Topics

- Malware Analysis Patterns
- Malware Modeling
- Injection Residue
- Example
Malware Patterns

Malware:
software that uses planned alteration of structure and behaviour of software to serve malicious purposes.

Malware analysis patterns:
intentional abnormal software structure and behavior patterns
Real scenario:

Simplified modeling scenario:

Coding post-attack effects
DLL Injection Example

LPWSTR szDLL = L"\winspool.dll";

int main(int argc, WCHAR* argv[]) {
  for (int i = 0; i < 100; ++i)
    _beginthread(thread, 0, (void *)INFINITE);

  Sleep(10000);

  CreateRemoteThread (GetCurrentProcess(), NULL, 0, reinterpret_cast<LPTHREAD_START_ROUTINE>(LoadLibraryW), szDLL, 0, NULL);

  Sleep(INFINITE);

  return 0;
}

// winspool.dll

BOOL APIENTRY DllMain( HMODULE hModule, DWORD ul_reason_for_call, LPVOID lpReserved)
{
  switch (ul_reason_for_call)
  {
    case DLL_PROCESS_ATTACH:
    case DLL_THREAD_ATTACH:
      StartSpying();  // calls CreateFile(L"RedOctober.dll", …);
      Sleep(INFINITE);
      break;
    case DLL_THREAD_DETACH:
    case DLL_PROCESS_DETACH:
      break;
  }

  return TRUE;
}
Injection Residue

Execution Residue:

Data Residue

00000000`08d4f2c0 00000000`005381f0 ""
00000000`08d4f2c8 000007fe`f6e3e248 ".\RedOctober.dll"
00000000`08d4f2d0 00000000`00000000

Call Footprint

00000000`08d4f2c0 00000000`005381f0
00000000`08d4f2c8 000007fe`f6e3e248 winspool+0xe248
00000000`08d4f2d0 00000000`00000000
00000000`08d4f2d8 00000000`00000000
00000000`08d4f2e0 00000000`00000000
00000000`08d4f2e8 00000000`76bf18ed kernel32!CreateFileWImplementation+0x7d
00000000`08d4f2f0 00000000`00000000

[...]
00000000`08d4f340 00000000`08d4f3d0
00000000`08d4f348 000007fe`fd4e1203 KERNELBASE!SleepEx+0x7d
00000000`08d4f350 00000000`08d4f408
<table>
<thead>
<tr>
<th>Date</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 1–4, 2013</td>
<td>Accelerated Windows Malware Analysis</td>
</tr>
<tr>
<td>February 20-25, 2013</td>
<td>Accelerated Windows Memory Dump Analysis</td>
</tr>
<tr>
<td>March, 25, 2013</td>
<td>Malware Narratives (FREE)</td>
</tr>
<tr>
<td>April, 26-29, 2013</td>
<td>Accelerated Windows Debugging³</td>
</tr>
<tr>
<td>2013</td>
<td>Philosophy of Software Diagnostics (FREE)</td>
</tr>
<tr>
<td>2013</td>
<td>The New Old Debugging</td>
</tr>
</tbody>
</table>

Debugging³ Now Available for Booking

© 2013 Software Diagnostics Institute
Debugging.TV

Now on YouTube!

http://www.youtube.com/DebuggingTV