Commit

Adding runscripthelper.exe to the blacklist ruleset

Browse files

Reference for the runscripthelper.exe bypass:
https://posts.specterops.io/bypassing-application-whitelisting-with-runscripthelper-exe-1906923658fc

Also giving credit to Lee Christensen for his visualuiaverifynative.exe
bypass contribution.

Loading branch information

Matt Graeber committed on Nov 2, 2017 1 parent f6d122d commit 937db70

Showing **1 changed file** with **3 additions** and **0 deletions**. Whitespace Ignore whitespace Split Unified

3

windows/device-security/device-guard/deploy-code-integrity-policies-steps.md

```
@@ -73,6 +73,7 @@ Unless your use scenarios explicitly require them, Microsoft recommends that you
|Matt Nelson | @enigma0x3|
|Oddvar Moe |@Oddvarmoe|
|Alex Ionescu | @aionescu|
+|Lee Christensen|@tifkin_|

<br />

@@ -134,6 +135,7 @@ Microsoft recommends that you block the following Microsoft-signed applications
    <Deny  ID="ID_DENY_FSI_ANYCPU"    FriendlyName="fsiAnyCpu.exe" FileName="fsiAnyCpu.exe" MinimumFileVersion = "65535.65535.65535.65535" />
```

```
135  136        <Deny  ID="ID_DENY_MSHTA"         FriendlyName="mshta.exe"          FileName="mshta.exe"
                MinimumFileVersion = "65535.65535.65535.65535" />
136  137        <Deny  ID="ID_DENY_VISUALUIAVERIFY"         FriendlyName="visualuiaverifynative.exe"
                FileName="visualuiaverifynative.exe" MinimumFileVersion = "65535.65535.65535.65535" />
     138  +     <Deny  ID="ID_DENY_RUNSCRIPTHELPER"         FriendlyName="runscripthelper.exe"
                FileName="runscripthelper.exe" MinimumFileVersion="65535.65535.65535.65535" />
137  139
138  140        <Deny ID="ID_DENY_D_1" FriendlyName="Powershell 1"
                Hash="02BE82F63EE962BCD4B8303E60F806F6613759C6" />
139  141        <Deny ID="ID_DENY_D_2" FriendlyName="Powershell 2"
                Hash="13765D9A16CC46B2113766822627F026A68431DF" />
                @@ -418,6 +420,7 @@ Microsoft recommends that you block the following Microsoft-signed
                applications
418  420              <FileRuleRef RuleID="ID_DENY_FSI_ANYCPU" />
419  421              <FileRuleRef RuleID="ID_DENY_MSHTA" />
420  422              <FileRuleRef RuleID="ID_DENY_VISUALUIAVERIFY" />
     423  +           <FileRuleRef RuleID="ID_DENY_RUNSCRIPTHELPER"/>
421  424              <FileRuleRef RuleID="ID_DENY_D_1" />
422  425              <FileRuleRef RuleID="ID_DENY_D_2" />
423  426              <FileRuleRef RuleID="ID_DENY_D_3" />
```

0 comments on commit `937db70`

Please sign in to comment.