Who’s that CARBANAKing at my door?
Hunting for Malicious Application Compatibility Shims

Benjamin Wiley
Associate Consultant, Mandiant Professional Services, FireEye
Introduction

- Ben Wiley, Associate Consultant
  - Mandiant Professional Services
  - Incident response, digital forensics, threat hunting
  - Hobbies: traveling, spending time outdoors
  - Previously: Network Support Analyst, SOC Analyst
- Today’s Topic: Case Study and Techniques for Hunting Malicious Application Compatibility Shims
A little background...
FIN7

- Active since late 2015
- Primary objective: point of sale compromise
- Over 100 U.S. companies targeted
- Victim companies in 47 U.S. states
- Restaurant, gaming, and hospitality industries
- US government announced the arrests of 3 members in August 2018
- Operated as a security company
Bob’s Breach

- Large Domestic Restaurant Chain
- Receive a Common Point of Purchase Notification
- 5,000+ Point-of-Sale systems
- Anti-virus never detected anything
- What’s going on? How do we move forward with the investigation?
Searching for Malware

- Running Processes
- Logs
- Evidence of Execution
  - Prefetch
  - ShimCache
  - AmCache
- Run Keys
- Startup Folder
- Scheduled Tasks
- Windows Services
Application Compatibility Infrastructure

- Resolves application compatibility issues with Windows codebase
- **Shim** = alternative code injected into a process
- **Fix** = a single change
- **Mode** = a bundle of changes
- Stored in databases (.sdb files)
  - C:\Windows\AppPatch\sysmain.sdb
  - C:\Windows\AppPatch\pcamain.sdb
  - C:\Windows\AppPatch\msimain.sdb
  - C:\Windows\AppPatch\frxmain.sdb
  - C:\Windows\AppPatch\drvmain.sdb
  - Custom SDB files
Process Shimming

- Parent process starts process creation function
- Checks if process should be shimmed
- Child process also checks to see if it should be shimmed
- SDB file is located and parsed, shim hooks the Import Address Table (IAT)
- Shim intercepts and manipulates Windows API calls
Legitimate Shim Uses

- Microsoft Fix It Patches
  - No longer supported in Windows 10
- EMET
  - End of Life – July 31, 2018
  - C:\WINDOWS\AppPatch\EMET.dll
  - aSetprocessdepp loaded
- Third party software
  - Common in video game industry
Shim Databases

```xml
<EXE>
  <NAME type='stringref'>AOLSETUP.EXE</NAME>
  <APP_NAME type='stringref'>AOL 9.0</APP_NAME>
  <VENDOR type='stringref'>AOL</VENDOR>
  <EXE_ID type='hex'>676ac648-f809-4175-9ee7-76f0fb4d6a12</EXE_ID>
  <APP_ID type='hex'>1e3048d0-af63-4533-9eec-abf73f2170e9</APP_ID>
  <MATCH_MODE type='integer'>0x2</MATCH_MODE>
  <MATCHING_FILE>
    <NAME type='stringref'>*\America Online, Inc.\AOL Download Utility</NAME>
    <COMPANY_NAME type='stringref'>America Online, Inc.</COMPANY_NAME>
    <FILE_DESCRIPTION type='stringref'>AOL Download Utility</FILE_DESCRIPTION>
    <UPTO_BINPRODUCT_VERSION type='integer'>0xaffffffffff</UPTO_BINPRODUCT_VERSION>
  </MATCHING_FILE>
  <MATCHING_FILE>
    <NAME type='stringref'>AOL90\SETUP90.EXE</NAME>
  </MATCHING_FILE>
  <NAME type='stringref'>AOLSETUP.CAB</NAME>
  <VENDOR type='stringref'>AOL</VENDOR>
  <EXE_ID type='hex'>676ac648-f809-4175-9ee7-76f0fb4d6a12</EXE_ID>
  <APP_ID type='hex'>1e3048d0-af63-4533-9eec-abf73f2170e9</APP_ID>
  <MATCH_MODE type='integer'>0x2</MATCH_MODE>
  <MATCHING_FILE>
    <NAME type='stringref'>*\America Online, Inc.\AOL Download Utility</NAME>
    <COMPANY_NAME type='stringref'>America Online, Inc.</COMPANY_NAME>
    <FILE_DESCRIPTION type='stringref'>AOL Download Utility</FILE_DESCRIPTION>
    <UPTO_BINPRODUCT_VERSION type='integer'>0xaffffffffff</UPTO_BINPRODUCT_VERSION>
  </MATCHING_FILE>
  <MATCHING_FILE>
    <NAME type='stringref'>AOL90\SETUP90.EXE</NAME>
  </MATCHING_FILE>
  <NAME type='stringref'>AOLSETUP.CAB</NAME>
  <VENDOR type='stringref'>AOL</VENDOR>
  <EXE_ID type='hex'>676ac648-f809-4175-9ee7-76f0fb4d6a12</EXE_ID>
  <APP_ID type='hex'>1e3048d0-af63-4533-9eec-abf73f2170e9</APP_ID>
  <MATCH_MODE type='integer'>0x2</MATCH_MODE>
  <MATCHING_FILE>
    <NAME type='stringref'>*\America Online, Inc.\AOL Download Utility</NAME>
    <COMPANY_NAME type='stringref'>America Online, Inc.</COMPANY_NAME>
    <FILE_DESCRIPTION type='stringref'>AOL Download Utility</FILE_DESCRIPTION>
    <UPTO_BINPRODUCT_VERSION type='integer'>0xaffffffffff</UPTO_BINPRODUCT_VERSION>
  </MATCHING_FILE>
  <MATCHING_FILE>
    <NAME type='stringref'>AOL90\SETUP90.EXE</NAME>
  </MATCHING_FILE>
  <NAME type='stringref'>AOLSETUP.EXE</NAME>
  <VENDOR type='stringref'>AOL</VENDOR>
  <EXE_ID type='hex'>676ac648-f809-4175-9ee7-76f0fb4d6a12</EXE_ID>
  <APP_ID type='hex'>1e3048d0-af63-4533-9eec-abf73f2170e9</APP_ID>
  <MATCH_MODE type='integer'>0x2</MATCH_MODE>
  <MATCHING_FILE>
    <NAME type='stringref'>*\America Online, Inc.\AOL Download Utility</NAME>
    <COMPANY_NAME type='stringref'>America Online, Inc.</COMPANY_NAME>
    <FILE_DESCRIPTION type='stringref'>AOL Download Utility</FILE_DESCRIPTION>
    <UPTO_BINPRODUCT_VERSION type='integer'>0xaffffffffff</UPTO_BINPRODUCT_VERSION>
  </MATCHING_FILE>
  <MATCHING_FILE>
    <NAME type='stringref'>AOL90\SETUP90.EXE</NAME>
  </MATCHING_FILE>
  <NAME type='stringref'>AOLSETUP.CAB</NAME>
  <VENDOR type='stringref'>AOL</VENDOR>
  <EXE_ID type='hex'>676ac648-f809-4175-9ee7-76f0fb4d6a12</EXE_ID>
  <APP_ID type='hex'>1e3048d0-af63-4533-9eec-abf73f2170e9</APP_ID>
  <MATCH_MODE type='integer'>0x2</MATCH_MODE>
  <MATCHING_FILE>
    <NAME type='stringref'>*\America Online, Inc.\AOL Download Utility</NAME>
    <COMPANY_NAME type='stringref'>America Online, Inc.</COMPANY_NAME>
    <FILE_DESCRIPTION type='stringref'>AOL Download Utility</FILE_DESCRIPTION>
    <UPTO_BINPRODUCT_VERSION type='integer'>0xaffffffffff</UPTO_BINPRODUCT_VERSION>
  </MATCHING_FILE>
  <MATCHING_FILE>
    <NAME type='stringref'>AOL90\SETUP90.EXE</NAME>
  </MATCHING_FILE>
</EXE>
```
Shim Registration and Installation

- **sdbinst.exe**
  - Registers
    - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom\n    - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\InstalledSDB\n  - Copies SDB to default file location
    - C:\Windows\AppPatch\Custom\n    - C:\Windows\AppPatch\Custom\Custom64\n  - Shows up in Add/Remove Programs

- **Custom installer**
  - sdb-explorer.exe
  - Shim registration requires Administrator level privileges
Who’s that CARBANAKing at my door?
The Case of the Missing CARBANAK

- Custom Base64 encoded PowerShell script
  - Utilized sdbinst.exe
- C:\Windows\Temp\sdbE376.tmp
The Case of the Missing CARBANAK

Upon execution of the script, the following changes were made to the system:

- HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\AppCompatFlags\Custom\services.exe
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\InstalledSDB\{8a2ccc5d-5332-7116-d3c1-a8437149ad4}
- C:\Windows\AppPatch\Custom\Custom64\{8a2ccc5d-5332-7116-d3c1-a8437149ad4}.sdb
- \REGISTRY\MACHINE\SOFTWARE\Microsoft\DRM\4
The Case of the Missing CARBANAK

<DATABASE>
<NAME type='stringref'>Microsoft KB2832077</NAME>
<DATABASE_ID type='guid'>51da9ecc- ac66- d6cf- bbd1- 6ed92ac6c3f1</DATABASE_ID>
<OS_PLATFORM type='integer'>0x2</OS_PLATFORM>
<PATCH>
<NAME type='stringref'>ServicesFix01</NAME>
<PATCH_BITS type='hex'>0200<REDACTED>0000</PATCH_BITS>
</PATCH>
<EXE>
<NAME type='stringref'>services.exe</NAME>
<APP_NAME type='stringref'>Microsoft Services</APP_NAME>
<EXE_ID type='hex'>e0b38a24- 6175- 24f5- d646- 6053230c45aa</EXE_ID>
<MATCHING_FILE>
<NAME type='stringref'>services.exe</NAME>
<COMPANY_NAME type='stringref'>Microsoft Corporation</COMPANY_NAME>
</MATCHING_FILE>
<PATCH_REF>
<NAME type='stringref'>ServicesFix01</NAME>
<PATCH_TAGID type='integer'>0x60</PATCH_TAGID>
</PATCH_REF>
</EXE>
</DATABASE>
### The Case of the Missing CARBANAK

<table>
<thead>
<tr>
<th>Opcode</th>
<th>Module Name</th>
<th>RVA</th>
<th>Unk</th>
<th>Payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>PATCH_REPLACE</td>
<td>services.exe</td>
<td>0x0001407c</td>
<td>0x00000000</td>
<td>00 00 00 00 00 5C 00 52 00</td>
</tr>
</tbody>
</table>
The Case of the Missing CARBANAK

services.exe

ScRegisterTCP Endpoint
RVA: 0x0001407c

Stage 1 Shellcode
The Case of the Missing CARBANAK

services.exe

\HKLM\SOFTWARE\Microsoft\DRM\4
Stage 1 Shellcode

services.exe

Stage 2 Shellcode
The Case of the Missing CARBANAK

services.exe

Stage 2 Shellcode

RtlDecompressBuffer API Call

services.exe

CARBANAK DLL
The Case of the Missing CARBANAK

services.exe

4 minute "nap"

svchost.exe

CARBANAK DLL
The Case of the Missing CARBANAK

The Windows loader checks the application compatibility registry location to see if any patches are required for the specific binary that is being loaded.

Reads the Windows Registry path:
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom\services.exe
Contains the value:
{812ccc5d-5332-7116-d3c1-a843714e9ad4}.sdb

1st Stage – The in-memory patch is installed for the 64-bit “services.exe”
Read the contents of the identified SDB file and applies the patch stored in the file:
C:\Windows\AppPatch\Custom\Custom64\{812ccc5d-5332-7116-d3c1-a843714e9ad4}.sdb

2nd Stage – “services.exe” attempts to call the function “ScRegisterTCPPEndpoint”, which has been patched (overwritten) with the shellcode.
The patch contains instructions to read additional shellcode and the CARBANAK payload stored in the registry:
HKLM\SOFTWARE\Microsoft\DRM\4
CARBANAK Capabilities

- Over 40 commands
- Key logger
- Form grabber
- HTTP proxy
- Desktop video recording
- Network tunnel
- RDP
- VNC
- Updater
- Add additional plugins
Oh, the possibilities....
What else can shims do?

Let’s get creative

- InjectDLL
- RedirectExe
- VirtualRegistry
- DisableWindowsDefender
- TerminateExe
- RunAsAdmin
- RedirectHKCUKeys
- CorrectFilePaths

- LoadLibraryRedirectFlag
- DisableNX
- DisableASLR
- DisableSEP
- NoSignatureCheck
- RedPill
- AlienVsPredator
REDSALT

- PLATINUM GROUP
- Backdoor functionality
- Shims CiscoVpn.exe
  - InjectDLL fix loads obfuscated 1st DLL (95% junk code)
  - 1st DLL decrypts and loads a second DLL
  - 2nd DLL decrypts and loads resource which is the packed payload

500 | Information | Compatibility fix applied to C:\Program Files (x86)\Cisco Systems\VPN Client\ciscovpn.exe. Fix information: InjectDll, {3432bc96-d181-4529-b261-1a3964961b6c}, 0x00010206.
BlackEnergy 2

- Sandworm Team
- Toolkit used in 2015 Ukraine power grid attack
  - 300,000 people without power
- If user is not admin, installer shims SndVol.exe
  - Autoelevates upon execution
  - RedirectEXE fix executes cmd.exe to install malware in an elevated state
- DisableNXShowUI – Disables DEP
T1138 – Application Shimming

ID: T1138

Tactic: Persistence, Privilege Escalation

Platform: Windows

Permissions Required: Administrator

Data Sources: Loaded DLLs, System calls, Windows Registry, Process monitoring, Process command-line parameters

Version: 1.0
So you’re telling me there’s a chance....
Hardening Against Shim Abuse

- Disable Shim Engine via Group Policy – Bad Idea
- Run Windows 10
  - Patch shim doesn’t work
  - RedirectEXE UAC bypass doesn’t work
- Install KB3045645
Detecting Malicious Shims

- **sdbinst.exe process execution**
  - EID 4688 – Process Creation
  - EDR/Sysmon logs
- **Registry keys**
  - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom\n  - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\InstalledSDB\n
Hunting Malicious Shims

- Microsoft-Windows-Application-Experience-Program-Telemetry.evtx
- Sample size: ~500 hosts, ~170k events
  - InjectDLL: 774 events, 3 applications
  - DisableNX: 0 events
  - RunAsAdmin: 3800 events, ~50 applications
  - RedirectExe: 2 events, 1 application

500 - Compatibility fix applied to
C:\Windows\syswow64\iscsicli.exe Fix
information: RedirectEXE, {cc47e060-a618-4d4f-9bbc-57c155c71125}, 0x00010205.
Hunting Malicious Shims

- Acquire SDB files, parse, HUNT
  - Custom SDBs
  - EXE File Name/File Path
  - Vendor Name
  - Description
  - Command Line
  - Compiler Version
  - Header timestamp
  - Fix Name
Hunting Malicious Shims

- Search Protect by Conduit

```xml
<DATABASE>
  <TIME type='integer'>0x1cffe17c1594b72f</TIME>
  <COMPILER_VERSION type='stringref'>2.1.0.3</COMPILER_VERSION>
  <NAME type='stringref'>Apps32</NAME>
  <OS_PLATFORM type='integer'>0x1</OS_PLATFORM>
  <DATABASE_ID type='guid'>8a4d5a43-c64a-45ab-bdf4-804fe18c8e8f</DATABASE_ID>
  <LIBRARY>
    <NAME type='stringref'>VC32Ldr</NAME>
    <SHIM_REF>
      <NAME type='stringref'>InjectDll</NAME>
      <COMMAND_LINE type='stringref'>\\.\globalroot\systemroot\apppatch\nbin\vc32loader.dll</COMMAND_LINE>
    </SHIM_REF>
  </LIBRARY>
  <EXE>
    <NAME type='stringref'>chrome.exe</NAME>
    <NAME type='stringref'>explorer.xxx</NAME>
    <NAME type='stringref'>firefox.exe</NAME>
    <NAME type='stringref'>iexplore.exe</NAME>
    <NAME type='stringref'>software_removal_tool.exe</NAME>
    <NAME type='stringref'>software_reporter_tool.exe</NAME>
  </EXE>
</DATABASE>
```
What’s the worst that could happen?
This is the worst that could happen

- Add new shim to sysmain.sdb
- Shim contains patch for services.exe
  - Payload is Meterpreter reverse shell completely contained within SDB file
- No sdbinst.exe process execution
- No custom SDB file
- Not found in Add/Remove Programs
Summary

- Both targeted and commodity threats are abusing ACI shims
- Usage will increase as organizations improve at detecting traditional malware persistence mechanisms, UAC bypasses, etc.
- Don’t let perfect be the enemy of good
Prior Work

- “Windows - Owned By Default!” – Mark Baggett @ DerbyCon 2013
- “Persist It - Using and Abusing Microsoft Fix It Patches” – Jon Erickson @ Black Hat Asia 2014
- "Defending Against Malicious Application Compatibility Shims” – Sean Pierce @ Black Hat Europe 2015
- "The Real Shim Shady" – Willi Ballenthin & Jonathan Tomczak @ BruCON 0x07
- “To SDB, Or Not To SDB: FIN7 Leveraging Shim Databases for Persistence” by Matthew McWhirt, Jon Erickson, & DJ Palombo
- “ATT&CKing FIN7: The Value of Using Frameworks for Threat Intelligence” – Regina Elwell, FireEye & Katie Nickels, MITRE @ FireEye Cyber Defense Summit 2018
Questions