crazy sexy hacking

MY CAREER ENDING TIN-FOIL HAT TALK
Mark Baggett
@MarkBaggett
Owner of In Depth Defense Penetration Testing & Incident Response Services
Instructor for these guys
SEC573 Python for Penetration Testers

Come challenge pyWars!
What keeps me up at night?

- This talk is a collection of research and attack techniques that scare me.
- Why career ending? Because this talk will reveal the full extent of my paranoia.
- Is my fear rational? You decide.
Stealing Private Keys based on Sound

- Acoustic RSA Key Extraction
  - Daniel Genkin
  - Adi Shamir
  - Eran Tromer

- [https://www.cs.tau.ac.il/~tromer/acoustic/](https://www.cs.tau.ac.il/~tromer/acoustic/)
  - 30 CM with cell phones
  - 4 meters parabolic microphones
  - "Greatly Extended range" with laser vibrometers
  - Attack can also be done from a web page using the computers build in microphone
Adi Shamir is a space alien
Backdoored SD Memory

- bunnie & xobs
- Every form of Solid State drive has a chip that is used to read and write to it
- Laptop Drives, USB Sticks, Smartphones memory
- They are programmed by this piece of software
SD Backdoors

- Can not access the phone or laptop using the device, but they don't need to!
- Can modify executables on the disk to obtain remote code execution
- Can modify data accessed by programs to create/receive beacon data from external hosts.
- Scenario: Backdoored USB drops outside Microsoft that always update targeted source code
Our phones are secretly taking naked photos of us and sending them to the iCloud!
Joshua Pitt created a tool called Backdoor Factory.

http://www.slideshare.net/midnite_runr/patching-windows-executables-with-the-backdoor-factory

It finds areas inside EXEs on disk and stuffs malware in those areas.

Legitimate program has malware inside it.
Code Caves

- Code Caves exist all over the place!!

- More difficult to find then adding a new section to the EXE file like msfvenom -k
Adolf Hitler is still alive and has been writing software compilers!
But there are other code caves!

Patched a vulnerability in VGX.DLL. A DLL used to register websites that are in “VML” format.

VML has been replace by SVG. No active development on VML since 1998.

Old functions in DLLs that aren't used any more are code caves!
Malware lives in code caves in legitimately loaded DLLs!

- DLLs listed in an uninfected CSRSS.EXE

<table>
<thead>
<tr>
<th>Image Name</th>
<th>PID</th>
<th>Modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Idle Process</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>System</td>
<td>4</td>
<td>N/A</td>
</tr>
<tr>
<td>smss.exe</td>
<td></td>
<td>ntdll.dll, CSRSRV.dll, basesrv.DLL, winsrv.DLL, USER32.dll, GDI32.dll,</td>
</tr>
<tr>
<td>csrss.exe</td>
<td></td>
<td>kernel32.dll, KERNELBASE.dll, LPK.dll, USP10.dll, msvcrtdll, sxssrv.DLL,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sxsdll, Rpcrt4.dll, CRYPTBASE.dll, ADVAPI32.dll, sechost.dll</td>
</tr>
</tbody>
</table>

- DLLs listed in an INFECTED CSRSS.EXE

<table>
<thead>
<tr>
<th>Image Name</th>
<th>PID</th>
<th>Modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Idle Process</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>System</td>
<td>4</td>
<td>N/A</td>
</tr>
<tr>
<td>smss.exe</td>
<td></td>
<td>ntdll.dll, CSRSRV.dll, basesrv.DLL, winsrv.DLL, USER32.dll, GDI32.dll,</td>
</tr>
<tr>
<td>csrss.exe</td>
<td></td>
<td>kernel32.dll, KERNELBASE.dll, LPK.dll, USP10.dll, msvcrtdll, sxssrv.DLL,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sxsdll, Rpcrt4.dll, CRYPTBASE.dll, ADVAPI32.dll, sechost.dll</td>
</tr>
</tbody>
</table>
Code caves in DLLs

- Can not be put in digitally signed DLLs

We could use DLLs that are not digitally signed

- Load it in a code cave AFTER the dll signature check has completed

- Or find some way to defeat digital signatures. That must be hard right?
C:\Windows\dir expl*.exe
Volume in drive C has no label.
Volume Serial Number is D6FA-177B

Directory of C:\Windows

03/04/2014  07:16 AM  2,088,160 explorer.exe
05/12/2014  06:25 AM  495,616 explorer.exe
  2 File(s)  2,583,776 bytes
  0 Dir(s)  48,004,001,792 bytes free

C:\Windows\tools\sigcheck.exe -h expl*.exe

Sigcheck v2.1 - File version and signature viewer
Copyright (C) 2004-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Windows\explorer.exe:
  Verified:   Signed
  Signing date:  3:03 PM 3/20/2014
  Publisher:  Microsoft Windows
  Description: Windows Explorer
  Product:  Microsoft Windows Operating System
  Prod version:  6.3.9600.17831
  File version:  6.3.9600.17831 <winblue_gdr.140221-1952>
  MachineType: 32-bit
  MD5:  119e091b5386379bc5a598ee9440c75
  SHA1:  4dca84b9ed945e08f00783344b41b5858ee088
  PESHA1:  7be80b3d92fe93f2a0a860120433b023c0796
  PE256:  9803440766aacc99bb254a9c3470e30a554464cf10fa02e86eef97029911d
  SHA256:  096f340c3c1d7fae4ec352fad3bd9a5820eca75014d06287371ba44855770f

C:\Windows\explorer.exe:
  Verified:   Signed
  Signing date:  3:03 PM 3/20/2014
  Publisher:  Microsoft Windows
  Description: Windows Explorer
  Product:  Microsoft Windows Operating System
  Prod version:  6.3.9600.17831
  File version:  6.3.9600.17831 <winblue_gdr.140221-1952>
  MachineType: 32-bit
  MD5:  119e091b5386379bc5a598ee9440c75
  SHA1:  4dca84b9ed945e08f00783344b41b5858ee088
  PESHA1:  7be80b3d92fe93f2a0a860120433b023c0796
  PE256:  9803440766aacc99bb254a9c3470e30a554464cf10fa02e86eef97029911d
  SHA256:  096f340c3c1d7fae4ec352fad3bd9a5820eca75014d06287371ba44855770f

C:\Windows>
Application Compatibility Toolkits

- Initial work by me and presented for the first time publicly at Derbycon 2012
- Demo
Jon found that SDB files has a "section" ie commands that is not configured through Compatibility Manager called patch_bits.

Patch_bits allow you do in memory patching of executables. This is how Microsoft "Fix-ups" work.

SDBEXPLORER also allows the registration if .SDB files so that they do not show up in Add/Remove Programs.

Jon patched explorer.exe, a signed executable adding new functions to the program.
EXPLORER.EXE IS USED BY BIGFOOT TO CONTROL OUR MINDS (he lives in a code cave)
As a matter of fact all of those things we can’t find are probably in code caves!!

CODE CAVE!!

WHAT HAPPENED TO JIMMY HOFFA?

The truth revealed...

CODE CAVE!!
Memory Caves??

- While experimenting with Winpmem by Johannes Stüttgen & Michael Cohen I noticed the memory dump skip several addresses when it is dumping memory.
Coloring outside the lines

▶ Can I read from addresses outside those ranges??

```python
>>> illegal_memory = readmem(fd, 0x9e000, 10000)
>>> print illegal_memory[7000:9000]
```

That interesting. But what is there?
PCI, DMA and other BIOS memory lives in RAM
You can write to this memory AFTER it has been loaded from the chip!
How we interface with hardware

- USER MODE APPLICATIONS
- KERNEL MODE APPLICATIONS
- DEVICE DRIVERS
- BUS ADAPTERS, BIOS, ETC IN MEMORY
How to avoid detection

- USER MODE APPLICATIONS
- KERNEL MODE APPLICATIONS
- DEVICE DRIVERS
- BUS ADAPTERS, BIOS, ETC IN MEMORY
- INFECTED CODE

ROOT KIT HUNTERS & MEMORY FORENSICS LOOK HERE
The internet is the pinnacle of human achievement!

- The Internet and modern technologies are AMAZING, EXTREMELY COMPLEX, and HORRIBLY FLAWED
- They are (dare I say) impossible to protect against attack
- THE BEST defense is one that detects attacks quickly and minimizes the impact of those attacks
- The Internet is the most influential and significant human creation of all times.
- THIS IS AS GOOD AS WE CAN DO!!
Do you really think we put a man on the moon?
Questions?

Twitter: @markbaggett

mbaggett@sans.org