PowerShell 2020

State of the Art / Hack / Infection

Jason Fossen

Securing Windows and PowerShell Automation (SANS Course SEC505)

https://sans.org/SEC505

Welcome
to
SANS London

7 September 2020

@JasonFossen

Author: Course SEC505

https://BlueTeamPowerShell.com

- What is PowerShell?

PowerShell
is not a
command shell

System.Management.Automation.dll

.NET

Full .NET on Windows

vs.

.NET Core

Windows PowerShell

vs.

PowerShell Core

Host Processes

powershell.exe

powershell_ise.exe

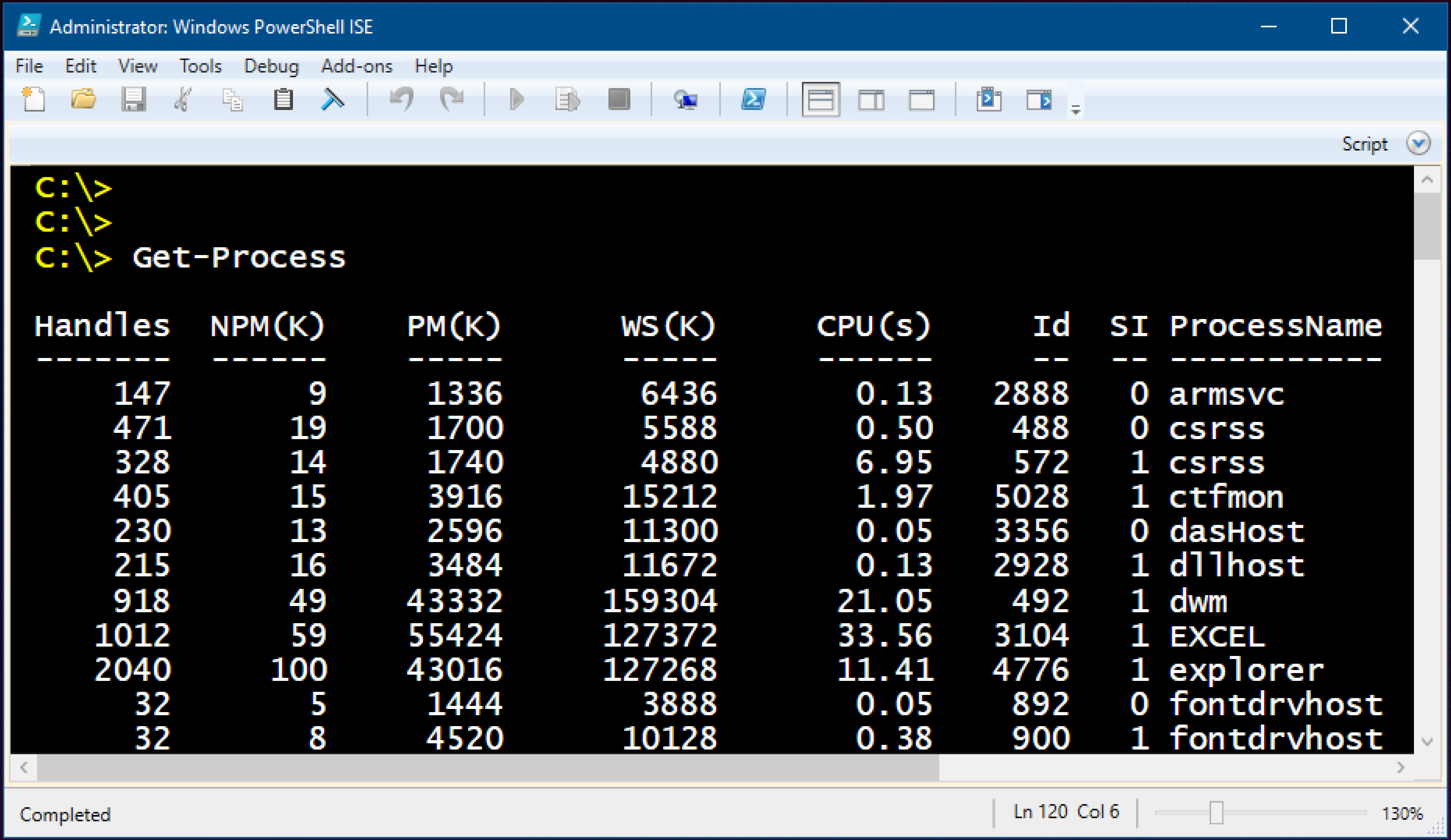
pwsh.exe

So what?

Piping Objects

(not text)

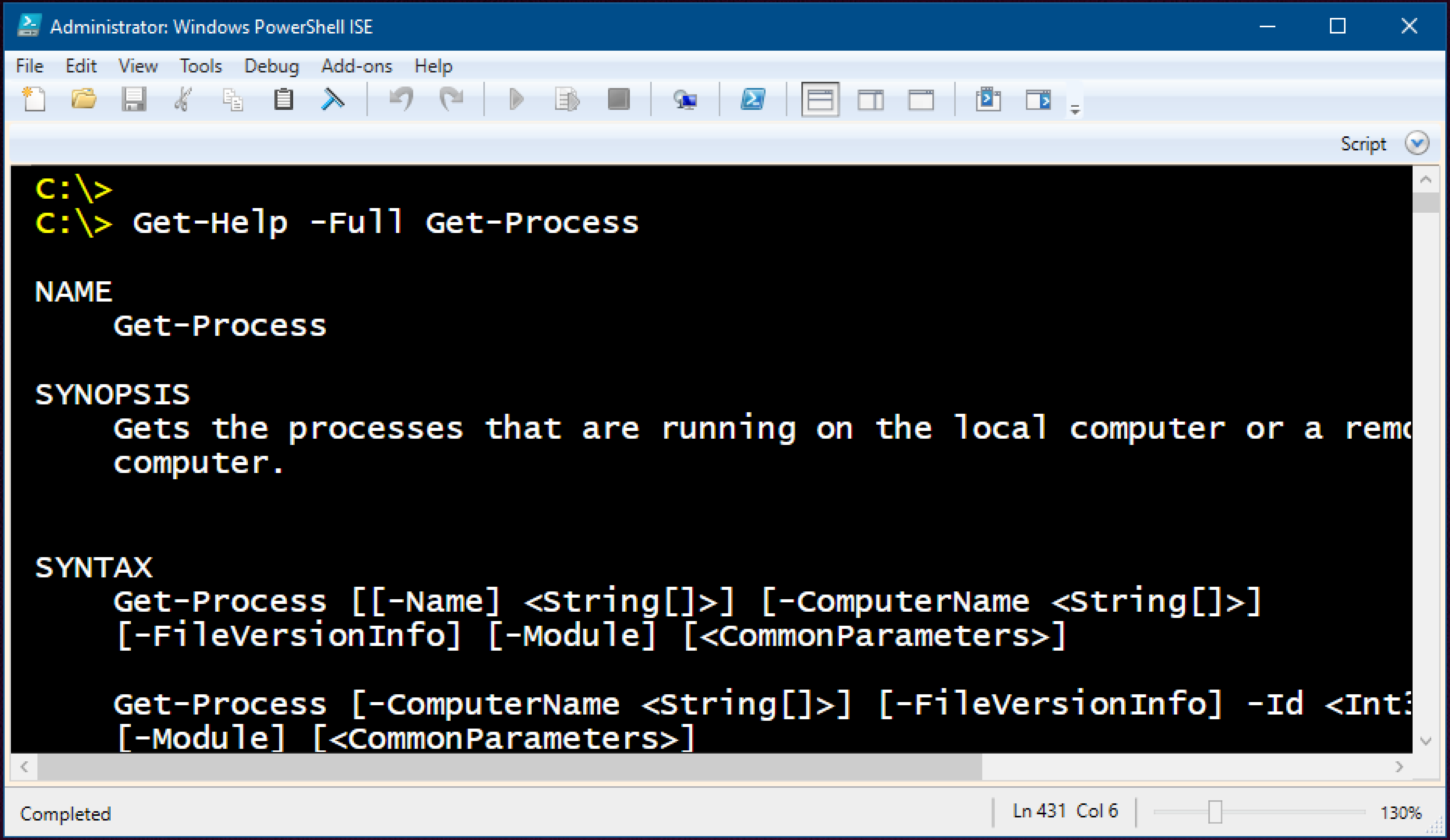
Get-Process



Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script

```
C:\>
C:\>
C:\> Get-Process

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    147       9     1336       6436       0.13   2888   0 armsvc
    471      19     1700       5588       0.50    488   0 csrss
    328      14     1740       4880       6.95    572   1 csrss
    405      15     3916      15212       1.97   5028   1 ctfmon
    230      13     2596      11300       0.05   3356   0 dasHost
    215      16     3484      11672       0.13   2928   1 dllhost
    918      49    43332     159304      21.05    492   1 dwm
   1012      59    55424     127372      33.56   3104   1 EXCEL
   2040     100    43016     127268      11.41   4776   1 explorer
     32       5     1444       3888       0.05    892   0 fontdrvhost
     32       8     4520      10128       0.38    900   1 fontdrvhost
```

```
Get-Help -Full Get-Process
```

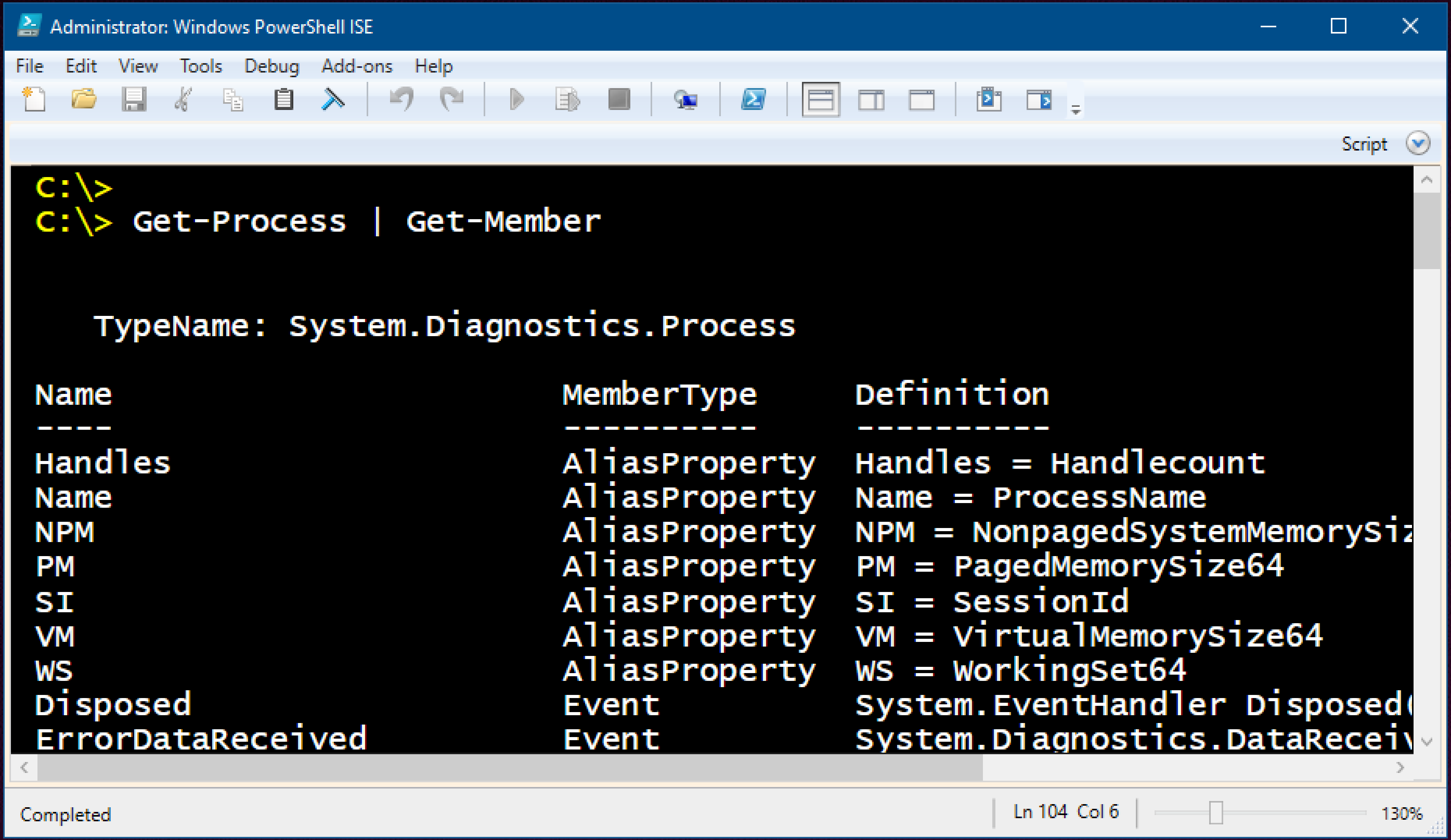


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script

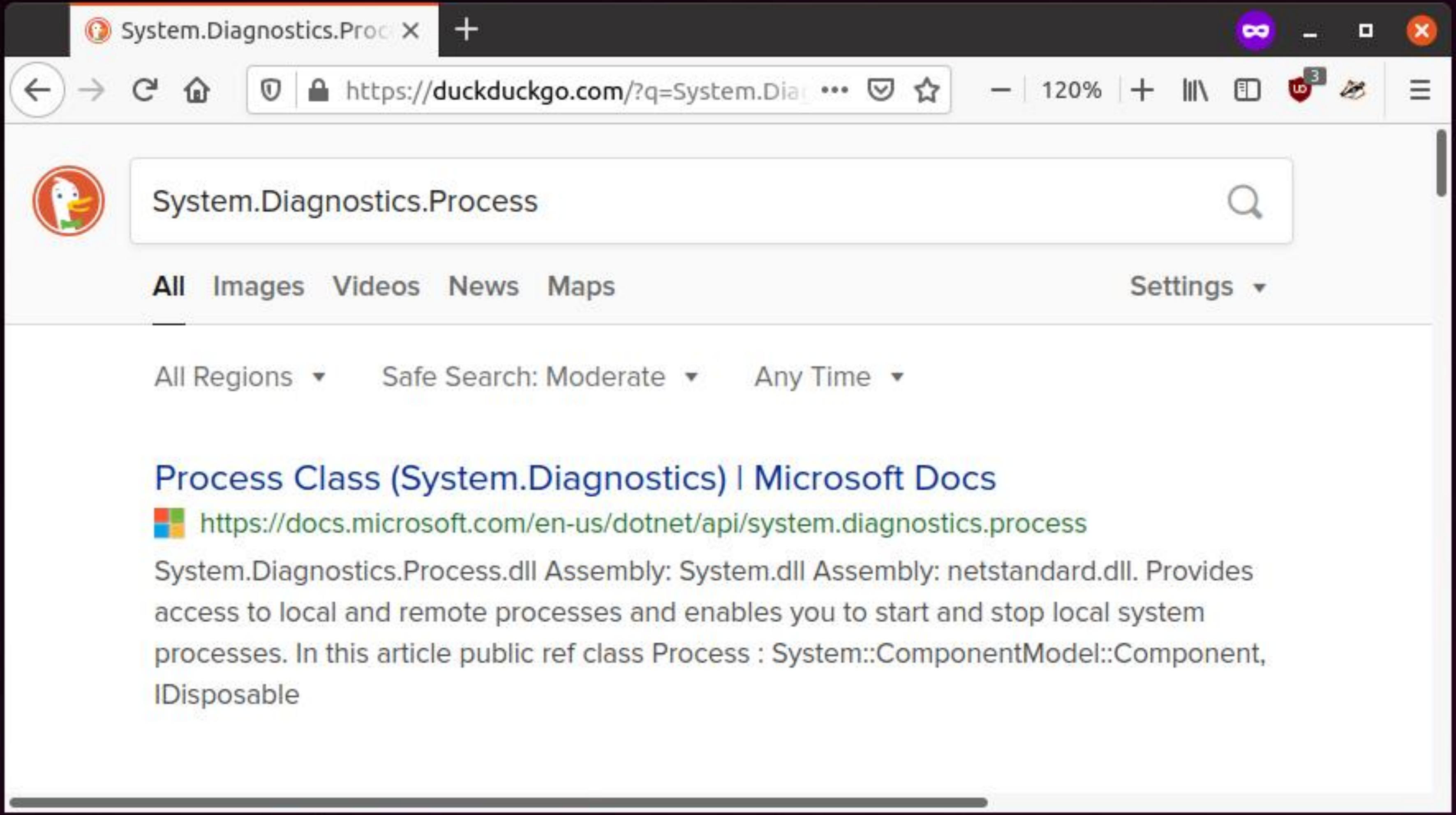
```
C:\>
C:\> Get-Help -Full Get-Process

NAME
    Get-Process

SYNOPSIS
    Gets the processes that are running on the local computer or a remo
    computer.


SYNTAX
    Get-Process [[-Name] <String[]>] [-ComputerName <String[]>]
    [-FileVersionInfo] [-Module] [<CommonParameters>]

    Get-Process [-ComputerName <String[]>] [-FileVersionInfo] -Id <Int
    [-Module] [<CommonParameters>]
```

Completed
Ln 431 Col 6
130%

Get-Process | Get-Member


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script
Completed
Ln 104 Col 6
130%

```
C:\>
C:\> Get-Process | Get-Member


   TypeName: System.Diagnostics.Process

Name                           MemberType     Definition
----                           ----------     ----------
Handles                        AliasProperty  Handles = Handlecount
Name                           AliasProperty  Name = ProcessName
NPM                            AliasProperty  NPM = NonpagedSystemMemorySiz
PM                             AliasProperty  PM = PagedMemorySize64
SI                             AliasProperty  SI = SessionId
VM                             AliasProperty  VM = VirtualMemorySize64
WS                             AliasProperty  WS = WorkingSet64
Disposed                       Event          System.EventHandler Disposed(
ErrorDataReceived              Event          System.Diagnostics.DataRecei
```



System.Diagnostics.Process

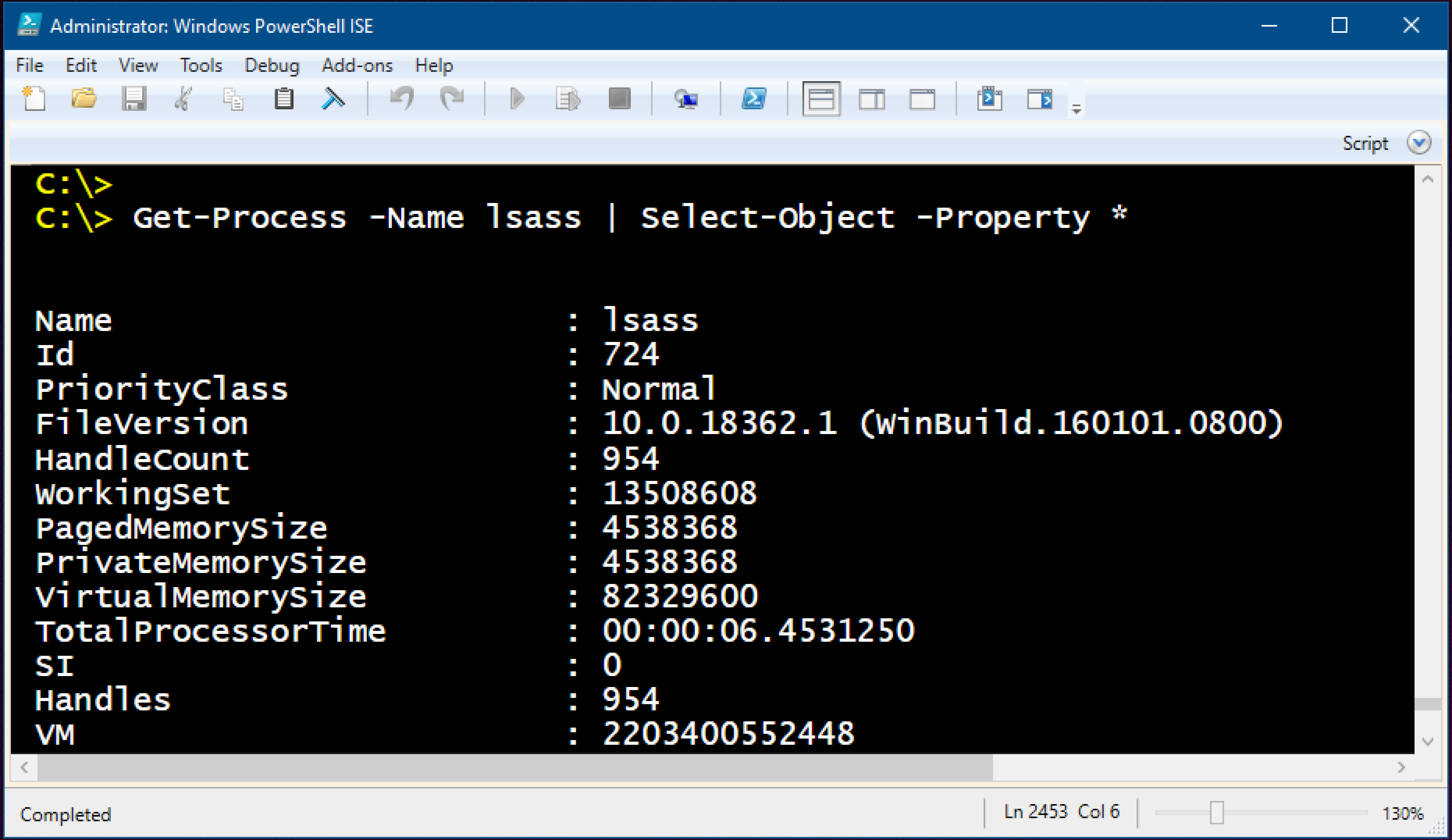
All Regions ▾ Safe Search: Moderate ▾ Any Time ▾

Process Class (System.Diagnostics) | Microsoft Docs

https://docs.microsoft.com/en-us/dotnet/api/system.diagnostics.process

System.Diagnostics.Process.dll Assembly: System.dll Assembly: netstandard.dll. Provides access to local and remote processes and enables you to start and stop local system processes. In this article public ref class Process : System::ComponentModel::Component, IDisposable

```
Get-Process |
Select-Object -Property *
```



Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script

```
C:\>
C:\> Get-Process -Name lsass | Select-Object -Property *


Name                        : lsass
Id                          : 724
PriorityClass               : Normal
FileVersion                 : 10.0.18362.1 (WinBuild.160101.0800)
HandleCount                 : 954
WorkingSet                  : 13508608
PagedMemorySize             : 4538368
PrivateMemorySize           : 4538368
VirtualMemorySize           : 82329600
TotalProcessorTime          : 00:00:06.4531250
SI                          : 0
Handles                     : 954
VM                          : 2203400552448
```

Completed
Ln 2453 Col 6
130%

```
Get-Help -Full <CmdLet>

<CmdLet> | Get-Member

<CmdLet> | Select-Object
```

- PowerShell Security

Why do ~~hackers~~ threat actors love PowerShell?

PowerShell is a
built-in and coder-friendly
wrapper for the entire OS

.NET Class Library

COM Objects

WMI Service

Windows API

Native Binary Tools

WSMan

RPC

SMB

HTTPS

SSH

Raw TCP/UDP

“PowerShell Attacks”

Post-Exploitation

vs.

Initial Compromise

CISO:

“How do I secure PowerShell?"

Separately from the OS?

You can't, not separately

Focus on
host and network
hardening

Upgrade to Windows 10

Quickly apply updates

Limit administrators

Use multi-factor authentication

Host-based firewalls

IPsec for zero trust

Antimalware Scan Interface (AMSI)

Application Control

PowerShell Constrained Language Mode

CISO:

"Why not just block PowerShell completely?"

CISO:

"Why not just run PowerShell in a sealed sandbox?"

PowerShell logging is great!

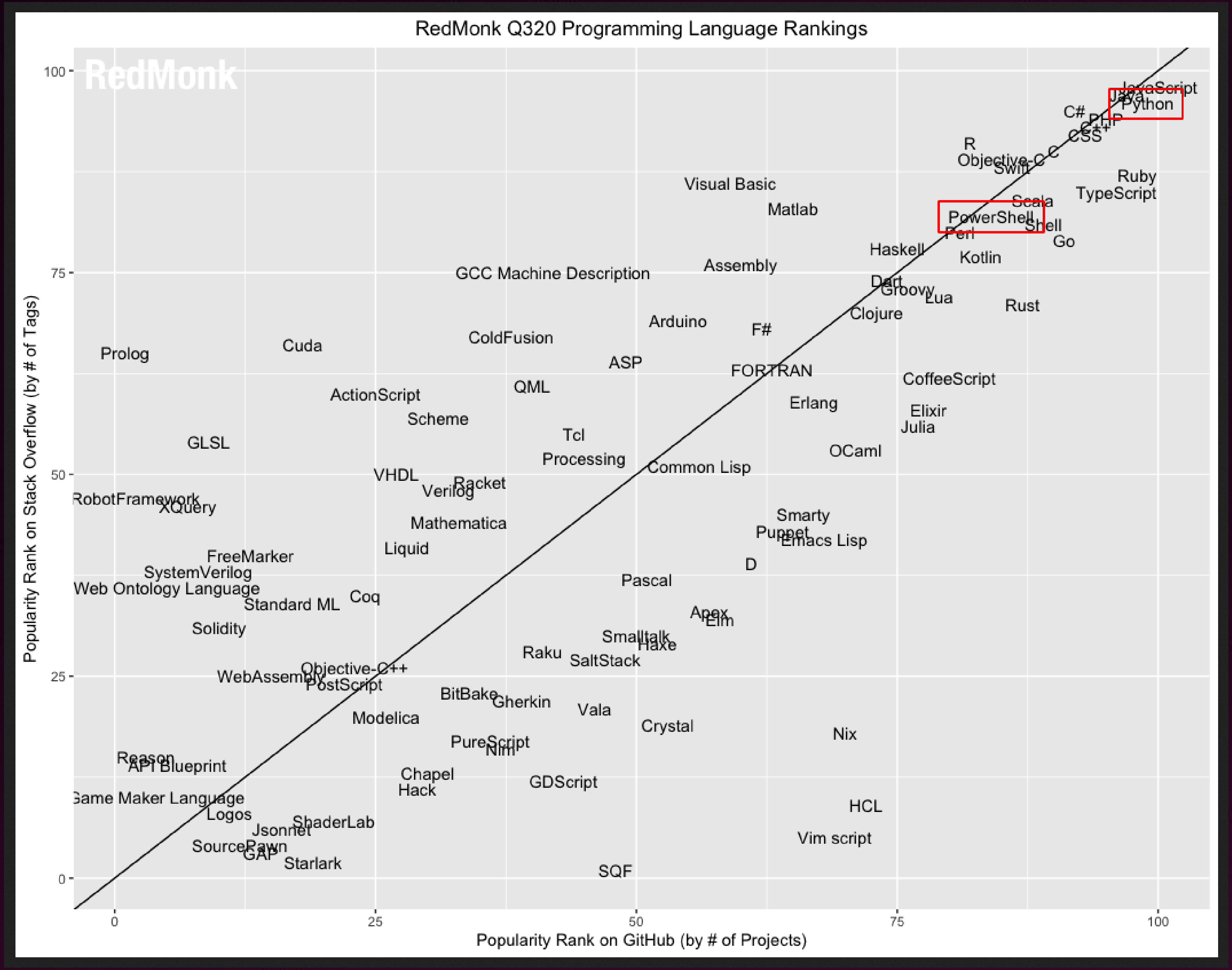
- The Future

Why PowerShell Core?

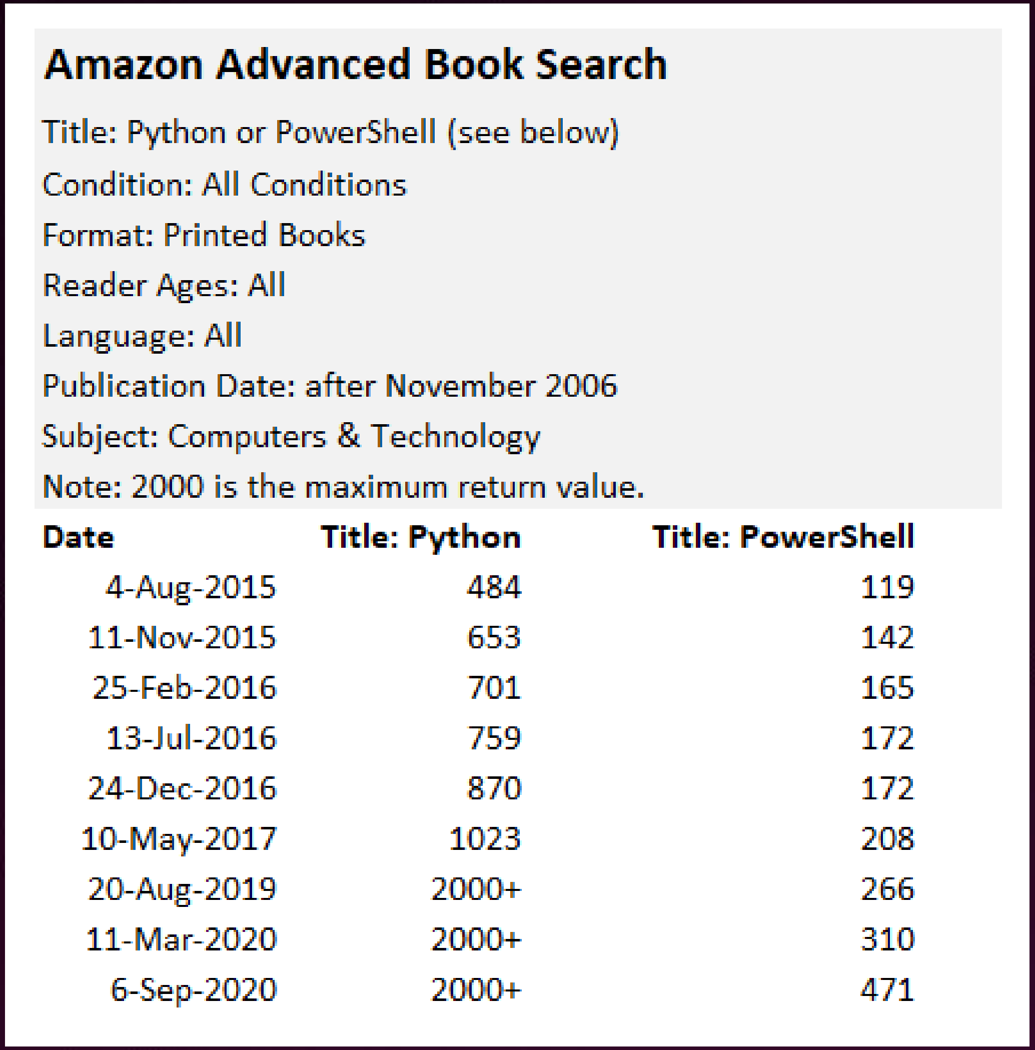
Over half the virtual machines in Azure run Linux

Most IoT devices run Linux

Many developers use macOS



https://redmonk.com/sogrady/2020/07/27/language-rankings-6-20/



Amazon Advanced Book Search

Title: Python or PowerShell (see below)

Condition: All Conditions

Format: Printed Books

Reader Ages: All

Language: All

Publication Date: after November 2006

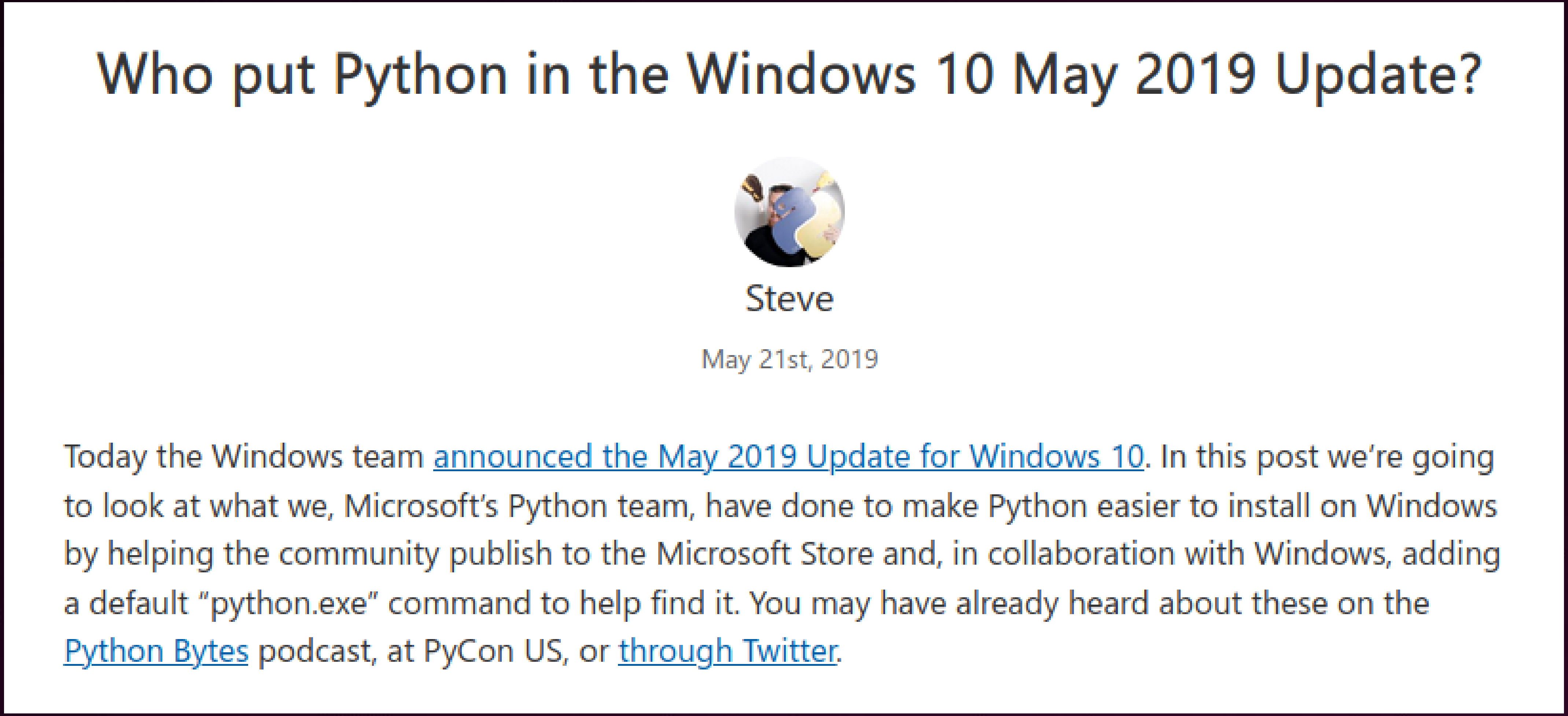
Subject: Computers & Technology

Note: 2000 is the maximum return value.

Date	Title: Python	Title: PowerShell
4-Aug-2015	484	119
11-Nov-2015	653	142
25-Feb-2016	701	165
13-Jul-2016	759	172
24-Dec-2016	870	172
10-May-2017	1023	208
20-Aug-2019	2000+	266
11-Mar-2020	2000+	310
6-Sep-2020	2000+	471

Python

- ☑ Coder-Friendly
- ☑ Cross-Platform
- ☑ Object-Oriented
- □ Built-In ?



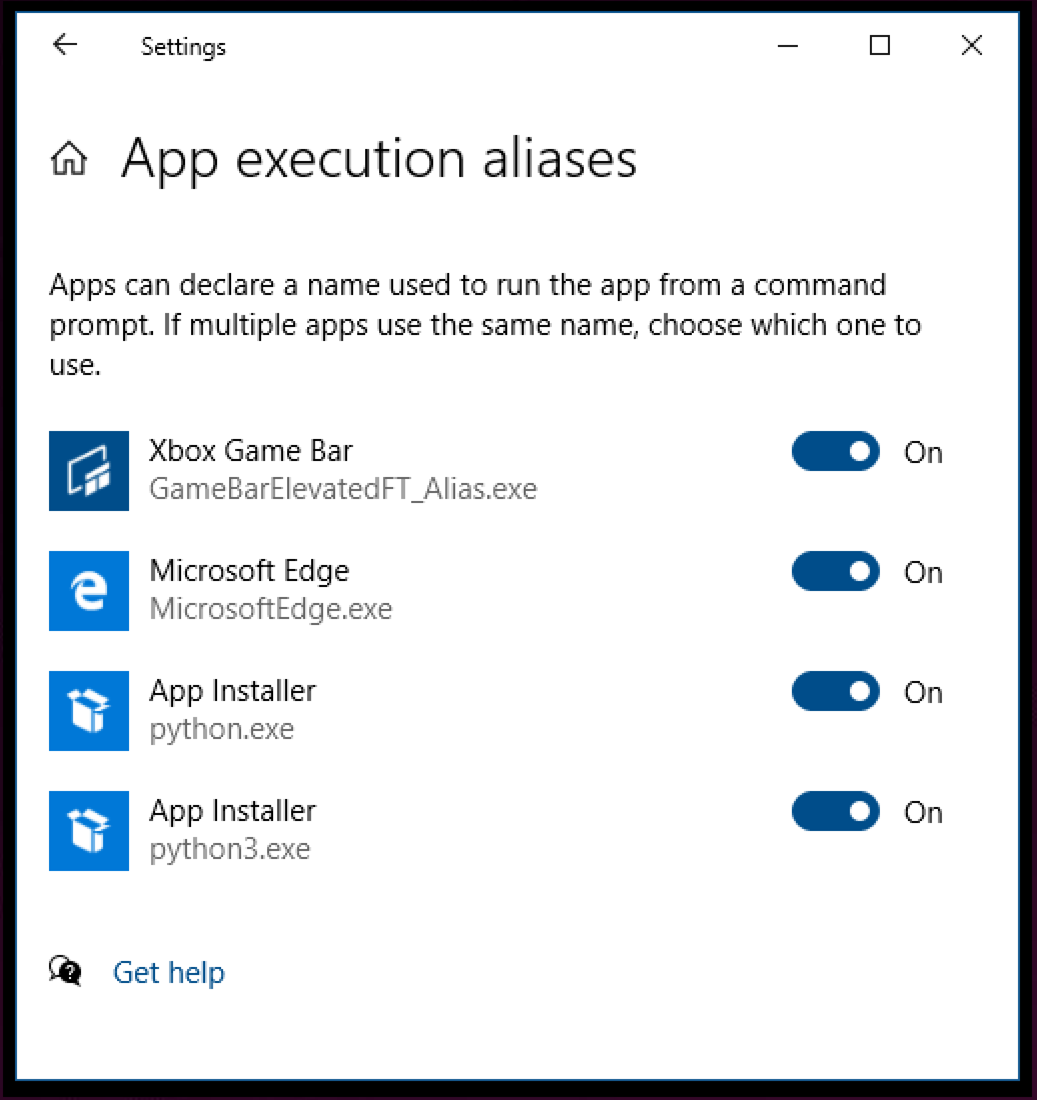
Who put Python in the Windows 10 May 2019 Update?

Steve

May 21st, 2019

Today the Windows team announced the May 2019 Update for Windows 10. In this post we're going to look at what we, Microsoft's Python team, have done to make Python easier to install on Windows by helping the community publish to the Microsoft Store and, in collaboration with Windows, adding a default "python.exe" command to help find it. You may have already heard about these on the Python Bytes podcast, at PyCon US, or through Twitter.

https://devblogs.microsoft.com/python/python-in-the-windows-10-may-2019-update/



App execution aliases

Apps can declare a name used to run the app from a command prompt. If multiple apps use the same name, choose which one to use.

Xbox Game Bar
GameBarElevatedFT_Alias.exe
On

Microsoft Edge
MicrosoftEdge.exe
On

App Installer
python.exe
On

App Installer
python3.exe
On

Windows Subsystem for Linux

PowerShell Core:

"If we build it,
they will come."

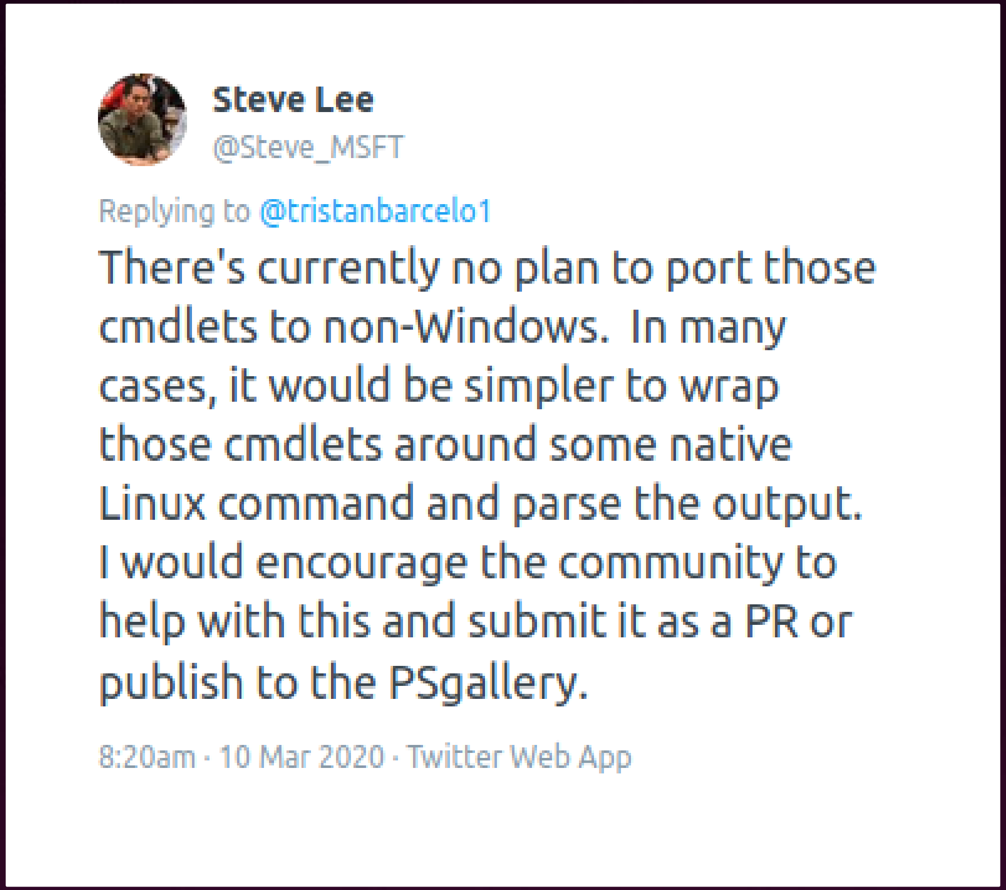
https://GitHub.com/PowerShell

.deb, .rpm, .pkg, .msi
snapcraft.io
C# source

Ubuntu 18.10 and later:

```
snap install powershell --classic
```

Regarding PowerShell networking cmdlets:



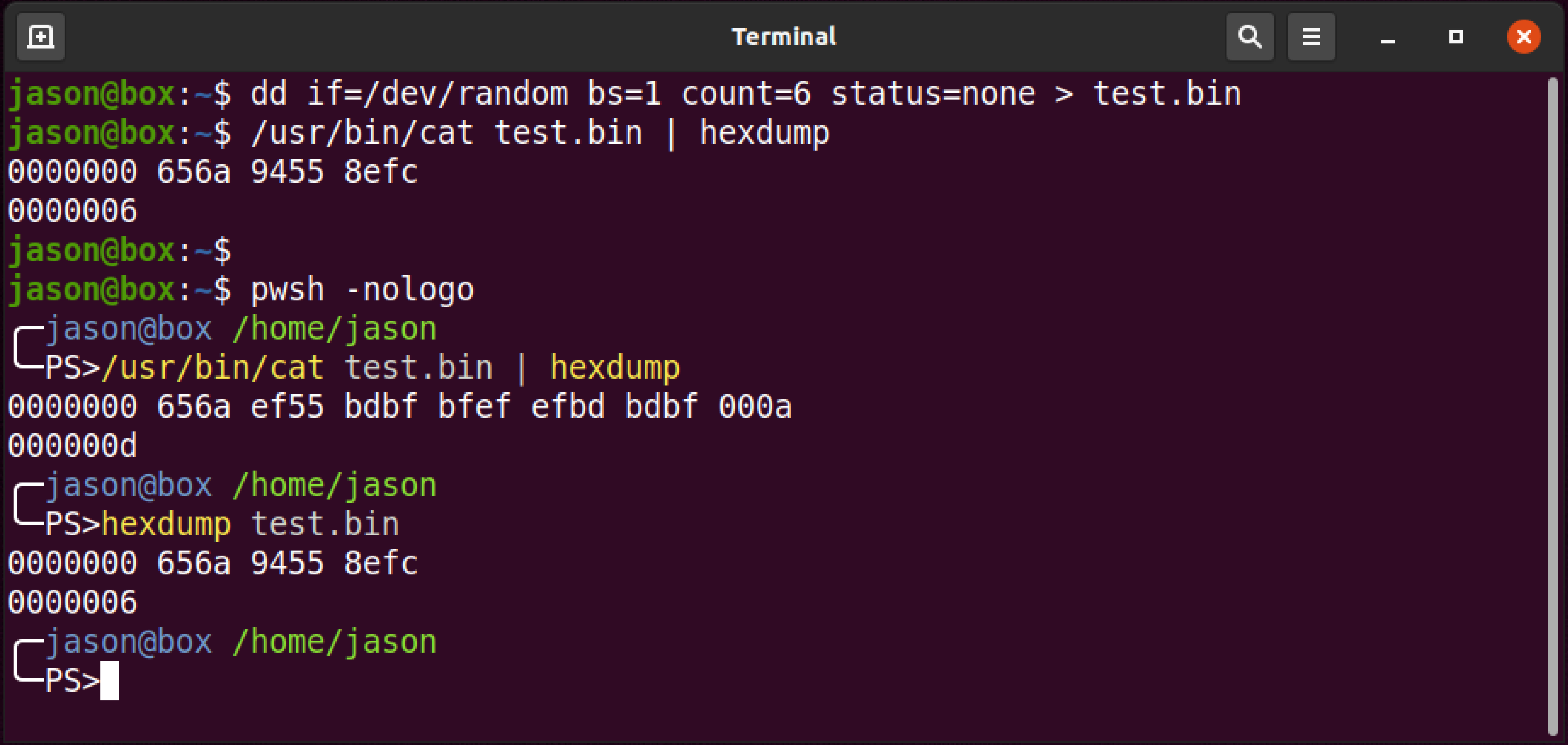
Steve Lee
@Steve_MSFT

Replying to @tristanbarcelo1

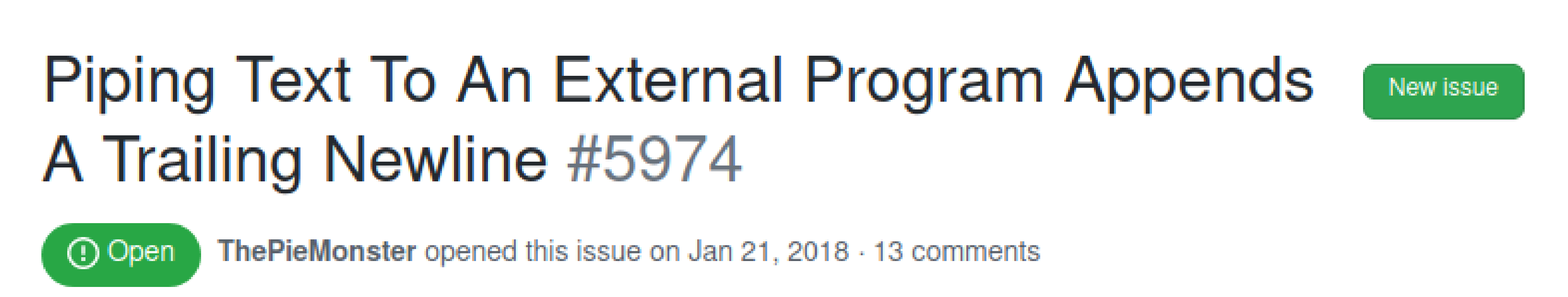
There's currently no plan to port those cmdlets to non-Windows. In many cases, it would be simpler to wrap those cmdlets around some native Linux command and parse the output. I would encourage the community to help with this and submit it as a PR or publish to the PSgallery.

8:20am · 10 Mar 2020 · Twitter Web App

Samba
systemd
ZFS

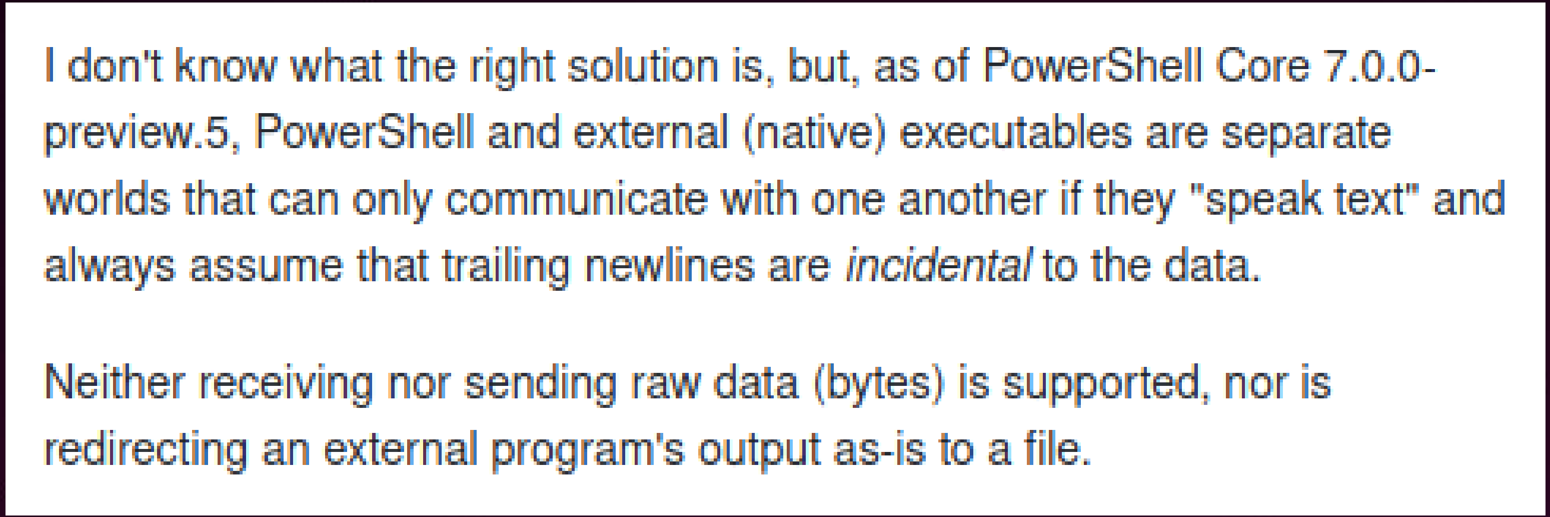


```
jason@box:~$ dd if=/dev/random bs=1 count=6 status=none > test.bin
jason@box:~$ /usr/bin/cat test.bin | hexdump
0000000 656a 9455 8efc
0000006
jason@box:~$
jason@box:~$ pwsh -nologo
┌jason@box /home/jason
└PS>/usr/bin/cat test.bin | hexdump
0000000 656a ef55 bdbf bfef efbd bdbf 000a
000000d
┌jason@box /home/jason
└PS>hexdump test.bin
0000000 656a 9455 8efc
0000006
┌jason@box /home/jason
└PS>
```



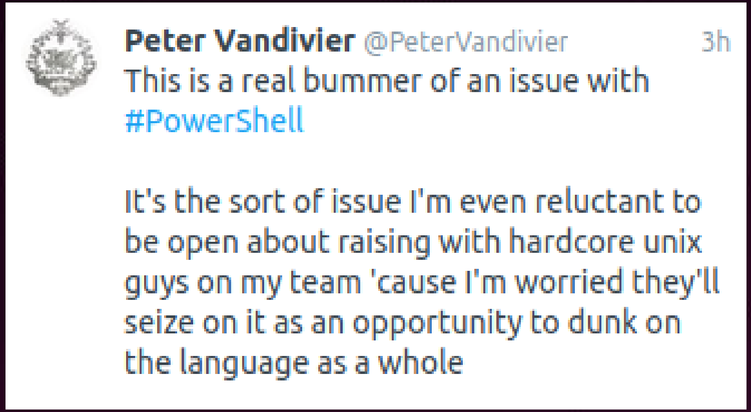
Piping Text To An External Program Appends A Trailing Newline #5974

ThePieMonster opened this issue on Jan 21, 2018 · 13 comments



I don't know what the right solution is, but, as of PowerShell Core 7.0.0-preview.5, PowerShell and external (native) executables are separate worlds that can only communicate with one another if they "speak text" and always assume that trailing newlines are *incidental* to the data.

Neither receiving nor sending raw data (bytes) is supported, nor is redirecting an external program's output as-is to a file.



Peter Vandivier @PeterVandivier 3h

This is a real bummer of an issue with #PowerShell

It's the sort of issue I'm even reluctant to be open about raising with hardcore unix guys on my team 'cause I'm worried they'll seize on it as an opportunity to dunk on the language as a whole

https://github.com/PowerShell/PowerShell/issues/5974
https://github.com/PowerShell/PowerShell/issues/13428
https://github.com/PowerShell/PowerShell/issues/1995

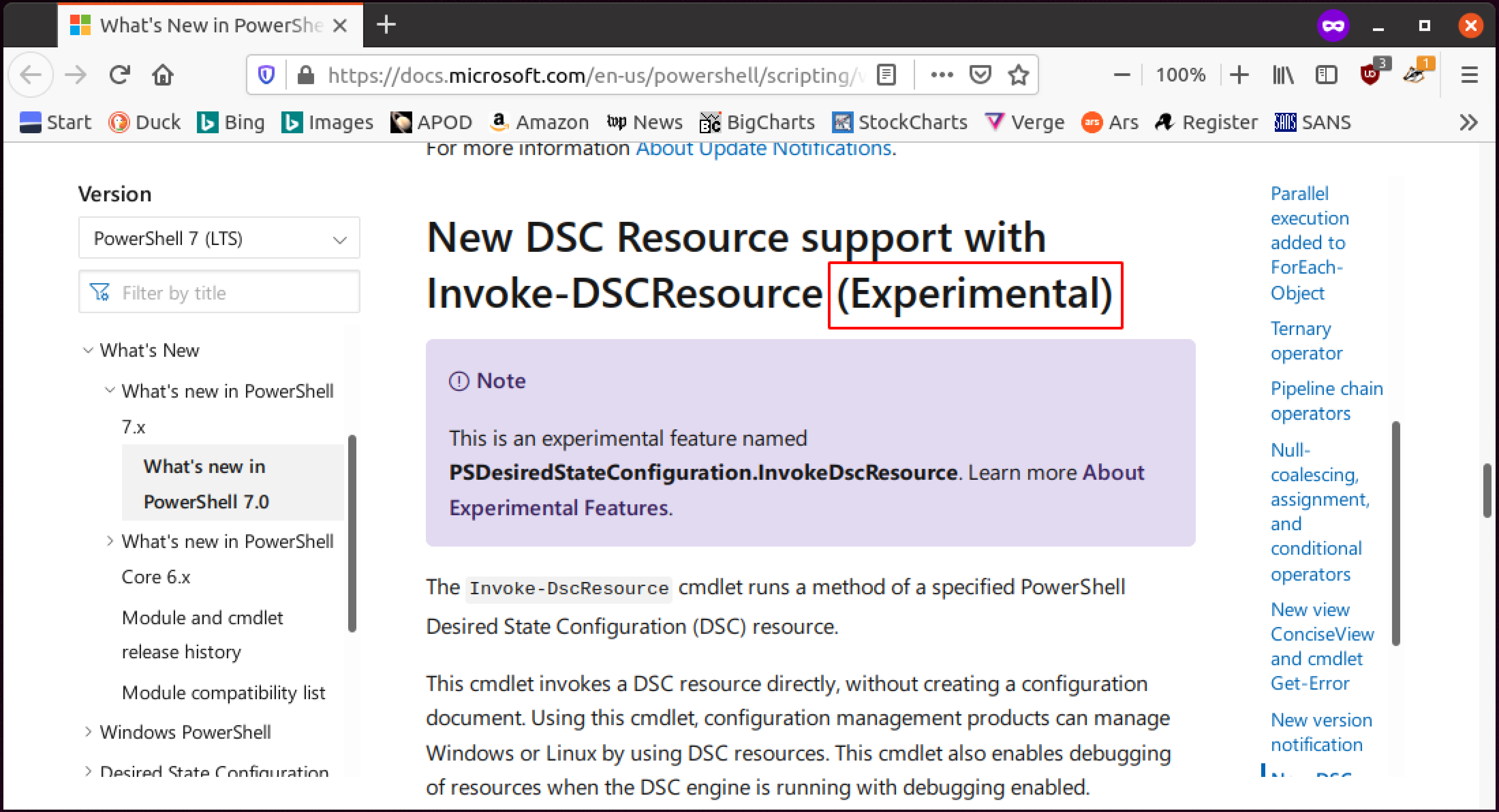
PowerShell

⇩ ⇧

/etc config files

Puppet
Chef
Ansible
Salt

Desired State Configuration


What's New in PowerShe
https://docs.microsoft.com/en-us/powershell/scripting/
100%
Start
Duck
Bing
Images
APOD
Amazon
News
BigCharts
StockCharts
Verge
Ars
Register
SANS
Version
PowerShell 7 (LTS)
Filter by title
What's New
What's new in PowerShell 7.x
What's new in PowerShell 7.0
What's new in PowerShell Core 6.x
Module and cmdlet release history
Module compatibility list
Windows PowerShell
Desired State Configuration
Parallel execution added to ForEach-Object
Ternary operator
Pipeline chain operators
Null-coalescing, assignment, and conditional operators
New view ConciseView and cmdlet Get-Error
New version notification

For more information About Update Notifications.

New DSC Resource support with Invoke-DSCResource (Experimental)

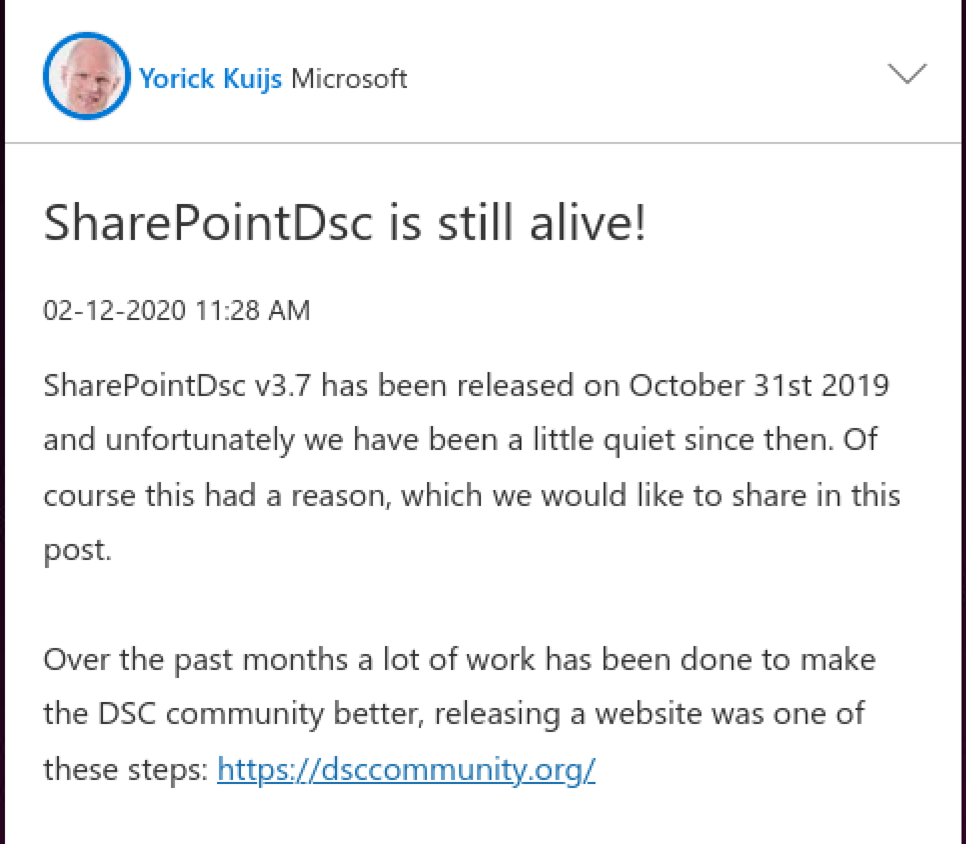
ⓘ **Note**

This is an experimental feature named **PSDesiredStateConfiguration.InvokeDscResource**. Learn more About Experimental Features.

The `Invoke-DscResource` cmdlet runs a method of a specified PowerShell Desired State Configuration (DSC) resource.

This cmdlet invokes a DSC resource directly, without creating a configuration document. Using this cmdlet, configuration management products can manage Windows or Linux by using DSC resources. This cmdlet also enables debugging of resources when the DSC engine is running with debugging enabled.

DSC is probably dead



Yorick Kuijs Microsoft

SharePointDsc is still alive!

02-12-2020 11:28 AM

SharePointDsc v3.7 has been released on October 31st 2019 and unfortunately we have been a little quiet since then. Of course this had a reason, which we would like to share in this post.

Over the past months a lot of work has been done to make the DSC community better, releasing a website was one of these steps: https://dsccommunity.org/

PowerShell Core on Windows?

PowerShell + OpenSSH is great!

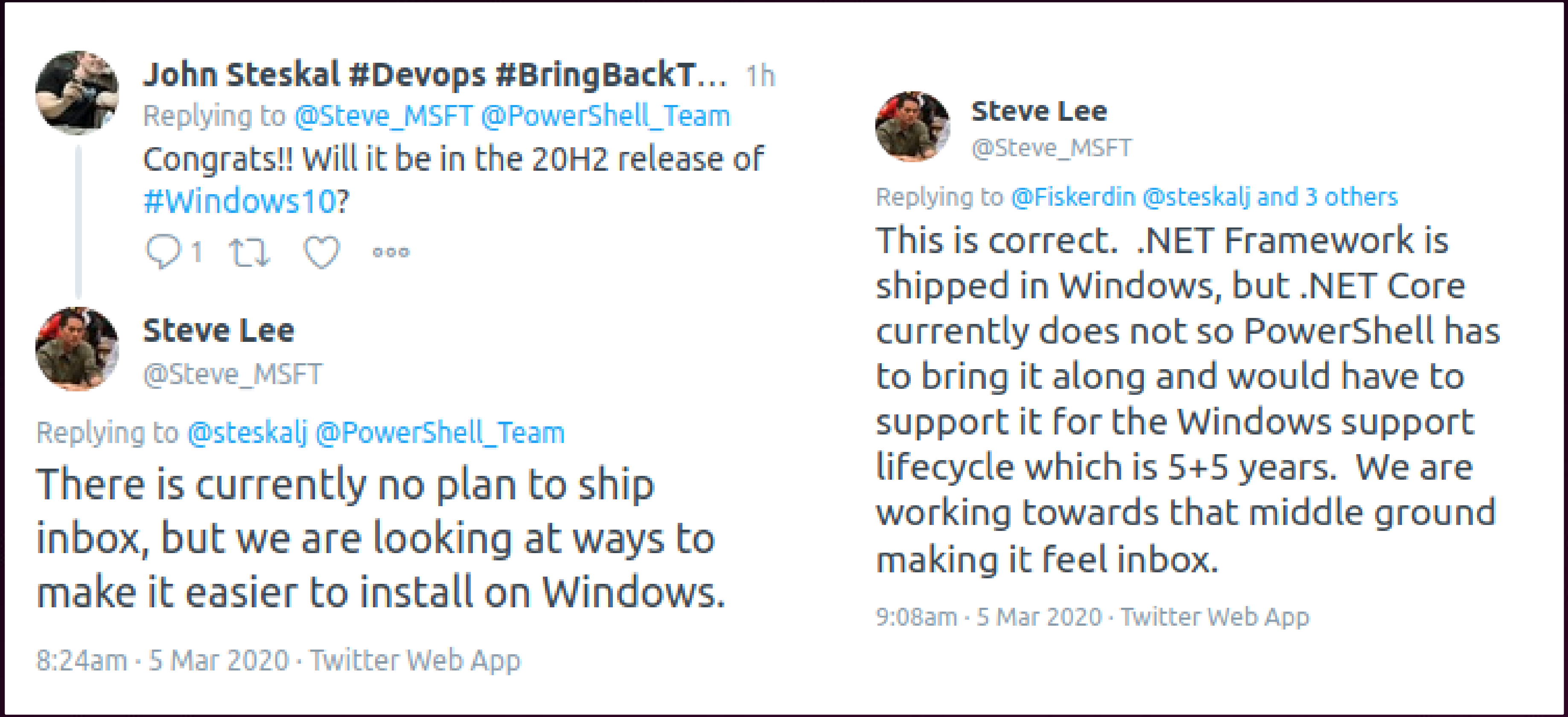
Faster Performance:

ForEach -Parallel

Invoke-RestMethod

Invoke-WebRequest

When will PowerShell Core be installed by default?



John Steskal #Devops #BringBackT… 1h

Replying to @Steve_MSFT @PowerShell_Team

Congrats!! Will it be in the 20H2 release of #Windows10?

Steve Lee
@Steve_MSFT

Replying to @steskalj @PowerShell_Team

There is currently no plan to ship inbox, but we are looking at ways to make it easier to install on Windows.

8:24am · 5 Mar 2020 · Twitter Web App

Steve Lee
@Steve_MSFT

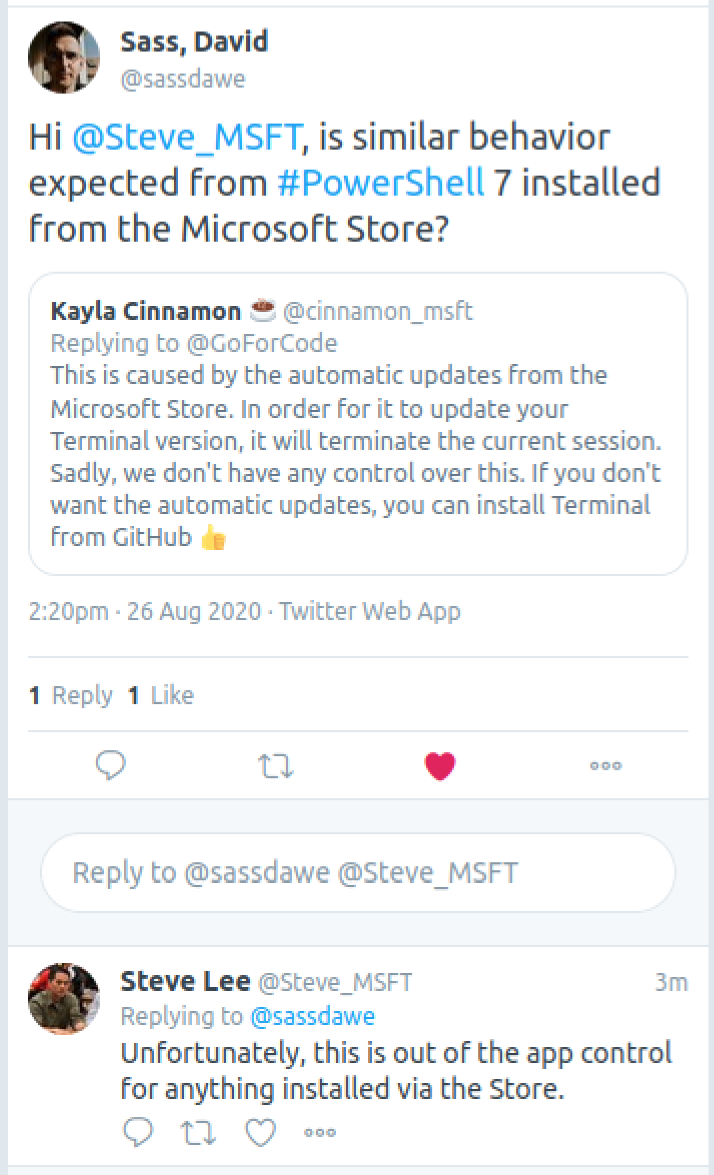
Replying to @Fiskerdin @steskalj and 3 others

This is correct. .NET Framework is shipped in Windows, but .NET Core currently does not so PowerShell has to bring it along and would have to support it for the Windows support lifecycle which is 5+5 years. We are working towards that middle ground making it feel inbox.

9:08am · 5 Mar 2020 · Twitter Web App

"In order for [automatic updates] to update your Terminal version, it will terminate the current session."

This includes PowerShell Core installed from the Microsoft Store too!



Sass, David
@sassdawe

Hi @Steve_MSFT, is similar behavior expected from #PowerShell 7 installed from the Microsoft Store?

> **Kayla Cinnamon** ☕ @cinnamon_msft
> Replying to @GoForCode
> This is caused by the automatic updates from the Microsoft Store. In order for it to update your Terminal version, it will terminate the current session. Sadly, we don't have any control over this. If you don't want the automatic updates, you can install Terminal from GitHub 👍

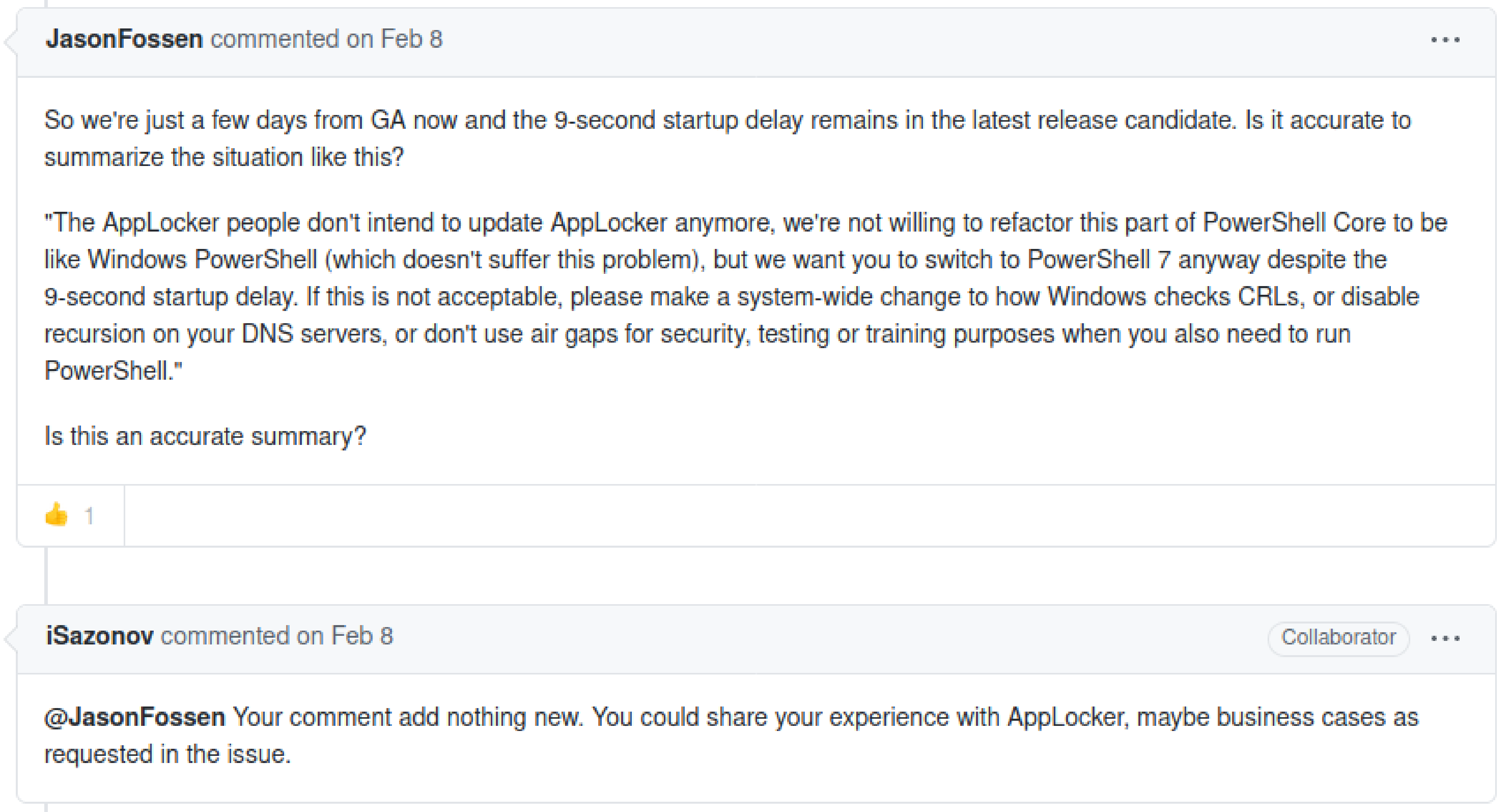
2:20pm · 26 Aug 2020 · Twitter Web App

1 Reply **1** Like

Reply to @sassdawe @Steve_MSFT

Steve Lee @Steve_MSFT 3m
Replying to @sassdawe
Unfortunately, this is out of the app control for anything installed via the Store.

9-second start delay on Windows running in some air gap networks



JasonFossen commented on Feb 8

So we're just a few days from GA now and the 9-second startup delay remains in the latest release candidate. Is it accurate to summarize the situation like this?

"The AppLocker people don't intend to update AppLocker anymore, we're not willing to refactor this part of PowerShell Core to be like Windows PowerShell (which doesn't suffer this problem), but we want you to switch to PowerShell 7 anyway despite the 9-second startup delay. If this is not acceptable, please make a system-wide change to how Windows checks CRLs, or disable recursion on your DNS servers, or don't use air gaps for security, testing or training purposes when you also need to run PowerShell."

Is this an accurate summary?

👍 1

iSazonov commented on Feb 8

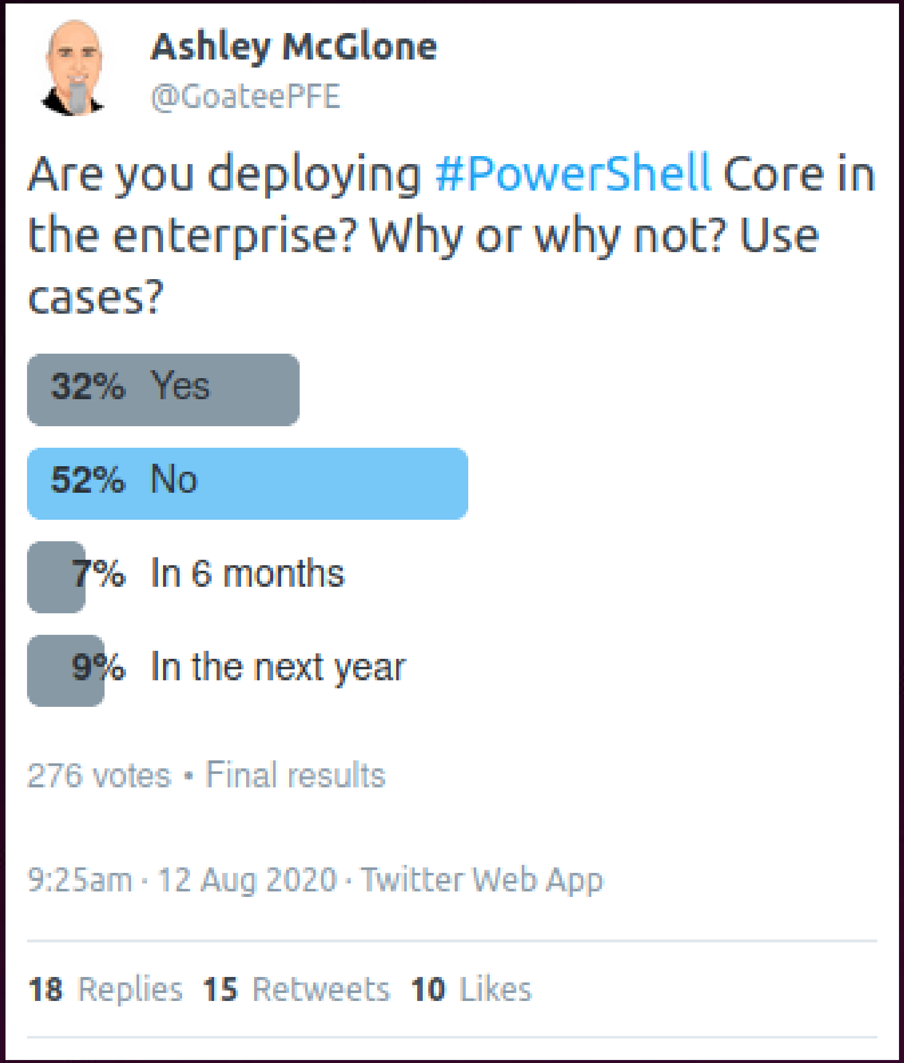
@JasonFossen Your comment add nothing new. You could share your experience with AppLocker, maybe business cases as requested in the issue.

https://github.com/PowerShell/PowerShell/issues/10983
https://github.com/PowerShell/PowerShell/issues/11074

The Windows Compatibility Module

"Pay no attention to that Windows PowerShell remoting session behind the curtain!"

Get-Help about_Windows_PowerShell_Compatibility



Ashley McGlone
@GoateePFE

Are you deploying #PowerShell Core in the enterprise? Why or why not? Use cases?

32% Yes

52% No

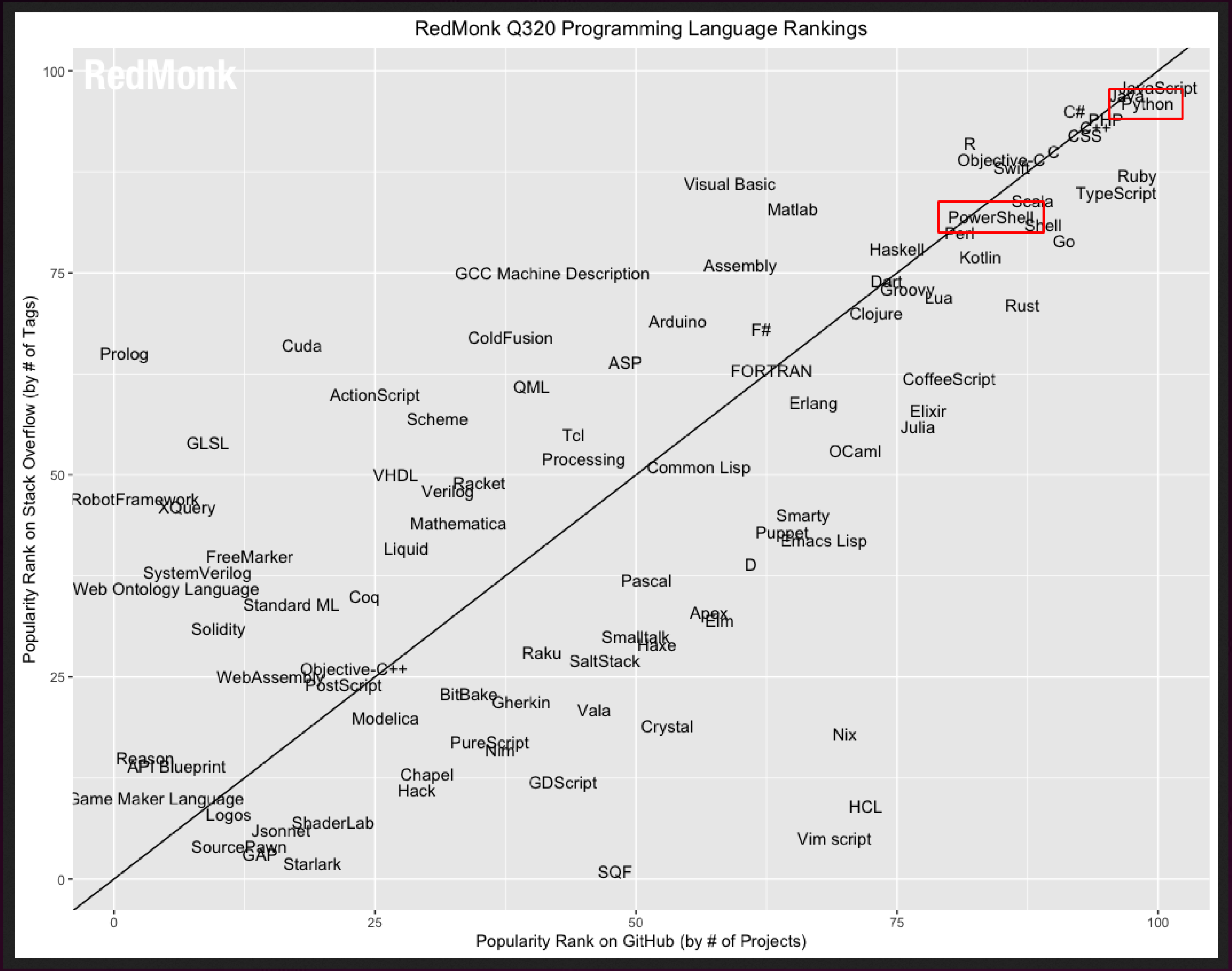
7% In 6 months

9% In the next year

276 votes • Final results

9:25am · 12 Aug 2020 · Twitter Web App

18 Replies **15** Retweets **10** Likes



https://redmonk.com/sogrady/2020/07/27/language-rankings-6-20/

The future of PowerShell on Windows is bright and getting more popular every year

Thank You
for attending!

SANS Institute Courses

PowerShell: SEC505

Python: SEC573

@JasonFossen

jason@sans.org

https://BlueTeamPowerShell.com