

Open in app ↗


Sign up Sign in

Medium

Search

Write

The Tale of SettingContent-ms Files



Matt Nelson · Follow

Published in Posts By SpecterOps Team Members · 9 min read · Jun 11, 2018

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

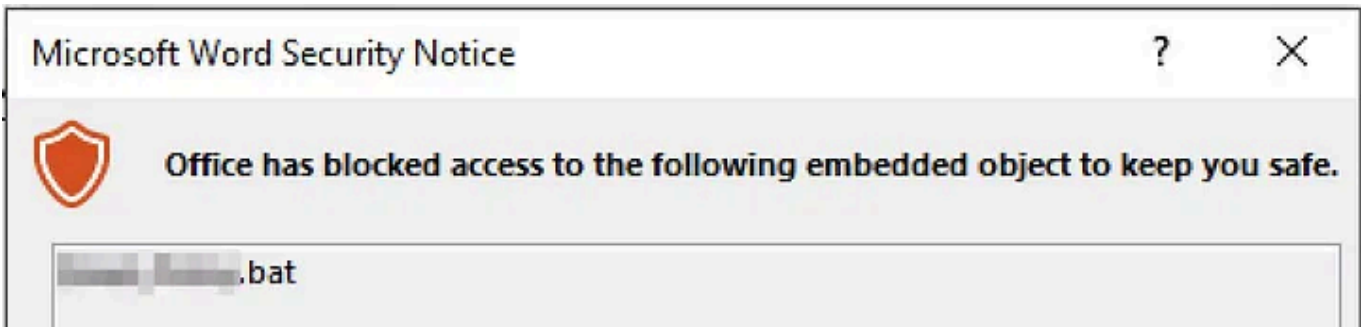
Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

being embedded via OLE by default. This reduces the effectiveness of one of the most relied upon payload delivery methods. When trying to activate a blocked file extension, Office will throw an error and prevent execution:



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

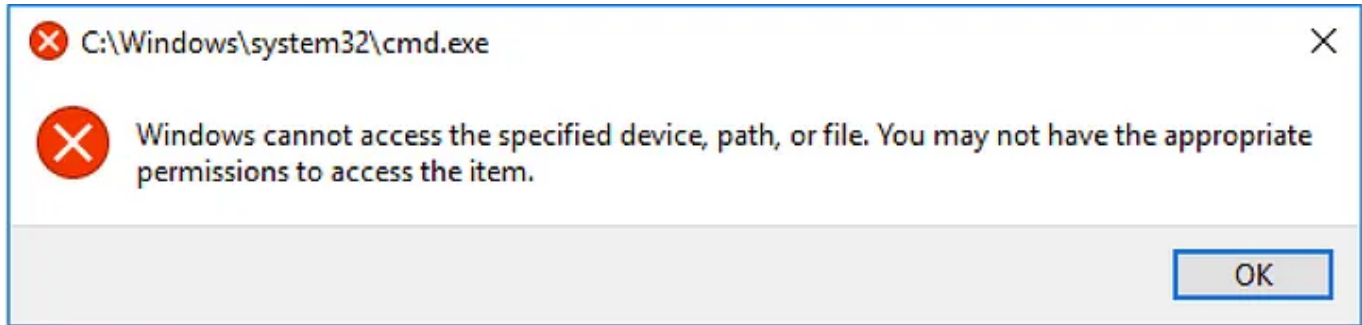
- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month



Attack Surface Reduction Rules blocking Office child processes

When you combine OLE blocking and ASR together, the options to execute code on an endpoint from the internet become a little more limited. Most

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

```
ControlPanel - Notepad
File Edit Format View Help
<?xml version="1.0" encoding="UTF-8"?>
<PCSettings>
  <SearchableContent xmlns="http://schemas.microsoft.com/Search/2013/SettingContent">
    <ApplicationInformation>
      <AppID>windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel</AppID>
      <DeepLink>%windir%\system32\control.exe</DeepLink>
      <Icon>%windir%\system32\control.exe</Icon>
    </ApplicationInformation>
    <SettingIdentity>
      <PageID></PageID>
      <HostID>{12B1697E-D3A0-4DBC-B568-CCF64A3F934D}</HostID>
    </SettingIdentity>
    <SettingInformation>
      <Description>@shell32.dll,-4161</Description>
      <Keywords>@shell32.dll,-4161</Keywords>
    </SettingInformation>
  </SearchableContent>
</PCSettings>
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

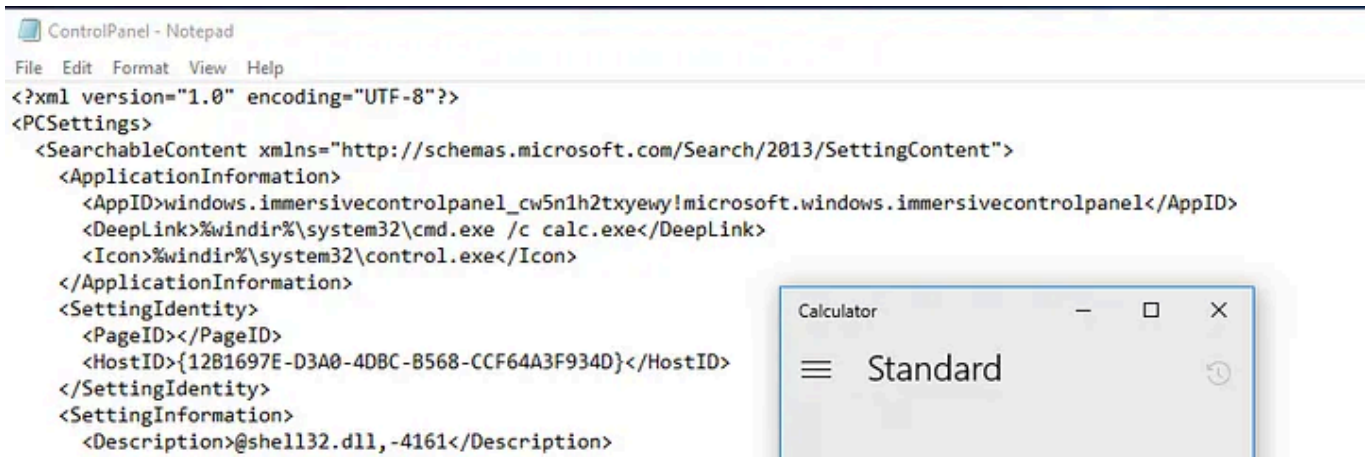
Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Then if we double-click the file:



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

When looking up the ZoneIds online, “3” equals “URLZONE_INTERNET”. For one reason or another, the file still executes without any notification or warning to the user.

So, we now have a file type that allows arbitrary shell command execution and displays zero warnings or dialogues to the user. When trying to get initial access, going across a target’s perimeter with an unusual file type can be risky. Ideally, this file would be placed in a container of a more common file type, such as an Office document.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

The <rule ID> parameter is the GUID of the rule you want to enabled. You can find the GUID for each ASR rule documented [here](#). For this test, I want to enable the Child Process Creation rule, which is GUID D4F940AB-401B-4EFC-AADC-AD5F3C50688A.

After enabling the rule, the attack no longer works:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

while clicking around in Word, I noticed that there were still child processes being spawned by Word.

Valid child process creation of Word

This makes sense, as Office needs to use features that rely on other programs. I thought that maybe the ASD rule blocks child processes based

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

The next step is to embed this new file into a Word document and see if ASR blocks “Excel.exe” from being spawned.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Execution of commands via ASR whitelisted "AppVI P.exe"

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

file type appears to give execution (even from the internet) immediately after it's opened, despite having the MOTW applied.

Defenses:

Great, so what can you do about it? Ultimately, a .SettingContent-ms file should not be executing anywhere outside of the “C:\Windows\ImmersiveControlPanel” path. Additionally, since the file format only allows for executing shell commands, anything being run through that file is subject to command line logging.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

As committed as SpecterOps is to transparency (<https://posts.specterops.io/a-push-toward-transparency-c385a0dd1e34>), we acknowledge the rate at which attackers adopt new offensive techniques once they are made public. This is why prior to publicization of a new offensive technique, we regularly inform the respective vendor of the issue, supply ample time to mitigate the issue, and notify select, trusted vendors in order to ensure detections can be delivered to their customers as quickly as possible.

2/16/2018• Report sent MSPC

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

[UPDATE] 8/14/2018: MSRC fixed the issue CVE-2018-8414
(<https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-8414>)

Cheers,

Matt N.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month