Using PowerShell to defeat malware

Jaap Brasser

About_jaap

@Jaap_Brasser

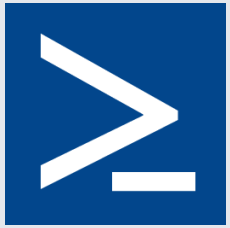
- Dutch PowerShell User Group
- Blogging
  - PowerShell Magazine
  - JaapBrasser.com
- Slack
- Reddit
- GitHub
- PowerShell Gallery
- TechNet Forums/Gallery

Agenda

- What is PowerShell security
- Example of PowerShell logging and limitations
- How to use PowerShell against real threats
- Example of utilizing PowerShell against ransomware
- How to secure your environment against ransomware
- What to expect in the future
- Questions and Answers

Why does malware love PowerShell

- Easy to automate
- Available by default on modern OS
- Access to .Net
- Now also on Linux & Mac
- Can execute C# sharp without compiler



What is PowerShell Security

PowerShell Security is regular security

How to secure PowerShell

- Execution Policy
- Using Constrained Remoting Endpoints
- Just enough administration
- Configure PowerShell logging

Tale of two users

Demo – PowerShell Logging

```
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

- How to enable PowerShell logging
- What to look for when logging
- How to obscure the logs

Trojan infection on critical system

- Name of the Trojan
- Generic description of its capabilities
- List of potential infected files
- A VLAN to which the Trojan was most likely contained

Ransomware

Lab environment

Windows 10

Server 2016

Demo – Start encrypting files

```
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

- Showed the outline of a basic Cryptolocker virus
  - Encrypts files in the background
  - Leaves ransom notes in folders with encrypted files
  - Can show pop-up screen with ransom note
  - Uses A-symmetrical encryption

Demo –
Find encrypted files and properties

```
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 robocopy to find files that match crypto naming
  - Backwards compatible
  - Faster file enumeration
  - Support for > 248 file paths
  - Can use seBackupPrivilege to ignore ACLs
- Filter the results with regular expressions
- Use this data to determine the scope of the damage

Demo –
Secure your file server using PowerShell

```
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

- How to use FSRM to setup filtering rules
- Setup scripts to run when a rule triggers
  - Configure the correct security permissions

What to expect in the future

- More threats that incorporate PowerShell
- Bigger role for cloud based security

Sponzoři konference