Sticky Keys to the Kingdom

PRE-AUTH SYSTEM RCE ON WINDOWS IS MORE COMMON THAN YOU THINK
DENNIS MALDONADO & TIM MCGUFFIN LARES
Agenda

• About Us
• Problem Background
• Our Solution
• Statistics
• Prevention / Remediation
• Summary
About Us

• Dennis Maldonado
  • Adversarial Engineer – LARES Consulting
  • Founder
  • Houston Locksport
  • Houston Area Hackers Anonymous (HAHA)

• Tim McGuffin
  • Red Team Manager – LARES Consulting
  • 10-year DEFCON Goon
  • DEFCON CTF Participant
  • Former CCDC Team Coach

www.lares.com
# Windows Accessibility Tools

<table>
<thead>
<tr>
<th>Binary</th>
<th>Description</th>
<th>How to access</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Windows\System32\Utilman.exe</td>
<td>Utility Manager</td>
<td>Windows Key + U</td>
</tr>
<tr>
<td>C:\Windows\System32\sethc.exe</td>
<td>Accessibility shortcut keys</td>
<td>Shift 5 times</td>
</tr>
<tr>
<td>C:\Windows\System32\osk.exe</td>
<td>On-Screen Keyboard</td>
<td>Locate the option on the screen using the mouse</td>
</tr>
<tr>
<td>C:\Windows\System32\Magnify.exe</td>
<td>Magnifier</td>
<td>Windows Key + [Equal Sign]</td>
</tr>
<tr>
<td>C:\Windows\System32\Narrator.exe</td>
<td>Narrator</td>
<td>Windows Key + Enter</td>
</tr>
<tr>
<td>C:\Windows\System32\DisplaySwitch.exe</td>
<td>Display Switcher</td>
<td>Windows Key + P</td>
</tr>
<tr>
<td>C:\Windows\System32\AtBroker.exe</td>
<td>Manages switching of apps between desktops</td>
<td>Have <code>osk.exe</code>, <code>Magnify.exe</code>, or <code>Narrator.exe</code> open then lock the computer. <code>AtBroker.exe</code> will be executed upon locking and unlocking</td>
</tr>
</tbody>
</table>
History

- “How to Reset Windows Passwords” websites
  - Replace `sethc.exe` or `utilman.exe` with `cmd.exe`
  - Reboot, Press Shift 5x or WIN+U
  - `net user (username) (password)`
  - Login!

- Nobody ever cleans up after themselves

- Can be used as a backdoor/persistence method

- No Windows Event Logs are generated when backdoor is executed

3. Type the following command (replace “c:” with the correct drive letter if Windows is not located on C:):

   ```
   copy c:\windows\system32\sethc.exe c:\
   ```
Implementation

• Binary Replacement
  • Replace any of the accessibility tool binaries
  • Requires elevated rights
  • May require taking ownership of files

• Registry (Debugger Method)
  • HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe
  • Debugger REG_SZ C:\Windows\System32\cmd.exe
  • Requires elevated rights
Limitations

• Elevated access or offline system required
• Replacing binary must be Digitally Signed
• Replacing binary must exist in \System32\n• Replacing binary must exist in Windows “Protected File” list
• You can’t use any old Binary, but you can cmd.exe /c file.bat
Background

• While working with an Incident Response Team:
  • Uncovered dozens of vulnerable servers and workstations via file checks
    • Identification was done from the filesystem side
    • Missed the Debugger Method

• Missed any unmanaged boxes

• Needed a network-based scanner
Background

• We wanted to write our own network-based tool
  • Started down the JavaRDP Path

• Ran across @ztgrace’s PoC script, Sticky Keys Hunter
  • It worked, and was a great starting point
  • Similar to “Peeping Tom”
    • Opens a Remote Desktop connection
    • Sends keyboard presses
    • Saves screenshot to a file
  • Needed bug fixes, additional checks, had a TODO list, but not actively developed
Our Solution

• Automated Command Prompt Detection
• Parallelized scanning of multiple hosts
• Tons of bug fixes
• Error Handling
• Dynamic Timing

• Requires **imagemagick, xdotool, bc, parallel**
  • All packages exist in the Kali repositories
DEMO
Solution - Limitations

- Ties up a Linux VM while scanning
  - Needed for window focus and screenshotting

- Will not catch binaries that are replaced with anything other than `cmd.exe`
  - You get to scroll through screenshots!
  - Ran across `taskmgr.exe`, `mmc.exe`, other custom applications
Statistics

• On a large Business ISP:
  • Over 100,000 boxes scanned
  • About 571 Command Prompts (every 1 out of 175)
  • All types of Institutions
    • Educational Institutions
    • Law Offices
    • Manufacturing Facilities
    • Gaming companies
    • Etc...
Recommendations

• Remediation
  • Delete or replace the effected file (sethc.exe, utilman.exe, ...)
  • `sfc.exe /scannow`
  • Remove the affected registry entry

• Prevention and Detection
  • Network Level Authentication for Remote Desktop Connection
  • Restrict local administrative access
  • Enable FDE and protect the key
  • End point monitoring
Summary

• Multi-threaded scanner for binary replacement backdoor with command prompt detection

• TODO:
  • Code Cleanup
  • Read in nmap output

• Code will be on Github

www.lares.com
Questions?

www.lares.com