



Windows PowerShell  
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

# Using PowerShell to defeat malware

Jaap Brasser

```
User: j.brasser
Hostname: brasser
OS: Microsoft Windows 10 Enterprise
Kernel: NT 10.0.10240
Uptime: 0 days, 3 hours, 46 minutes
Shell: Powershell 5.0
CPU: Intel Core i5-4200M @ 2.50GHz
Processes: 102
Current Load: 4%
Memory: 4435mb/16297mb Used
Disk: 502gb/698gb Used
```

# About\_jaap



**@Jaap\_Brasser**

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

User: j.brasser

Hostname: brasser

OS: Microsoft Windows 10 Enterprise

Kernel: NT 10.0.10240

Uptime: 10 days, 3 hours, 46 minutes

Build: 1507

CPU: Intel Core i5-4200M @ 2.50GHz

Processes: 102

Current Load: 4%

Memory: 4435mb/16297mb Used

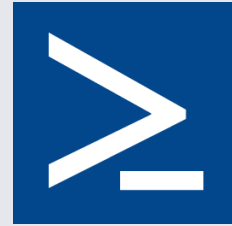
Disk: 502gb/698gb Used

# 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

```
Hostname: brasserie
Kernel: NT 10.0.10240
Shell: Powershell 5.0
CPU: Intel Core i5-4200M @ 2.50GHz
Processes: 102
Current Load: 4%
Memory: 4435mb/16297mb Used
Disk: 502gb/698gb Used
```

# 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

```
User: j.brasser
Hostname: brasser
OS: Microsoft Windows 10 Enterprise
Kernel: NT 10.0.10240
Uptime: 3 hours, 46 minutes
Shell: Powershell 5.0
CPU: Intel Core i5-4200M @ 2.50GHz
Processes: 102
Current Load: 4%
Memory: 4435mb/16297mb Used
Disk: 502gb/698gb Used
```

# What is PowerShell Security

**PowerShell Security is regular security**

11/29/2015 10:41:31 AM

User: j.brasser

OS: Microsoft Windows 10 Enterprise

Kernel: NT 10.0.10240

Uptime: 0 days, 3 hours, 46 minutes

Shell: Powershell 5.0

CPU: Intel Core i5-4200M @ 2.50GHz

Processes: 102

Current Load: 4%

Memory: 4435mb/16297mb Used

Disk: 502gb/698gb Used

# How to secure PowerShell

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

```
User: j.brasser
Hostname: brasser
OS: Microsoft Windows 10 Enterprise
Kernel: NT 10.0.10240
Uptime: 0 days, 3 hours, 46 minutes
Shell: Powershell 5.0
CPU: Intel Core i5-4200M @ 2.50GHz
Processes: 102
Current Load: 4%
Memory: 4435mb/16297mb Used
Disk: 502gb/698gb Used
```



# Tale of two users



```
E:::z33L @EEEtttt:::z3F
{3=*^`'4E3) ;EEEtttt:::tZ`
:EEEtttt:::z7
'VEzjt;;z>*
```



11/2

User  
Host  
OS:  
Kern  
Upti  
Shel  
CPU:  
Proc

Current Load: 4%  
Memory: 4435mb/16297mb Used  
Disk: 502gb/698gb Used

# 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], UnauthorizedAccessException
+ 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], UnauthorizedAccessException
+ 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], UnauthorizedAccessException
+ FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```





# Demo Summary

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

```
tt::tt333FE3
E:::tt333FE3
;tt::tt333FE7 ;EEEEttttt33#
;Et::tt333FE7 ;EEEEttttt33#
it:::tt333EEF @EEEEttttt33F
;3=*A` `` `*4EEV ;EEEEttttt33@.
,,::::it=., @EEEEttttz33QF
;:::zt33) `4EEttttji3P*
;t:::tt33.:Z3z.. `` ,..g.
i:::zt33F AEEtttt:::ztF
;:::t33V ;EEttttt:::t3
E:::zt33L @EEtttt:::z3F
{3=*A` `` `*4E3) ;EEtttt:::tZ`
:EEEEtttt:::z7
`VEzjt; ;z>*`
```

2015/2015 10:41:31 AM

```
User: j.brasser
Hostname: brasser
OS: Microsoft Windows 10 Enterprise
Kernel: NT 10.0.10240
Uptime: 0 days, 3 hours, 46 minutes
Shell: Powershell 5.0
CPU: Intel Core i5-4200M @ 2.50GHz
Processes: 102
Current Load: 4%
Memory: 4435mb/16297mb Used
Disk: 502gb/698gb Used
```

# 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

```

;tt::tt33EE3
;tt::tt33EE7 ;EEEEttttt33#
;Et::tt33EEF @EEEEttttt33F
;it::tt33EEF @EEEEttttt33F
;3=*A` ``' *4E3) ;EEtttt:::tZ`
      :EEEEtttt:::z7
      'VEzjt;;z>*`

```

```

10:41:31 AM
User: j.brasser
Hostname: brasser
OS: Microsoft Windows [Version 6.0.6002] Copyright (c) 2009 Microsoft Corporation. All rights reserved.
Kernel: NT 10.0.10240
Uptime: 0 days, 3 hours, 46 minutes
Shell: Powershell 5.0
CPU: Intel Core i5-4200M @ 2.50GHz
Processes: 102
Current Load: 4%
Memory: 4435mb/16297mb Used
Disk: 502gb/698gb Used

```



Windows PowerShell

Windows PowerShell

Copyright (c) Microsoft Corporation. All rights reserved.

# Ransomware



enterprise

minutes

50GHz

'VEzjt;;z>\*

# Lab environment



Windows 10



Server 2016

11/29/2015

User: j.br  
Hostname:  
OS: Micros  
Kernel: NT  
Uptime: 0  
Shell: Pow  
CPU: Intel  
Processes: 102  
Current Load: 4%  
Memory: 443mb/1024mb  
Disk: 502gb/698gb Used

Enterprise  
5 minutes  
2.50GHz

# 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], UnauthorizedAccessException
+ 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], UnauthorizedAccessException
+ 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], UnauthorizedAccessException
+ 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], UnauthorizedAccessExcep
tion
+ 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], UnauthorizedAccessExcep
tion
+ 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
ption
+ 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

11/29/2015 10:41:31 AM

User: j.brasser

Hostname: brasser

OS: Microsoft Windows 10 Enterprise

Kernel: NT 10.0.10240

Uptime: 6 days, 5 hours, 46 minutes

Shell: PowerShell 5.0

CPU: Intel Core i5-4200M @ 2.50GHz

Processes: 102

Memory: 4435mb/16297mb Used

Disk: 502gb/698gb Used



# 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], UnauthorizedAccessExcep
tion
+ 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], UnauthorizedAccessExcep
tion
+ 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
ption
+ 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

```

;tt::tt33EE?
Et::z333F
;tt::tt33EE7 FEEFttttt33#
;Et::z333F @EEEEEt33F
it::tt33EEF @EEEEEt33F
;3=*A` ` '*4EEV :EEEEEt33@.
,,:it=., @EEEEEt33QF
;:::zt33) '4EEtttji3P*
;t:::tt33.:Z3z.. ,.g.
i:::zt33F AEEtttt:::ztF
;:::t33V ;EEttttt:::t3
E:::zt33L @EEtttt:::z3F
{3=*A` ` '*4E3) ;EEtttt:::tZ`
:EEEEtttt:::z7
'VEzjt;;z>*\

```

Hostname: brasser  
 OS: Microsoft Windows 10 Enterprise  
 Kernel: NT 10.0.10240  
 Uptime: 0 days, 3 hours, 46 minutes  
 Shell: Powershell 5.0  
 CPU: Intel Core i5-4200M @ 2.50GHz  
 Processes: 102  
 Current Load: 4%  
 Memory: 4435mb/16297mb Used  
 Disk: 502gb/698gb Used

# What to expect in the future

- More threats that incorporate PowerShell

- Bigger role for cloud based security

```

;tt:::tt33EE3
;tt:::tt33EE7 ;EEEEEttttt33#
;Et:::zt33EEQ. SEEEEEttttt33QL
it:::tt33EEF @EEEEEttttt33F
;3=*A`""*4EEV :EEEEEttttt33@.
,,::::it=., @EEEEEtttt33QF
;:::zt33) '4EEEttti3P*
;t:::tt33.:Z3z.. ,..g.
i:::zt33F AEEEtttt:::ztF
;:::t33V ;EEEtttt:::t3
E:::zt33L @EEEtttt:::z3F
{3=*A`""*4E3) ;EEEtttt:::tZ`
:EEEEtttt:::z7
'VEzjt;.;z>*\
    
```

```

User: j.brasser
Hostname: brasser
OS: Microsoft Windows 10 Enterprise
Kernel: NT 10.0.10240
Uptime: 0 days, 3 hours, 46 minutes
Shell: Powershell 5.0
CPU: Intel Core i5-4200M @ 2.50GHz
Processes: 102
Current Load: 4%
Memory: 4435mb/16297mb Used
Disk: 502gb/698gb Used
    
```

# Sponzoři konference



MATEMATICKO-FYZIKÁLNÍ  
FAKULTA  
Univerzita Karlova

