Host-Based Censorware

• Network-based censorship is *hard*
  – Thanks to Tor bridges and other evasion tools!

• Censors trying to strike a fine balance
  – Major restrictions (eg. whitelisting) = angry users
  – Whack-a-mole network filtering = leaky sieve

• “Hey, let's push down the censorship functionality to the end host!”
Green Dam Youth Escort

• Host-based censorship software introduced by the Chinese government

• Originally mandated to be installed on all personal computers purchased in China
Green Dam Features

• Content / text filter
  – Blocking political and adult content

• Networking filtering for URLs / keywords
  – Blacklists stolen from Cybersitter software

• Image pornography filtering
  – OpenCV skin tone detection heuristics

• Bonus “features”
  – Trivial stack smashes via long URL

• Great report from my U of M colleagues
  – http://www.cse.umich.edu/~jhalderm/pub/gd/
Technical Operation

- Lots o' interposition!
- SetWindowsHookEx hooks
  - WH_MOUSE, WH_KEYBOARD, WH_GETMESSAGE
- Winsock LSP hooks
  - eg. DBFP_Recv in SurfGd.dll
- Remote process DLL injection
  - eg. InjLib32.dll / HAServ.dll
- Select processes targeted
  - iexplore.exe, notepad.exe, winword.exe, qq.exe, outlook.exe, msgmsgr.exe, etc
Ring-3 Hooking

• API hooking in userspace
  – Usually used in crappy “rootkits”, spyware, etc
  – IAT patching / jmp code overwriting

• Traditionally done with “viral” hooking
  – Inject into all running processes (CreateRemoteThread)
  – Hook CreateProcess routines
  – New processes will be auto-injected/hooked

• We're on a level playing field
  – Oh, you just injected yourself into Firefox?
  – I'll follow you in and undo everything you just did!
• The Dam Burst tool
  – Instead of pwn'ing Green Dam users, let's actually help the users who may face censorship.
  – Disables Green Dam without administrative access (eg. internet cafes, public computers)
  – Transient, in-memory patching (avoid persistent system changes)
  – Closes off the vulnerable Green Dam routines
In-Process Memory Patching

• Injection:

**VirtualAllocEx()**
allocate memory in remote process

**VirtualProtectEx()**
make remote memory writeable

**WriteProcessMemory()**
inject our code

  LoadLibrary(“damburst.dll”)
  burst = GetProcAddress(“Burst”)
  Call burst

**VirtualProtectEx()**
restore memory protection

**CreateRemoteThread()**
execute injected code

• Patching:

**Neuter Winsock LSP hooks**

  addr = GetProcAddress(“DBFP_*”)
  VirtualProtect(addr)
  memcpy(addr, NOP)
  VirtualProtect(addr)
  FlushInstructionCache(addr)

**Disable API hooks / SetWindowsHookEx**

  GetModuleHandle(“InjLib32.dll”)
  GetProcAddress(“InjectLibrary”)
  InjectLibrary(FALSE) // HA!

**Unload Green Dam**

  FreeLibrary(“Handler.dll”)
  FreeLibrary(“InjLib32.dll”)

Jon Oberheide - Green Dam - DEFCON 18
### Demo

**Green Dam - DEFCON 18**

#### Process Table

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Green Dam</th>
<th>PID</th>
<th>Start Time</th>
<th>CPU Time</th>
<th>Memory Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMwareTray</td>
<td>Disabled</td>
<td>824</td>
<td>10:26 PM</td>
<td>0.02</td>
<td>37524k</td>
</tr>
<tr>
<td>VMwareAux</td>
<td>Disabled</td>
<td>888</td>
<td>10:26 PM</td>
<td>0.15</td>
<td>17632k</td>
</tr>
<tr>
<td>xNet2</td>
<td>Enabled</td>
<td>856</td>
<td>10:26 PM</td>
<td>0.18</td>
<td>31244k</td>
</tr>
<tr>
<td>ommon</td>
<td>Disabled</td>
<td>1012</td>
<td>10:26 PM</td>
<td>0.09</td>
<td>3234k</td>
</tr>
<tr>
<td>DamBust</td>
<td>Enabled</td>
<td>1244</td>
<td>2:27 AM</td>
<td>0.17</td>
<td>18524k</td>
</tr>
<tr>
<td>explorer</td>
<td>Disabled</td>
<td>1544</td>
<td>10:26 PM</td>
<td>0.21</td>
<td>21324k</td>
</tr>
<tr>
<td>TSVNCache</td>
<td>Disabled</td>
<td>1988</td>
<td>10:26 PM</td>
<td>0.02</td>
<td>4204k</td>
</tr>
<tr>
<td>XDemon</td>
<td>Enabled</td>
<td>1396</td>
<td>10:27 PM</td>
<td>0.13</td>
<td>3664k</td>
</tr>
<tr>
<td>mx</td>
<td>Disabled</td>
<td>2364</td>
<td>2:27 AM</td>
<td>0.09</td>
<td>42145k</td>
</tr>
<tr>
<td>notepad</td>
<td>Disabled</td>
<td>2364</td>
<td>2:27 AM</td>
<td>0.09</td>
<td>42145k</td>
</tr>
<tr>
<td>procsp</td>
<td>Disabled</td>
<td>3048</td>
<td>2:27 AM</td>
<td>0.05</td>
<td>19324k</td>
</tr>
</tbody>
</table>

#### Process List

- DBFilter.dll
- InjLib32.dll
- Handler.dll
- SutiGd.dll

**Search Results**

- **porn**

  ![Google Search](https://www.google.com)
  - About 327,000,000 results (0.15 seconds)
Green Dam Defeated, But...

• An initial attempt at host-based censorware
  – Executed pretty poorly
  – Subsequent attempts will learn from Green Dam's mistakes

• We'll undoubtedly see more in the future...
  – Driven by proliferation of tools like Tor that effectively evade network-based censorship