Allows members of the Everyone group to run applications
          that are located in the Windows
          folder." UserOrGroupSid="S-1-1-0" Action="Allow"><Conditions><FilePathCondition
          Path="%WINDIR%\*" /></Conditions></FilePathRule>
fd686d83-a829-4351-8ff4-27c7de5755d2 Value : <FilePathRule Id="fd686d83-a829-4351-8ff4-27c7de5755d2" Name="(Default Rule)
5755d2    All files" Description="Allows
          members of the local Administrators group to run all applications."
          UserOrGroupSid="S-1-5-32-544"
          Action="Allow"><Conditions><FilePathCondition
          Path="*" /></Conditions></FilePathRule>
```

CLM

CLM

AppLocker

CLM

Powershell

C

**\$ExecutionContext.SessionState.LanguageMode**

```
$ExecutionContext.SessionState.LanguageMode
```

```
PS C:\Users\john> $ExecutionContext.SessionState.LanguageMode
FullLanguage
PS C:\Users\john> $ExecutionContext.SessionState.LanguageMode="ConstrainedLanguage"
PS C:\Users\john> $ExecutionContext.SessionState.LanguageMode
ConstrainedLanguage
PS C:\Users\john> [Math].Cos(1)
Cannot invoke method. Method invocation is supported only on core types in this language mode.
At line:1 char:1
+ [Math].Cos(1)
+ ~~~~~
+ CategoryInfo          : InvalidOperation: (:) [], RuntimeException
+ FullyQualifiedErrorId : MethodInvocationNotSupportedInConstrainedLanguage

PS C:\Users\john>
```

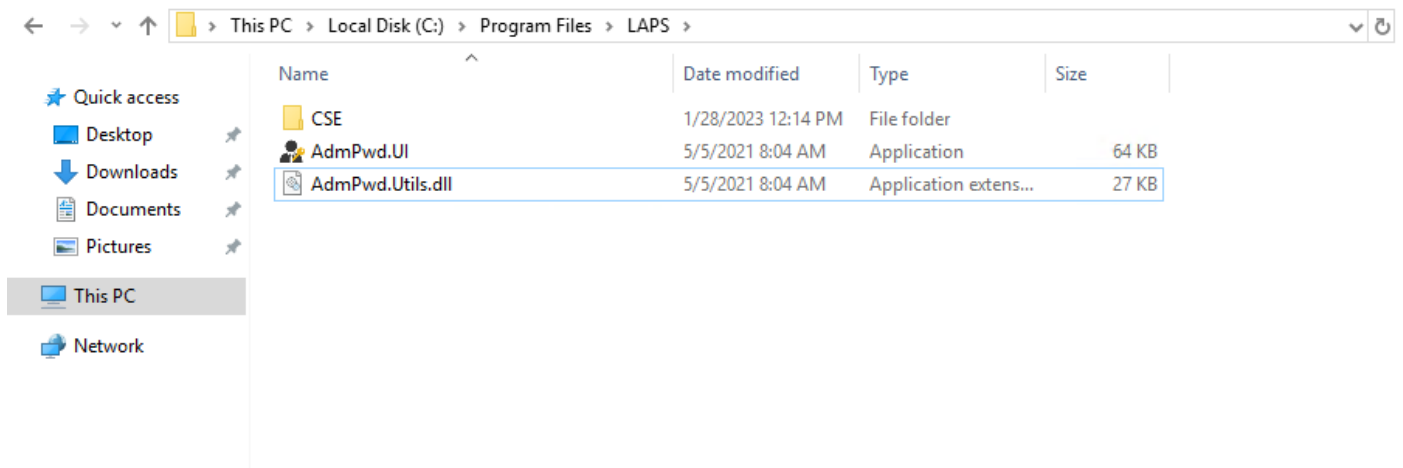
LAPS

LAPS

AdmPwd

LAPS

LAPS



## RunAsPPL

RunAsPPL      Isass.exe      mimikatz      **Get-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Control\Lsa -Name "RunAsPPL"**      PPL

```
Get-ItemProperty -Path  
HKLM: \SYSTEM\CurrentControlSet\Control\Lsa -Name "RunAsPPL"
```

```
PS C:\Users\sql_service> Get-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Control\Lsa -Name "RunAsPPL"  
  
RunAsPPL      : 1  
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa  
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control  
PSChildName   : Lsa  
PSDrive       : HKLM  
PSProvider    : Microsoft.PowerShell.Core\Registry
```

Revision #5  
Created 5 September 2022 03:03:04 by  
Updated 20 July 2023 19:19:16 by unknown