DuPSUG

PowerShell and Security

The how, what and why

Jaap Brasser

@Jaap_Brasser

Most important information...

- SSID: xxxxxxxx
- Password: xxxxxxxx

About_Jaap

- Dutch PowerShell User Group
- Blogging
  - PowerShell Magazine
  - JaapBrasser.com
- Slack
- Reddit
- GitHub
- PowerShell Gallery
- TechNet Forums/Gallery

@Jaap_Brasser

Agenda

- PowerShell security
- Malware and PowerShell
- Configuring and securing PowerShell
- Just enough administration (JEA)
- Questions and discussion

Why does malware love PowerShell

- Easy to automate
- Available by default on modern OS
- Access to .Net
- Now also on Linux & Mac
- Can run C#

We know you have your choice of post-exploitation languages
so we thank you for hacking with PowerShell

Demo 1 – Configure PS Logging

```
1  Describe 'This is my Pester test' {
2      Context 'Certainly nothing will fail' {
3          It 'This almost never fails' {
4              42.0001 | Should Be 42
5          }
6          It 'Simple text comparison' {
7              'Hello' | Should Match 'World'
8          }
9          It 'Compare two arrays' {
10             @(1,2) | Should BeExactly @(1,2,3)
11         }
12     }
13 }
```

```
Describing This is my Pester test
   Context Certainly nothing will fail
    [-] This almost never fails 76ms
      Expected: {42}
      But was:  {42.0001}
      4:              42.0001 | Should Be 42
      at <ScriptBlock>, <No file>: line 4
    [-] Simple text comparison 69ms
      Expected: {Hello} to match the expression {World}
      7:              'Hello' | Should Match 'World'
      at <ScriptBlock>, <No file>: line 7
    [+] Compare two arrays 28ms
```

Demo Summary

- How to configure PowerShell logging
- The different logging mechanisms

Demo 2 – Obfuscate Logging

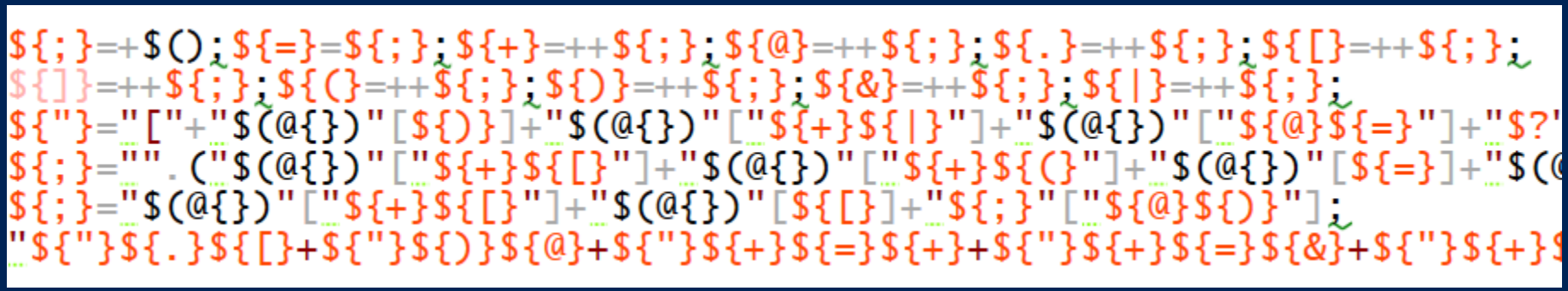
```
1  Describe 'This is my Pester test' {
2      Context 'Certainly nothing will fail' {
3          It 'This almost never fails' {
4              42.0001 | Should Be 42
5          }
6          It 'Simple text comparison' {
7              'Hello' | Should Match 'World'
8          }
9          It 'Compare two arrays' {
10             @(1,2) | Should BeExactly @(1,2,3)
11         }
12     }
13 }
```

```
Describing This is my Pester test
   Context Certainly nothing will fail
    [-] This almost never fails 76ms
      Expected: {42}
      But was:  {42.0001}
      4:              42.0001 | Should Be 42
      at <ScriptBlock>, <No file>: line 4
    [-] Simple text comparison 69ms
      Expected: {Hello} to match the expression {World}
      7:              'Hello' | Should Match 'World'
      at <ScriptBlock>, <No file>: line 7
    [+] Compare two arrays 28ms
```

Demo Summary

- How to obfuscate logging
- What techniques are there
- How to detect obfuscated code

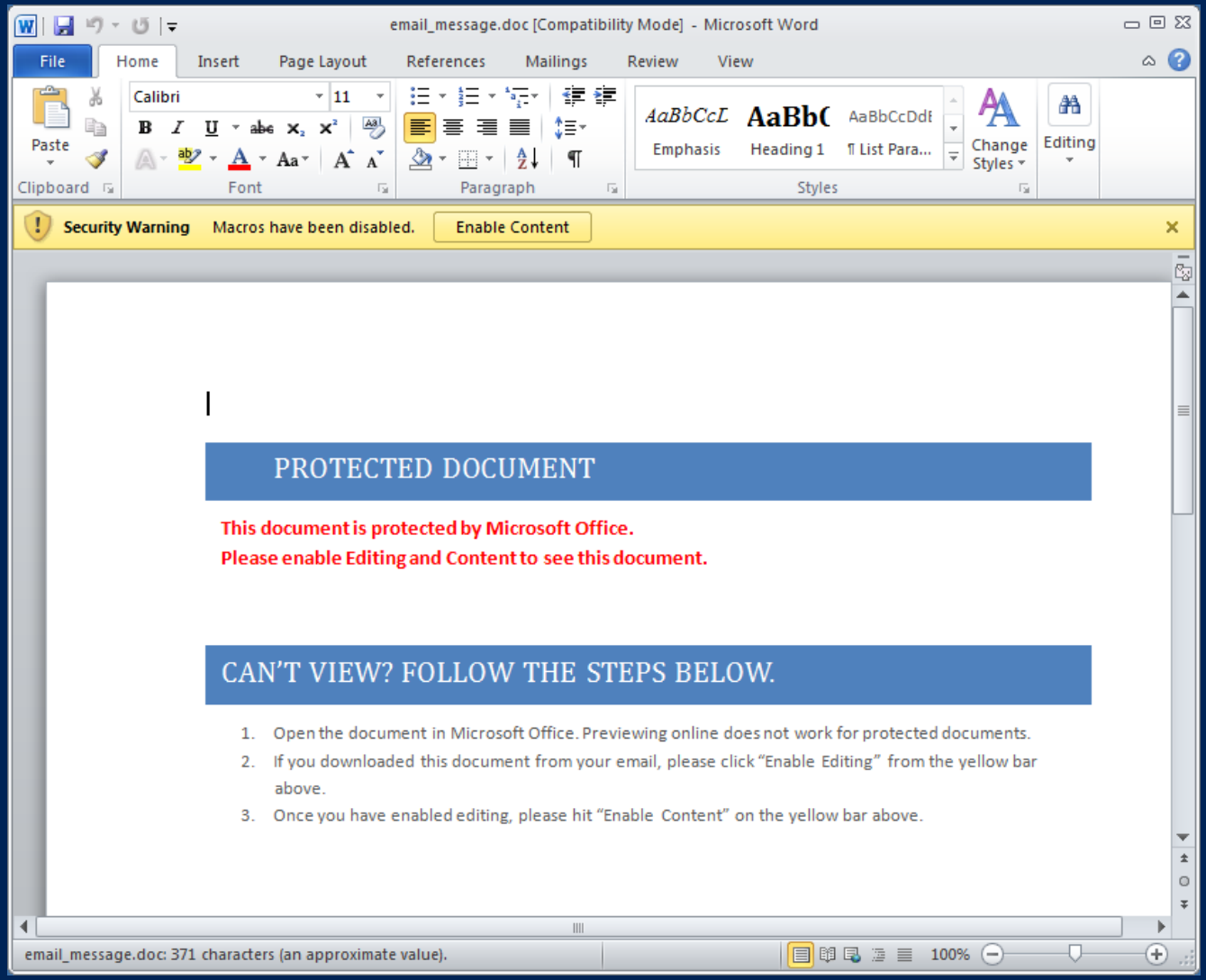
DuPSUG



Compromized system

Just Enough Administration

- Introduced in 2014
- Delegated administration
- Limit what users can do
- Anything managed by PowerShell


email_message.doc [Compatibility Mode] - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Calibri
11
Paste
Clipboard
Font
Paragraph
Emphasis
Heading 1
List Para...
Change Styles
Editing
Styles
Security Warning
Macros have been disabled.
Enable Content
PROTECTED DOCUMENT
This document is protected by Microsoft Office.
Please enable Editing and Content to see this document.
CAN'T VIEW? FOLLOW THE STEPS BELOW.
1. Open the document in Microsoft Office. Previewing online does not work for protected documents.
2. If you downloaded this document from your email, please click "Enable Editing" from the yellow bar above.
3. Once you have enabled editing, please hit "Enable Content" on the yellow bar above.
email_message.doc: 371 characters (an approximate value).
100%

PowerShell Endpoints

- Available in PowerShell since 2.0
- Allows for delegation
- Default endpoints
  - microsoft.powershell
  - microsoft.powershell.workflow
  - microsoft.powershell32

PowerShell Language Modes

- Different language modes
  - FullLanguage
  - ConstrainedLanguage
  - RestrictedLanguage
  - NoLanguage
- Determines what the console can do

DuPSUG

JEADemo1 – Create endpoints

```
PS C:\Users\JaapBrasser> $Files = Get-ChildItem -Path C:\Windows\ -Recurse
Get-ChildItem : Access to the path 'C:\Windows\appcompat\Programs' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\appcompat\Programs:String) [Get-ChildItem], UnauthorizedAc
   cessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\CSC' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\CSC:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\InfusedApps' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\InfusedApps:String) [Get-ChildItem], UnauthorizedAccessExc
   eption
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\LiveKernelReports' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\LiveKernelReports:String) [Get-ChildItem], UnauthorizedAcc
   essException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```

Demo Summary

- Created two endpoints
- Viewed the resources used
- View the generated start up script
- View SDDL

DuPSUG

JEADemo2 – Connect JEA endpoint

```
PS C:\Users\JaapBrasser> $Files = Get-ChildItem -Path C:\Windows\ -Recurse
Get-ChildItem : Access to the path 'C:\Windows\appcompat\Programs' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\appcompat\Programs:String) [Get-ChildItem], UnauthorizedAc
   cessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\CSC' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\CSC:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\InfusedApps' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\InfusedApps:String) [Get-ChildItem], UnauthorizedAccessExc
   eption
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\LiveKernelReports' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\LiveKernelReports:String) [Get-ChildItem], UnauthorizedAcc
   essException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```

Demo Summary

- Connect to a JEA endpoint
- View the output
- What is retricted in the languagemode

DuPSUG

JEADemo3 – Edit Configuration

```
PS C:\Users\JaapBrasser> $Files = Get-ChildItem -Path C:\Windows\ -Recurse
Get-ChildItem : Access to the path 'C:\Windows\appcompat\Programs' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\appcompat\Programs:String) [Get-ChildItem], UnauthorizedAc
   cessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\CSC' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\CSC:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\InfusedApps' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\InfusedApps:String) [Get-ChildItem], UnauthorizedAccessExc
   eption
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\LiveKernelReports' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\LiveKernelReports:String) [Get-ChildItem], UnauthorizedAcc
   essException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```

Demo Summary

- Use a non-administrative user
- Configure single user SDDL
- Change the start up script
  - Can be used to set own defaults

DuPSUG

JEADemo4 – GUI Uses for JEA

```
PS C:\Users\JaapBrasser> $Files = Get-ChildItem -Path C:\Windows\ -Recurse
Get-ChildItem : Access to the path 'C:\Windows\appcompat\Programs' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\appcompat\Programs:String) [Get-ChildItem], UnauthorizedAc
   cessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\CSC' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\CSC:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\InfusedApps' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\InfusedApps:String) [Get-ChildItem], UnauthorizedAccessExc
   eption
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\LiveKernelReports' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\LiveKernelReports:String) [Get-ChildItem], UnauthorizedAcc
   essException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```

Demo Summary

- Use JEA endpoint for GUI apps
- Use JEA endpoint in scripts

Questions?

powershell.reageer.tv

Learn more about PowerShell

- github.com/PowerShell/PowerShell
- www.powershellmagazine.com
- www.dupsug.com
- www.jaapbrasser.com/how-learn-powershell
- Github.com/jaapbrasser/events