PowerShell Security and Threat management

Jaap Brasser

@Jaap_Brasser

Jaap Brasser

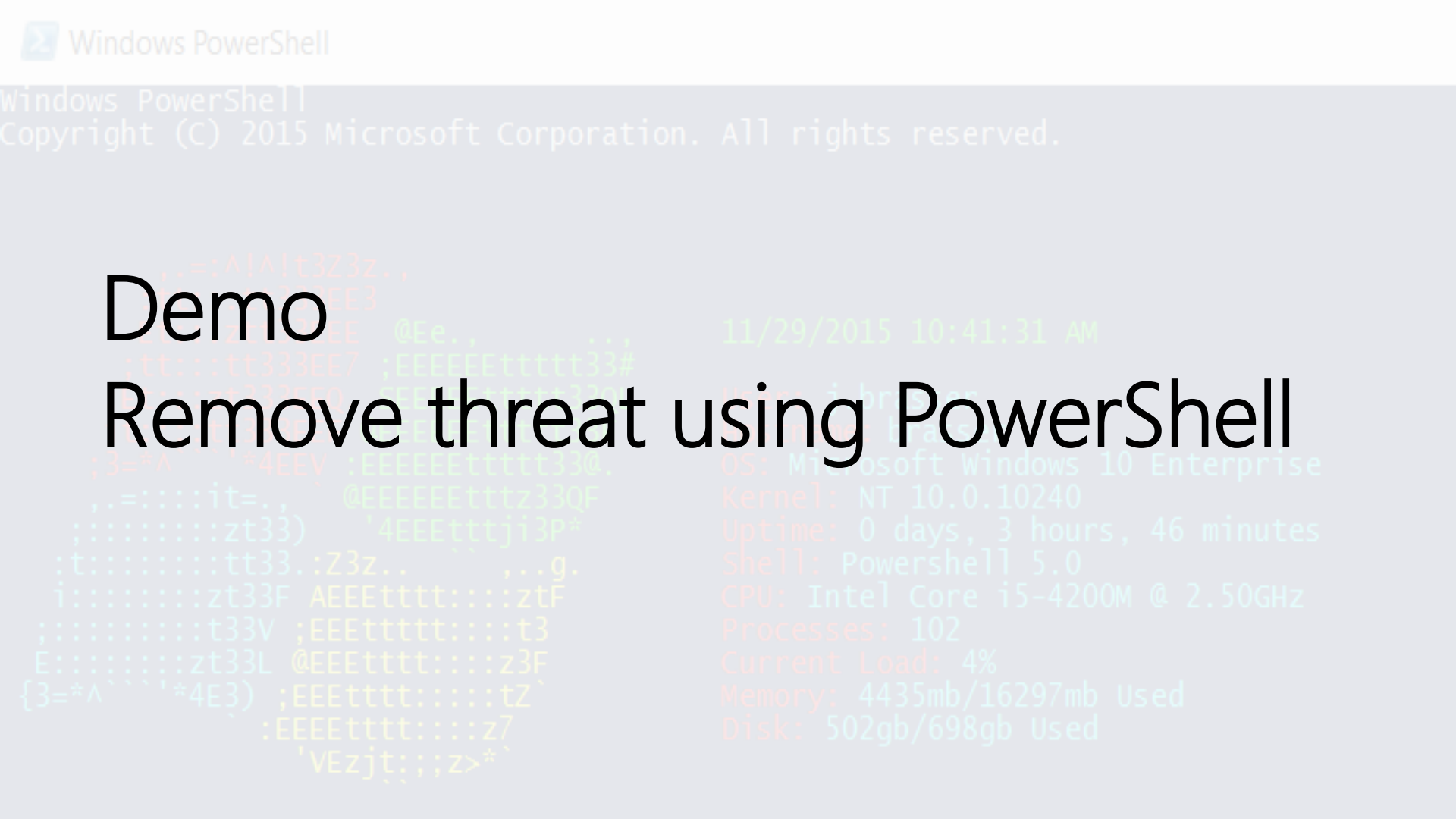
- Blogger
  - JaapBrasser.com
  - PowerShell Magazine
- Speaker
  - PowerShell Conference
  - Dutch PowerShell User Group

Agenda

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

Windows Defender

- Eleven cmdlets
- Used for direct interaction with engine
- Can be used to identify threats



Demo
Remove threat using PowerShell

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

Transcription in PowerShell

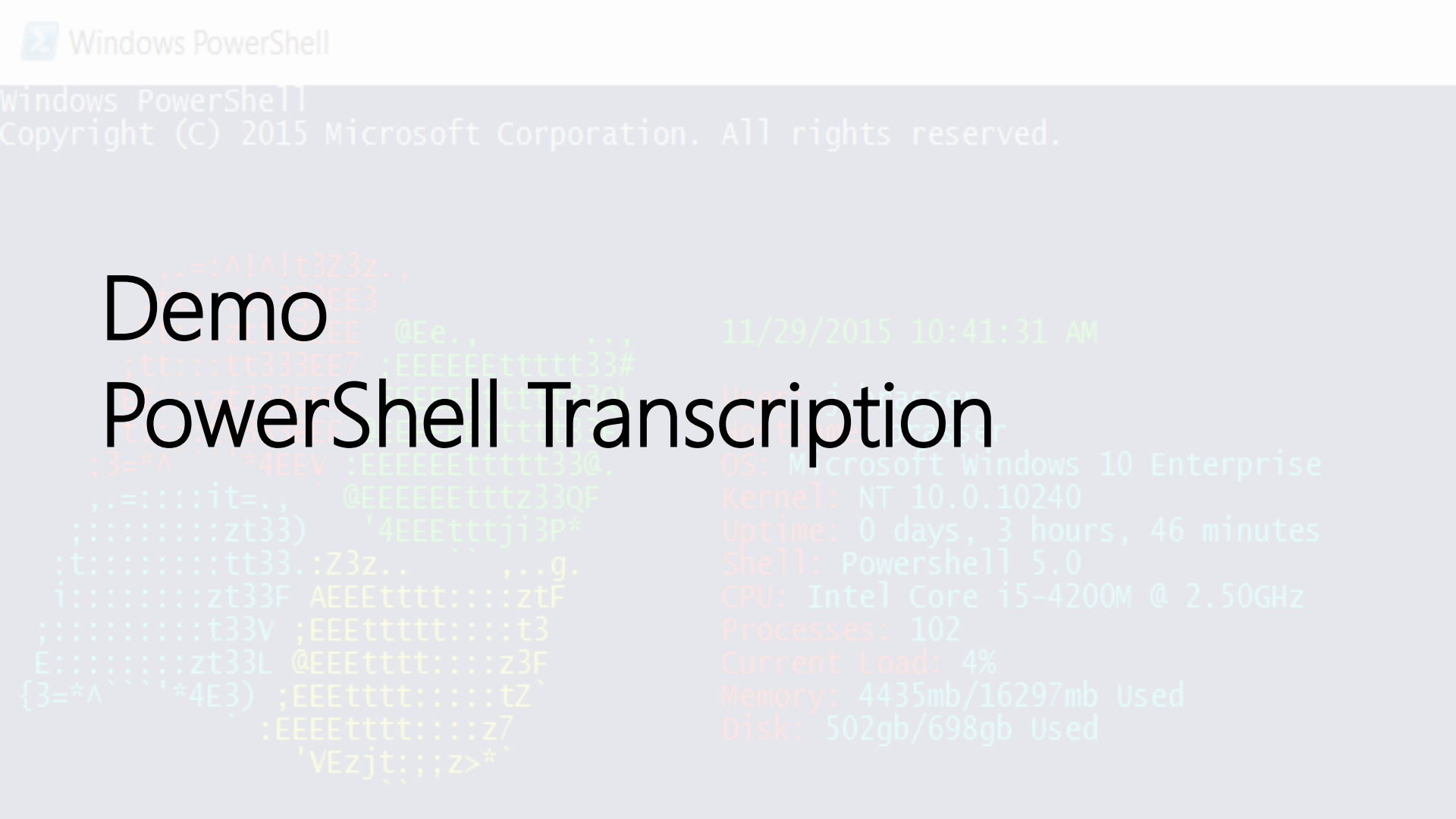
- Available in PowerShell since 1.0
- Provide logging for console commands
- Useful when experimenting with PowerShell

Security by transcription

- Have a record of recent PowerShell activity
- Troubleshooting
- Investigating malicious actions
- Auditing
- Start-Transcript
- Module-Logging

Over-the-shoulder Transcription

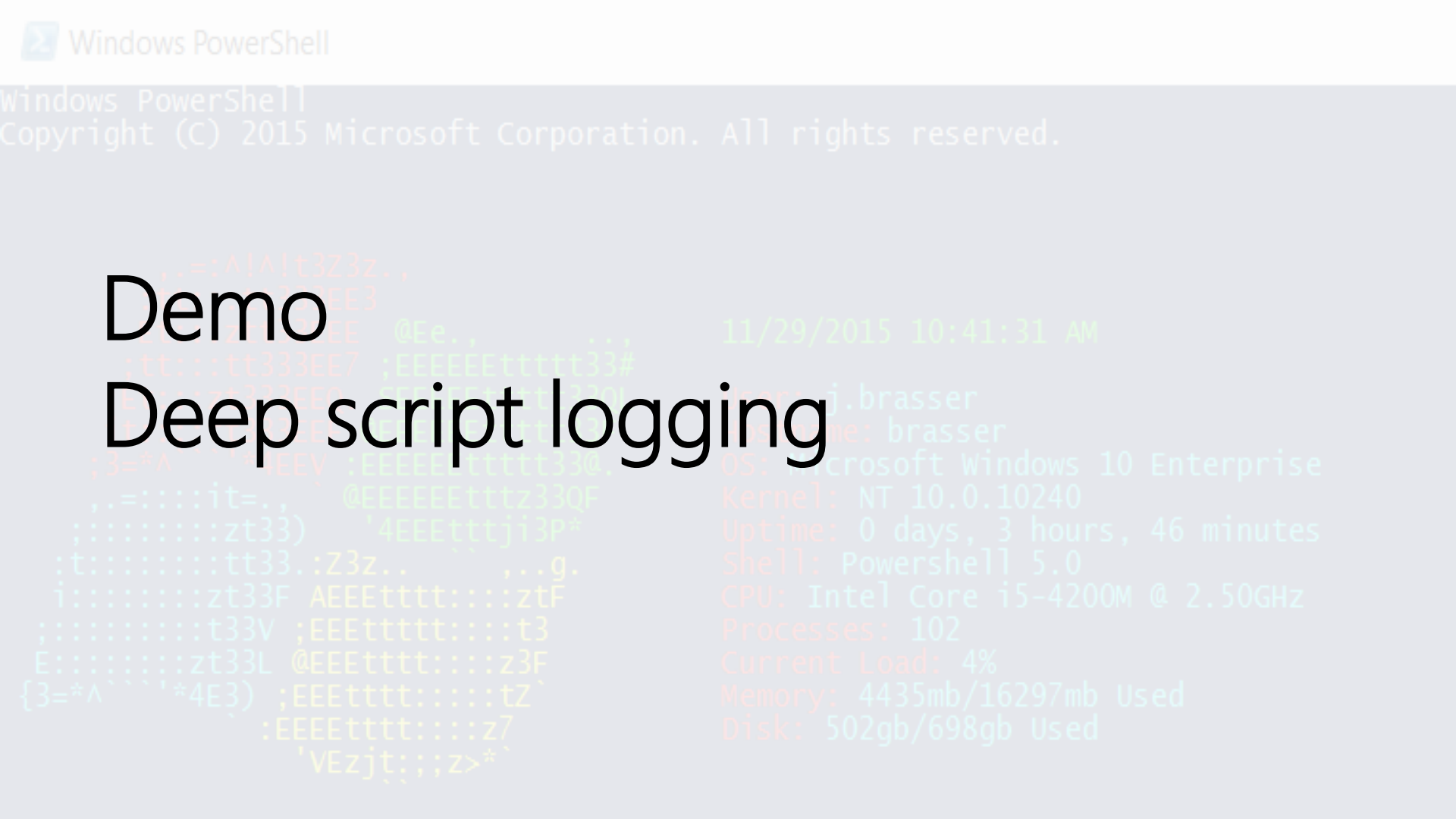
- New in PowerShell 5.0
- Allow for system wide transcription
- Captures all streams into a log file
- Can be stored on another system



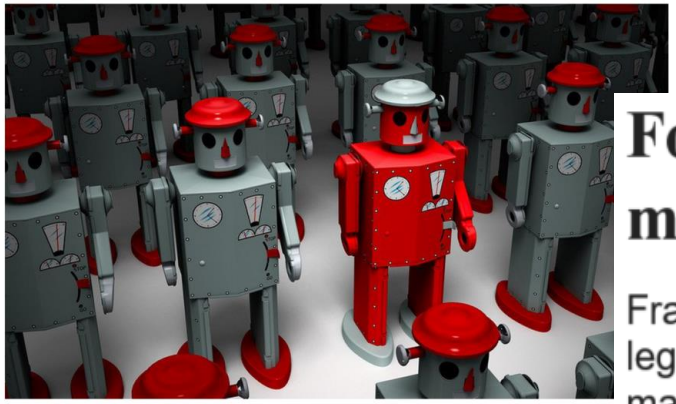
Demo
PowerShell Transcription

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


Windows PowerShell
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.
11/29/2015 10:41:31 AM
brasser
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
Demo
Deep script logging

Current security landscape



Watch Out for CoreBot

For discerning hackers, malware is so last year

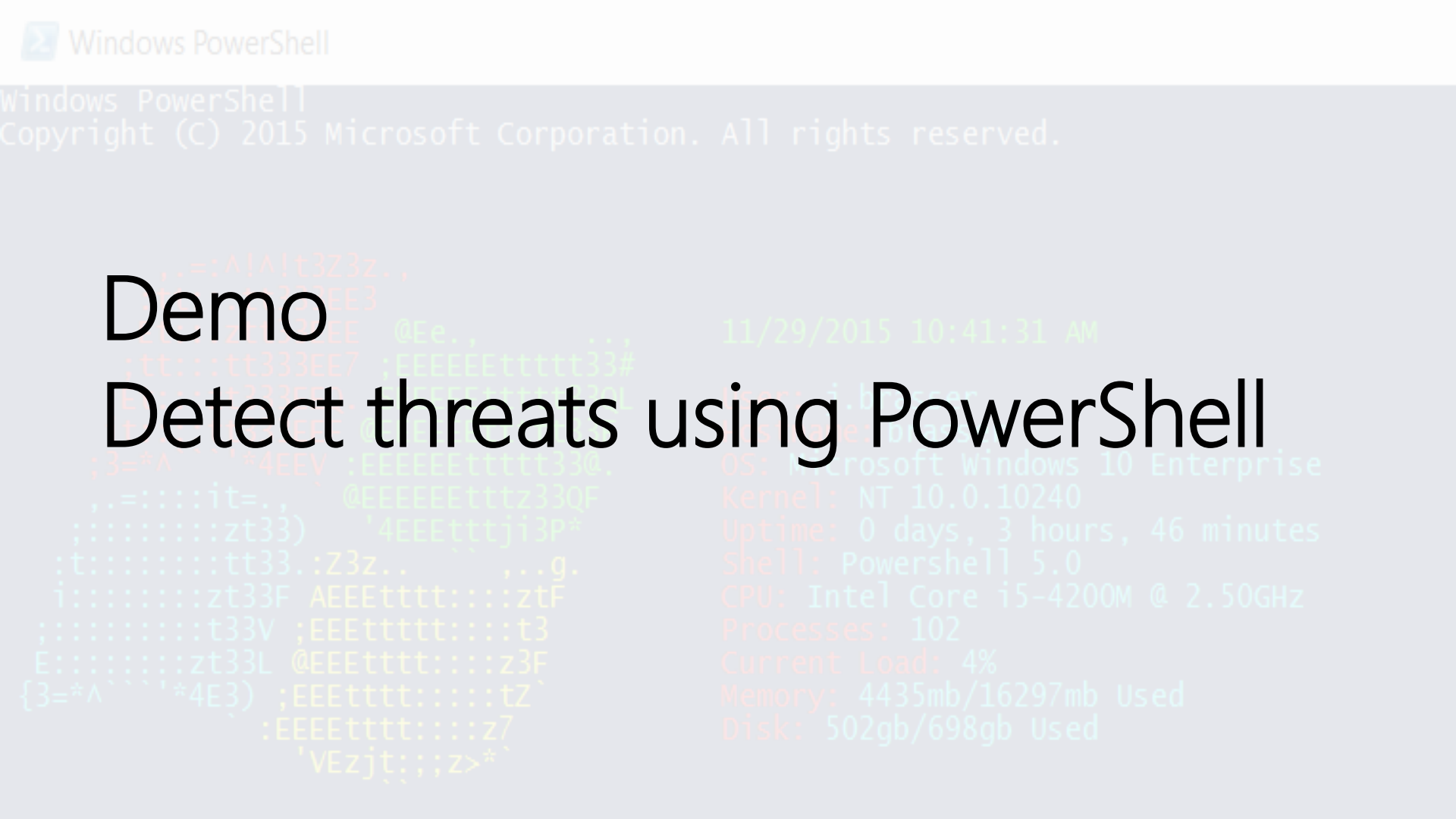
Fraudsters increasingly rely on legitimate administrator tools instead of malware to successfully breach systems

Turkish security bod puts Ransomware on GitHub

The 'Hidden Tear' ransomware, available at GitHub

PowerShell threats

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



Demo
Detect threats using PowerShell

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

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

Sponzoři konference