Getting Windows to Play with Itself
A Hacker’s Guide to Windows API Abuse

Brady Bloxham
Founder/Principal Security Consultant
@silentbreaksec
http://www.silentbreaksecurity.com
http://www.blacksquirrel.io
Background

- Shorten the gap between penetration test and actual attack
- Few covert persistence tools
- Reduce reliance on Metasploit
Got a lot to cover

- DLL Injection
- Persistence
- Throwback
- Lots of demos along the way
DLL Injection

• Traditional methods
  • CreateRemoteThread()
  • NtCreateThreadEx()
  • RtlCreateUserThread()
  • NtQueueApcThread ()
    • Can blue screen certain OSes
• Code Cave
  • Suspend process
  • Inject code
  • Change EIP to location of injected code
  • Resume process
  • Difficult on x64
AddMonitor()

- +
  - Injects into spoolsv.exe
  - Doesn’t require matching architecture
  - Easy to use
- -
  - Dll must be on disk
  - Requires administrator privs

The `AddMonitor` function installs a local port monitor and links the configuration, data, and monitor files.

### Syntax

```c++
BOOL AddMonitor(
    _In_  LPTSTR pName,
    _In_  DWORD Level,
    _In_  LPBYTE pMonitors
);
```
Dll Injection Demo
Persistence

• Lots of persistence in Windows
  • Service
  • Run keys
  • Schtasks
  • ...
• And lots still to find...
• Lots of techniques
  • Process monitor
  • Hook LoadLibrary()
Persistence

1st Technique

- Requires VMware Tools be installed
- Just drop a dll to disk
- `c:\windows\system32\wbem\ntdsapi.dll`
- Note: Dll must export same functions as real ntdsapi.dll

2nd Technique

- VMware patched in ESXi 5.5
- Requires VMware Tools be installed
- Just drop a dll to disk
- `c:\windows\system32\wbem\tpgenlic.dll`
- `c:\windows\system32\wbem\thinmon.dll`
Persistence

• 3rd "Technique"

• HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors"

• Create a new key"

• Create a new value named "Driver" with "the" dll name

• Create as many as you like
Persistence Demo
Windows API HTTP Cheatsheet

• WinHTTP
  • Intended for services
  • Does not pull user proxy settings
  • Supports impersonation

• WinINet
  • More robust in proxy environment
    • Variety of flags that enable/disable functionality automatically
  • Prompts user for password if authentication is required
  • Uses IE settings
What is Throwback?

- C++ HTTP/S beaconing backdoor
- PHP control panel w/ MySQL backend
- Built for stealth
- Persistence built-in
  - DII
  - Exe
Throwback Features

• Robust proxy detection
• Distributed LPs
• Uses MSGRPC to generate MSF payloads
• RC4 encrypted comms
• Implements reflective dll injection
• String encryption
<table>
<thead>
<tr>
<th>Status</th>
<th>Version</th>
<th>IP Address</th>
<th>Target Name</th>
<th>Callback Period</th>
<th>Last Callback</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2.50</td>
<td>192.168.20.183</td>
<td>IETEMPLATE</td>
<td>1 minutes</td>
<td>Aug 5, 2014 4:04 pm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.50</td>
<td>192.168.20.1</td>
<td>IE11TEMPLATE</td>
<td>1 minutes</td>
<td>Aug 4, 2014 10:35 pm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.16</td>
<td>192.168.20.1</td>
<td>IE10TEMPLATE</td>
<td>1 minutes</td>
<td>Aug 2, 2014 12:28 am</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.16</td>
<td>192.168.20.112</td>
<td>IE9TEMPLATE</td>
<td>10 minutes</td>
<td>Aug 1, 2014 5:55 pm</td>
<td></td>
</tr>
</tbody>
</table>
Throwback Demo
Going Forward...

• Community based project!!!

• Create modules
  • Keylogger, Mimikatz, Hashdump, etc.
  • Various transport methods

• Additional persistence techniques

• Modification of comms
The End Shameless Plug

- Interested in writing custom malware/backdoors?
  - Dark Side Ops: Custom Penetration Testing
  - Blackhat Europe and East Coast Trainings

- Pen test networks from your browser
  - https://www.blacksquirrel.io

- Silent Break Security
  - Blackbox/Red Team Pen Testing
  - brady@silentbreaksecurity.com
  - @silentbreaksec
  - https://github.com/silentbreaksec