



Windows PowerShell

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

PowerShell Security and Threat management

Jaap Brasser

11/29/2015 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

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



@Jaap_Brasser

Jaap Brasser

Blogger

- JaapBrasser.com
- [PowerShell Magazine](#)

Speaker

- [PowerShell Conference](#)
- [Dutch PowerShell User Group](#)

11/29/2015 10:41:31 AM

ttttt333
tttt33Q
tttt33F
ttt33@.
tz33QF
ji3P*

Jaap Brasser

Hostname: brasser

10 Enterprise

Kernel: NT 10.0.10240

Uptime: 0 days, 3 hours, 46 minutes

CPU: Intel Core i5-4200M @ 2.50GHz

Memory: 4435mb/16297mb Used

Disk: 502gb/698gb Used

System Load: 4%



Windows PowerShell
Copyright (c) Microsoft Corporation. All rights reserved.

Agenda

- Windows Defender
- Deep script logging and transcripts
- Current security landscape
- PowerShell as a threat

11/29/2015 10:41:31 AM

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

Windows Defender

- Eleven cmdlets

- Used for direct interaction with engine

- Can be used to identify threats

11/29/2015 10:41:31 AM

Hostname: brasser

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



Windows PowerShell

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

Demo

Remove threat using PowerShell

11/29/2015 10:41:31 AM

Host: i386
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



Remove threat demo

- Windows Defender to identify the threat

- Looked up information about the threat

- Removed the threat

- Checked in explorer what the results were

```
Hostname: brasser
OS: Microsoft Windows 10 Enterprise
Kernel: NT 10.0.10240
Uptime: 2 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
```



Transcription in PowerShell

- Available in PowerShell since 1.0
- Provide logging for console commands
- Useful when experimenting with PowerShell

```
..=:A!A!t3Z3z.,
;tt:::tt333FE3
Et: 2015 10:41:31 AM
;tt:::tt333FE7 ;FFFFFFttttt33#
Et:
it:::tt333FEF @EEEEEttttt33F Hostname: brasser
;3=*A vs 10 Enterprise
..=::::it=., @EEEEEttt233QF Kernel: NT 10.0.10240
;:::zt33) '4EEEtttji3P* Uptime: 0 days, 3 hours, 46 minutes
;t:::tt33.:Z3z.. ,...g. Shell: Powershell 5.0
i:::zt33F AEEEtttt:::ztF CPU: Intel Core i5-4200M @ 2.50GHz
;:::t33V ;EEEttttt:::t3 Processes: 102
E:::zt33L @EEEtttt:::z3F Current Load: 4%
{3=*A` `` '*4E3) ;EEEtttt:::tZ` Memory: 4435mb/16297mb Used
:EEEEtttt:::z7 Disk: 502gb/698gb Used
'VEzjt;;z>*
```



Security by transcription

- Have a record of recent PowerShell activity

- Troubleshooting

- Investigating malicious actions

- Auditing

- Start-Transcript

- Module-Logging

```
User: j.brasser
Hostname: brasser
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
```


Over-the-shoulder Transcription

- New in PowerShell 5.0
- Allow for system wide transcription
- Captures all streams into a log file
- Can be stored on another system

11/29/2015 10:41:31 AM

Hostname: brasser

Microsoft Windows 10 Enterprise

Kernel: NT 10.0.10240

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

Demo PowerShell Transcription

11/29/2015 10:41:31 AM

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



Deep script logging

- New in PowerShell 5.0
- Addition to transcription
- Uses the event log to display what actions occur in script block
- Can break script blocks into multiple parts

11/29/2015 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

Processor: Intel(R) Core(TM) i7-4200M @ 2.50GHz

Processes: 102

Current Load: 4%

Memory: 4435mb/16297mb Used

Disk: 502gb/698gb Used



Windows PowerShell

Windows PowerShell

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

Demo

Deep script logging

11/29/2015 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

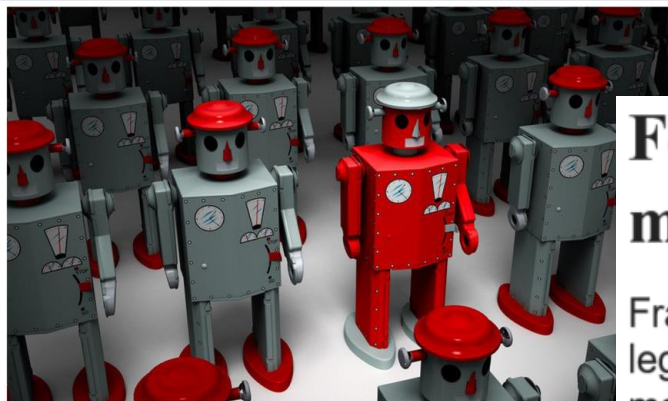
Processes: 102

Current Load: 4%

Memory: 4435mb/16297mb Used

Disk: 502gb/698gb Used

Current security landscape



Watch Out for CoreBot

For discerning hackers, malware is so last year

Fraudsters increasingly rely on legitimate administrator tools instead of malware to successfully breach systems and steal data

Turkish security bod puts Ransomware on GitHub

The 'Hidden Tear' ransomware, available at [GitHub](#)

97mb Used
Used



PowerShell threats

- File-less threats
- Stored in registry, eventlog or task scheduler

```

..=:A!A!t3Z3z.,
:tt:::tt333EEF
Et: 11/29/2015 10:41:31 AM
;tt:::tt333EEF7 :FFFFFFttttt33#
Et:
it:::tt333EEF @EEEEEttttt33F
;3=*A` `` `*4EEV :EEEEEttttt33@.
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
..=::::it=., @EEEEEtttt33QF
;:::z33) `4EEEtttji3P*
:t:::tt33.:Z3z.. `` ,..g.
i:::z33F AEEEtttt:::ztF
;:::t33V ;EEEtttt:::t3
E:::zt33L @EEEtttt:::z3F
{3=*A` `` `*4E3) ;EEEtttt:::tZ`
:EEEEtttt:::z7
`VEzjt; ;z>*`

```



Windows PowerShell

Windows PowerShell

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

Demo

Detect threats using PowerShell

11/29/2015 10:41:31 AM

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



Detect File-less threats

- Store PowerShell code in the registry
- Setup a Runkey in the registry to execute code
- Manipulate an existing Scheduled Task to execute code

10:41:31 AM

Hostname: brasser

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



More information

Demo code will be available on GitHub:

<https://github.com/jaapbrasser/Events/tree/master/MSFestPraha2015>

Additional information available:

<http://www.jaapbrasser.com/tag/msfest/>

http://www.twitter.com/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
Dedicated memory: 102
Used memory: 4%
Memory: 4435mb/16297mb Used
Disk: 502gb/698gb Used
```

Sponzoři konference

