The Role of Malware Analysis in Incident Response
Who We Are

• Rob Kraus
  – Director of Research, Solutionary Security Engineering Research Team (SERT)
  – RobKraus@Solutionary.com
  – Twitter: @robkraus

• Jeremy Scott
  – Research Analyst, Solutionary Security Engineering Research Team (SERT)
  – JeremyScott@Solutionary.com
  – Twitter: @jeremyscott_org
Incident Response Phases

- Preparation
- Detection and Analysis
- Containment, Eradication and Recovery
- Post-Incident Activity
Where Malware Analysis Fits

• Detection and analysis

• Is that the only place?
  – Preparation
  – Training
  – Equipment
  – Containment, Eradication and Recovery
  – Understanding the attack
  – Post-Incident Activity
  – Reports
  – Information sharing
Why Malware Analysis?

- Important step in incident response
- Extent of attack and compromise
- Identify technical indicators
Technical Indicators

• Identify possible compromise or infection

www.badguymalwaredomain.com

MD5: 5f22df635217319439ea56e056b617a

Executive bonuses - 2012.pdf

127.0.0.1

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

GET www.malwarehost.com/secondarypayload.zip

SpoofedEmail@yourdomain.com
Malware Analysis

- **Static analysis**
  - Basic
  - Advanced

- **Dynamic analysis**
  - Basic
  - Advanced
Basic Static Analysis

• **Results in identification of simple indicators**
  – File name
  – MD5 hash
  – File type
  – Virus detection
Basic Dynamic Analysis

- **Additional indicators**
  - Domain names
  - IP addresses
  - Registry keys
  - Additional files
  - Download more malware
Advanced Static Analysis

• Take it one step further
• Additional details

```
pop ecx
mov esi, offset aAcceptLanguage ; "Accept-Language: en-gb\r\n"
rep movsd
movsb
push 11h
mov ecx, ebx
lea esi, [ebx+42h]
call sub_460800
push eax
push esi
push 8
mov ecx, ebx
call sub_403800
push eax
push 0Ah
mov ecx, ebx
call sub_4037A5
push eax
push esi
lea eax, [ebx+10h]
push eax
push eax
push offset aHttpDevice_S_ ; "http://%s/device_%s.asp?device_t=%s&key"
push dword ptr [ebx+94h] ; Dest
call sprintf
add esp, 20h
push dword ptr [ebx+98h] ; int
mov ecx, ebx
push 0 ; int
push dword ptr [ebx+94h] ; Source
call request file
```
Advanced Dynamic Analysis

- Another way to extract detailed information

```
00402890  50  PUSH EAX
00402891  56  PUSH ESI
00402892  6A 08  PUSH 8
00402894  8BCB  MOV ECX, EBX
00402896  E8 650F0000  CALL iTunesHe.00403800
0040289B  50  PUSH EAX
0040289C  6A 0A  PUSH 0A
0040289E  8BCB  MOV ECX, EBX
004028A0  E8 000F0000  CALL iTunesHe.004037A5
004028A5  50  PUSH EAX
004028A6  56  PUSH ESI
004028A7  8D43 10  LEA EAX, [EBX+10]
004028AA  50  PUSH EAX
004028AB  68 3C784000  PUSH iTunesHe.0040783C
004028B0  FFB3 9400000  PUSH DWORD PTR [EBX+94]
004028B6  E8 ED370000  CALL <jmp,&MSVC90.sprintf>
004028BB  83C4 20  ADD ESP, 20
004028BE  FFB3 9800000  PUSH DWORD PTR [EBX+98]
004028C4  8BCB  MOV ECX, EBX
004028C6  6A 00  PUSH 0
004028C8  FFB3 9400000  PUSH DWORD PTR [EBX+94]
```

---

<s>"www.BusinessForMars.com/Resource"</s>
<s>"STL"</s>
<s>"www.BusinessForMars.com/Resource"</s>
format = "http://<s>/device_%s.asp?device_t=<s>&key=<s>&s=00F70DA0"<s>

<s>sprintf</s>
Where to Start

• **Two approaches**
  – Host-based
  – Network-based
Host-based

- Malware analysis and reverse engineering
  - Starting with the suspicious files
Network-based

- Network forensics and reverse engineering
  - Starting with logs and packet captures
How Solutionary Uses Technical Indicators
Response Scenario
Basic Static

C:\Documents and Settings\Solutionary VM User\Desktop>md5sum badfile.exe
a5cdaa71b517c8b260a36085c810c38e *badfile.exe

<table>
<thead>
<tr>
<th>pFile</th>
<th>Data</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000F4</td>
<td>014C</td>
<td>Machine</td>
<td>IMAGE_FILE_MACHINE_I386</td>
</tr>
<tr>
<td>000000F6</td>
<td>0005</td>
<td>Number of Sections</td>
<td></td>
</tr>
<tr>
<td>000000F8</td>
<td>4FAFF060</td>
<td>Time Date Stamp</td>
<td></td>
</tr>
<tr>
<td>000000FC</td>
<td>00000000</td>
<td>Pointer to Symbol Table</td>
<td></td>
</tr>
<tr>
<td>00000100</td>
<td>00000000</td>
<td>Number of Symbols</td>
<td></td>
</tr>
<tr>
<td>00000104</td>
<td>000F</td>
<td>Size of Optional Header</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2012/05/13 Sun 17:33:20 UTC</td>
</tr>
</tbody>
</table>

Image file:
- IMAGE_FILE_RELOCS_STRIPPED
- IMAGE_FILE_EXECUTABLE_IMAGE
- IMAGE_FILE_32BIT_MACHINE

PEiD v0.94

File: C:\Documents and Settings\Solutionary VM User\Desktop\badfile.exe
Entry point: 0000A181
File offset: 00009581
Linker Info: 9.0

EP Section: .text
First Bytes: E8,1E,FF,FF
Subsystem: Win32 GUI

Nothing found [ZIP SFX]*
Basic Dynamic
Advanced Static
How Do You Eat an Elephant?
Questions?