ETERNAL BLUE MS17-010

HOW YOU CAN GET HACKED
ABOUT ME

• Director of CyberResponse and Development @ Compass IT compliance
• Hacker/Pen Tester
• Assistant Professor @ New England Institute of Technology
ETERNAL BLUE

• Software vulnerability in Microsoft's Windows operating system. MS17-010

• The vulnerability works by exploiting the Microsoft Server Message Block 1.0

• SMB allows applications on a computer to read and write to files and to request services that are on the same network
ETERNAL BLUE CONT...

• All versions of Windows are vulnerable
• Many computers are still un-patched
• Security update was Published March 14, 2017
• Over two years ago......
TWO YEARS IS A LONG TIME
IS IT STILL AN ISSUE????
**SMB1 EternalBlue Targets**

Search for `port:445 "SMB Version: 1" os:Windows |product:Samba` returned 976,785 results on 01-04-2019

<table>
<thead>
<tr>
<th>Top Countries</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. United States</td>
<td>354,216</td>
</tr>
<tr>
<td>2. Japan</td>
<td>81,267</td>
</tr>
<tr>
<td>3. Russian Federation</td>
<td>74,359</td>
</tr>
<tr>
<td>4. Taiwan</td>
<td>49,999</td>
</tr>
<tr>
<td>5. Germany</td>
<td>47,110</td>
</tr>
<tr>
<td>6. China</td>
<td>26,480</td>
</tr>
<tr>
<td>7. United Kingdom</td>
<td>23,659</td>
</tr>
<tr>
<td>8. Netherlands</td>
<td>21,073</td>
</tr>
<tr>
<td>9. Hong Kong</td>
<td>20,146</td>
</tr>
<tr>
<td>10. Turkey</td>
<td>18,614</td>
</tr>
</tbody>
</table>
LET'S NARROW DOWN THE LIST TO ORLANDO
SO OVER 1,166 LOCALLY POTENTIAL TARGETS AS OF 10-2019
CRAZY........
DISCLAIMER

• I am not saying all the hosts are indeed vulnerable
• I am saying that they are potential targets that a hacker will try to exploit
• The eternal blue vulnerability is very easy to execute
START PROTECTING YOURSELF

• Know your inventory
• Get Audited
• Get Pen Tested
THANK YOU.....

Jesse Roberts

jroberts@compassitc.com