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/

<table>
<thead>
<tr>
<th>unique packages</th>
<th>total downloads</th>
<th>total packages</th>
</tr>
</thead>
<tbody>
<tr>
<td>2,023</td>
<td>3,734,874</td>
<td>8,536</td>
</tr>
</tbody>
</table>
PsGet

PsGet - search and install PowerShell modules easy

http://psget.net
Security Review

- Requested to do a review
- Started with one VM
  - Tried to install 1800 chocolatey packages
Well there’s your first problem…


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+XBVOncfH+YhskwwhSkQ3akfYPv7ATPCZwm8aFj2ED8
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
The $env:PATH

```powershell
PS C:\Users\Administrator> ($env:Path).split(";")
\%SystemRoot%\system32\WindowsPowerShell\v1.0\WindowsPowerShell\v1.0\Windows\system32\Windows\Program Files\Microsoft Network Monitor 3\Python33
PS C:\Users\Administrator>
```
PSv3 uses the PATH...
So a user can...
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

I HAVE NO IDEA WHAT I'M DOING
Thanks

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