Balancing the Pwn Trade Deficit Series: APT Secrets in Asia

{Anthony Lai,Benson Wu,Jeremy Chiu} Xecure Founder and Researcher
PK, Security Researcher

There is no national secret here ☺

We welcome spies and SS here.
Spies/SS are human, too :)

Why we are here again

- Last year, Val Smith, Colin Ames and I (Anthony) have worked together on analyzing China-made malware, making first east-meets-west research and studies. We continue this effort.
- This year, we have dealt with many targeted attack cases, we would like to share the case studies with you and the correlation analysis with my Taiwanese research fellows.
- We are happy about this presentation is accepted in first-round selection of DEFCON 19, however, it is rejected in Blackhat with reviewer comment: " *We are curious about your automated analysis*." - Thank you for their comment ;-)

Who we are?

- **Anthony Lai (a.k.a Darkfloyd)**
  - He works on code audit, penetration test, crime investigation and threat analysis and acted as security consultant in various MNCs. His interest falls on studying exploit, reverse engineering, analyse threat and join CTFs, it would be nice to keep going and boost this China-made security wind in malware analysis and advanced persistent threat areas.
  - He found security research group called VXRL in Hong Kong and has been working as visiting lecturer in HK Polytechnic University on hacking course :)
  - Spoken at Blackhat USA 2010, DEFCON 18 and Hack In Taiwan 2010/2011

- **Benson Wu**
  - He currently works as Postdoctoral Researcher from Research Center for Information Technology Innovation at Academia Sinica in Taiwan.
  - He focuses research on malware and threat analysis, code review, secure coding and SDLC process implementation. He graduated from National Taiwan University with PhD degree in Electrical Engineering. He had spoken at NIST SATE 2009, DEFCON 18 (with Birdman), OWASP China 2010, and wrote the "Web Application Security Guideline" for the Taiwan government.

- **Jeremy Chiu (a.k.a Birdman)**
  - He has more than ten years of experience with host-based security, focusing on kernel technologies for both the Win32 and Linux platforms. In early 2001 he was created Taiwan's first widespread trojan BirdSPY. The court dropped charges after Jeremy committed to allocate part of his future time to assist Taiwan law enforcement in digital forensics and incidence response.
  - Jeremy specializes in rootkit/backdoor design. Jeremy also specializes in reverse engineering and malware analysis, and has been contracted by law enforcements to assist in forensics operations. Jeremy is a sought-after speaker for topics related to security, kernel programming, and object-oriented design

- **PK**
  - Peikan (aka PK) has intensive computer forensic, malware and exploit analysis and reverse engineering experience. He has been the speaker in Syscan and HIT (Hack In Taiwan) and convey various training and workshop for practitioners.

Agenda

- APT Vs Malware
- Case Studies
- Research Methodology
- Clustering Analysis and Results

Abstract

- APT (Advanced Persistent Threat) means any targeted attacks against any specific company/organization from an or/and a group of organized attack party(ies).
- Other than providing the case studies, we would like to present and analyze APT from the malicious email document, throughout our automated analysis, we could identify and cluster the correlation among the samples featured with various exploit, malware and Botnet .

Major APT Activity: Targeted-Attack Email

- We have observed there are three major types of Targeted-Attack Email：
  1. Phishing mail: Steal user ID and password
  2. Malicious script: Detect end-use computing environment
  3. Install and deploy Malware (Botnet) !

APT Mail = Document Exploit + Malware

APT Attack Vs Traditional Botnet Activities

	APT Botnet Activities	Traditional Botnet Activities
Distribution	With organized planning	Mass distribution over regions
Cause damage?	No	No
Targeted or not?	Targeted (only a few groups/organizations)	Not targeted (large area spreadout)
Target Audience	Particular organization/company	Individual credentials including online banking account information
Attack Effective Duration	Long duration	Relative Short
Frequency of attacks	Many times	Once or twice
Weapon	• 0-day Exploit • Drop Embedded Malware	• Use existent multiple exploits • URL Download Malware
AV Detection Rate	Detection rate is lower than 10% if the sample comes out within one month	Detection rate is around 95% if the sample comes out within one month

Remarks: IPS, IDS and Firewall cannot help and detect in this area

Part 1:
Case Studies:
Against a Political Party in Hong Kong

Case 1: Calling from Mr. X

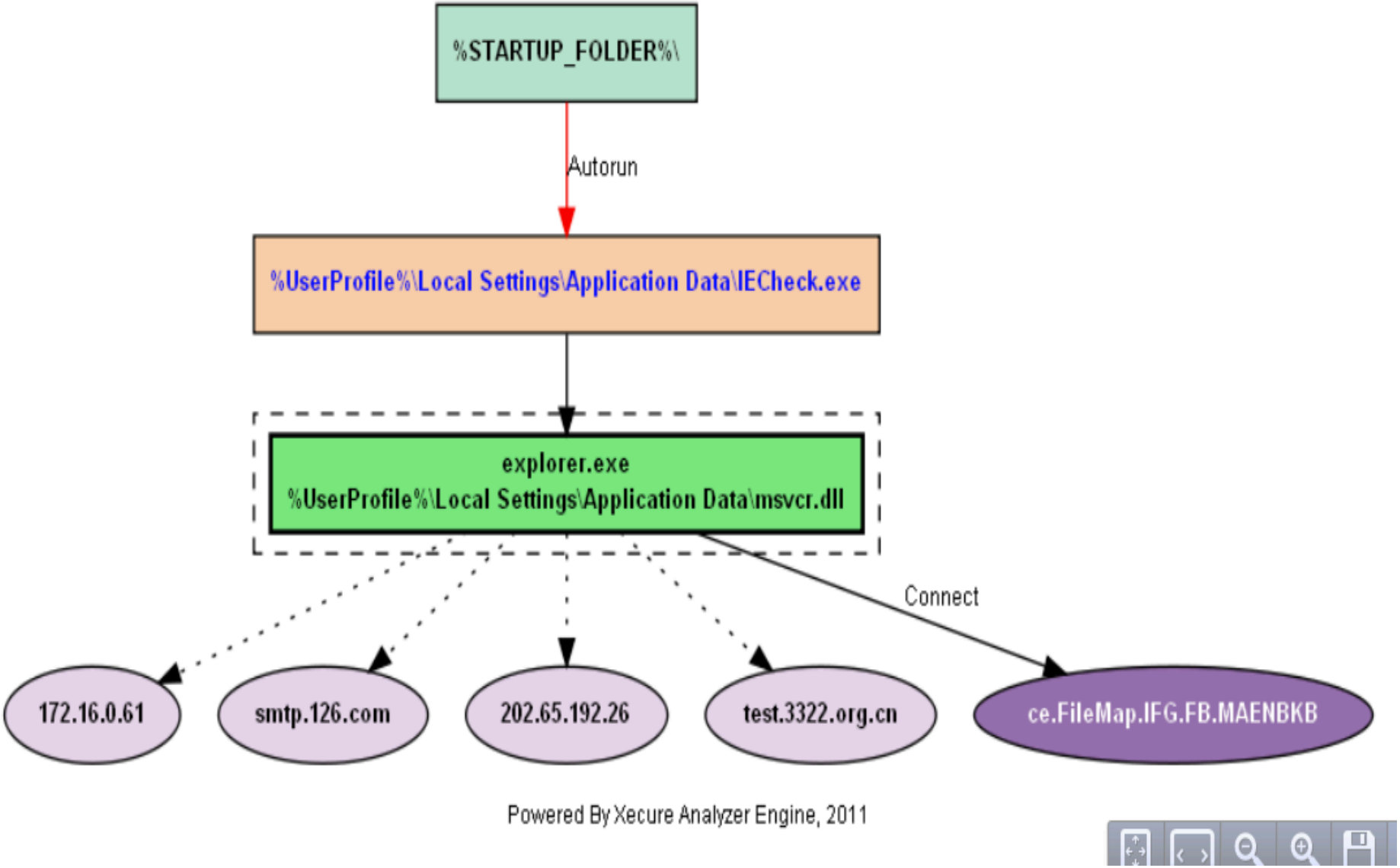
- Mr. X is a one of the key persons of political party in Hong Kong.
- He dropped us an email as he feels suspicious on an attachment called meeting.zip and it contains two files, agenda.doc and minutes.doc
- It looks like a member meeting agenda.
- The email targets all committee members in his organization.
- Mr. X said he always got this kind of mails before 4 June, 1 July and election.

Xecure Lab

Analysis

- Running analysis in our Xecure analyzer engine
- Basically, it is not a fake.doc but a PE file and minutes.doc is a document shortcut .lnk file which triggers to execute agenda.doc

Xecure Analyzer Engine



%UserProfile%\Local Settings\Application Data\IECheck.exe
(D24BB2618C181EFF733801BAFF14D4AF)

Malware Family	
Build Time	2011-05
Malware Type	**China Spyware**
Severity	
Behavior	• **This Malware has been identified the following behavior: DLL-Injection (Target: explorer.exe), Fake Program functions.**
Modules	• Base=02470000 Size=00039000 explorer.exe
Files	• [EXE] **%UserProfile%\Local Settings\Application Data\IECheck.exe** (Copyright (C) Microsoft Corp. 1997-2005) D24BB2618C181EFF733801BAFF14D4AF • [DLL] **%UserProfile%\Local Settings\Application Data\msvcr.dll** (Microsoft) 2353BD4D09909CFB672814E0D40FEE4E
Autoruns	• %STARTUP_FOLDER%\
Network	• 172.16.0.61 • 202.65.192.26 • ce.filemap.ifg.fb.maenbkb • smtp.126.com • test.3322.org.cn

Analysis - CnC location

- Connect to remote IP address in Hong Kong at 8080 port.
- It is still alive ☺

Analysis – CaptureBAT

Recorded in chronological order
C:\Documents and Settings\Administrator\Local Settings\Application Data\ws2help.PNF was added by “Agenda.doc”
C:\Documents and Settings\Administrator\Local Settings\Application Data\msvcr.dll was added by “Agenda.doc”
C:\WINDOWS\system32\netstat.exe was [written/accessed] by “Agenda.doc”
C:\WINDOWS\inf\1.txt was deleted by “Agenda.doc”
C:\WINDOWS\system32\netstat.exe was modified by “Agenda.doc”

C:\Documents and Settings\Administrator\Local Settings\Application Data\IECheck.exe was added by “Agenda.doc”
C:\WINDOWS\system32\ipsecstap.dat was added by “explorer.exe”
C:\Documents and Settings\Administrator\Start Menu\Programs \Startup\Internet Explorer Security Check.lnk was added by “explorer.exe”

Analysis - Regshot

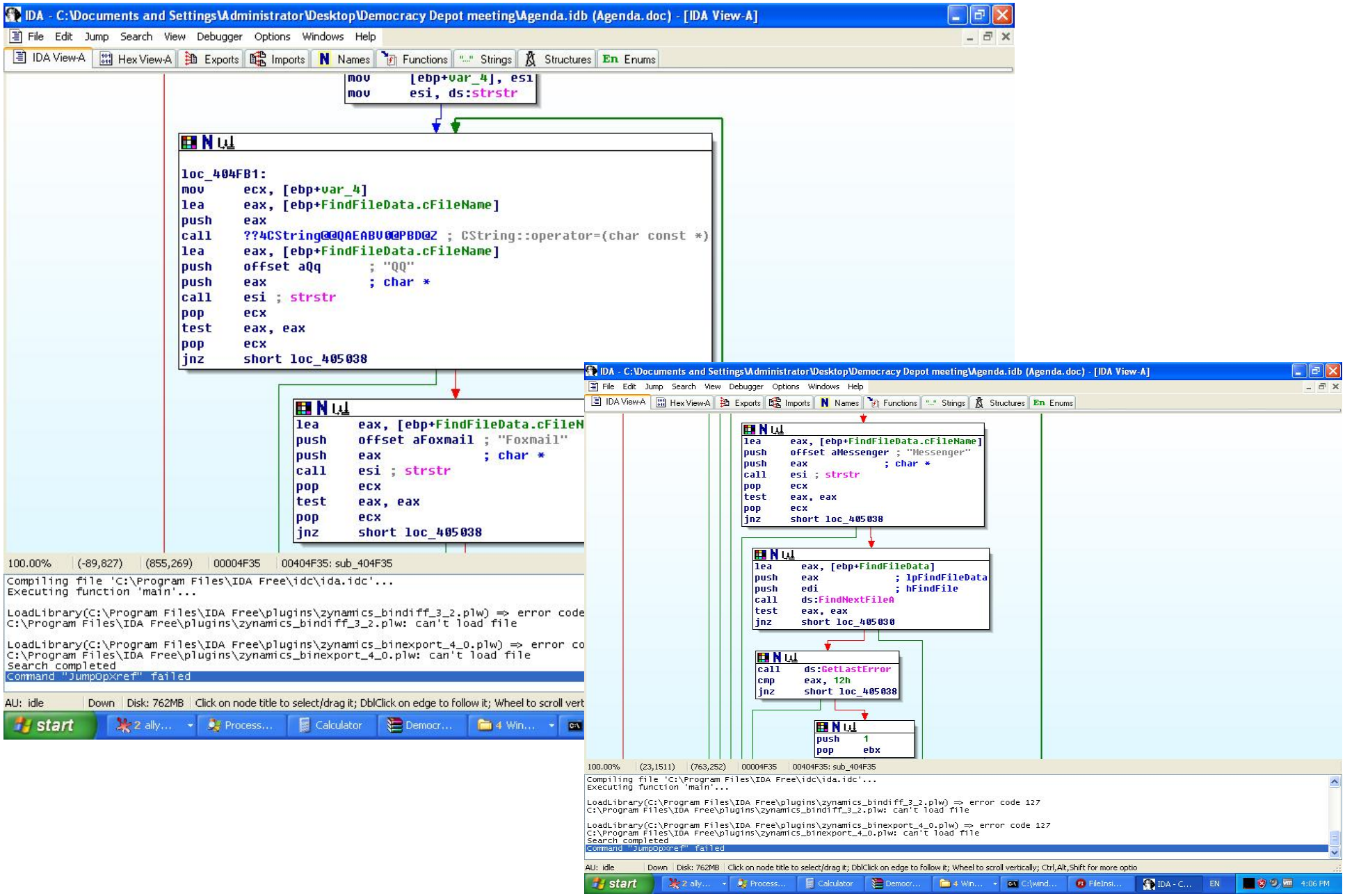
Files added

C:\Documents and Settings\Administrator\Local Settings\Application Data\IECheck.exe
C:\Documents and Settings\Administrator\Local Settings\Application Data\msvcr.dll
C:\Documents and Settings\Administrator\Local Settings\Application Data\ws2help.PNF
C:\Documents and Settings\Administrator\My Documents\My Pictures_@D.tmp
C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\Internet Explorer Security Check.lnk
C:\WINDOWS\system32\2525
C:\WINDOWS\system32\ipsecstap.dat

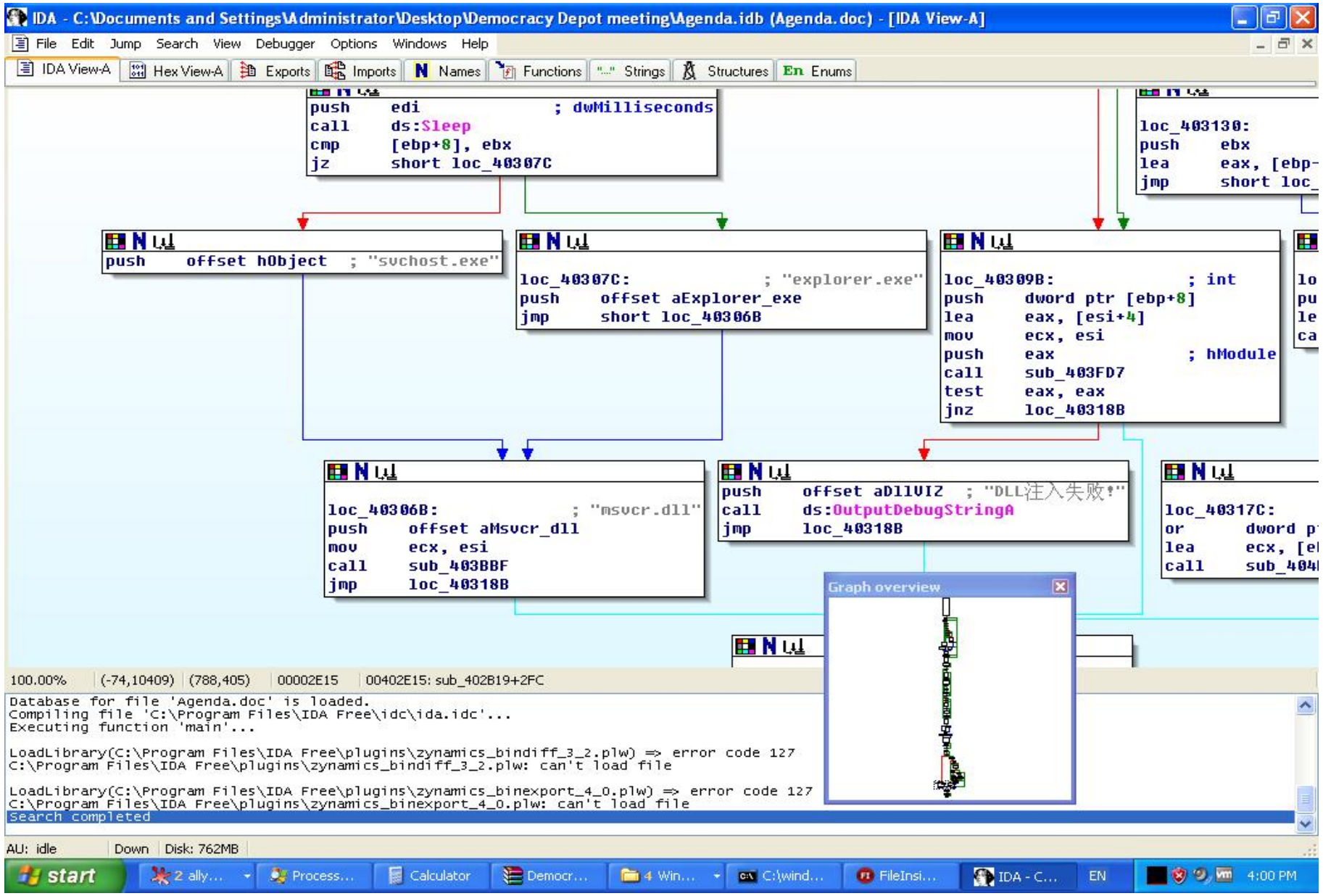
Files deleted

C:\Documents and Settings\Administrator\Desktop\Democracy Depot meeting\Sample\Agenda.doc

Analysis - Target popular IM and emails



Analysis - Injection to explorer.exe

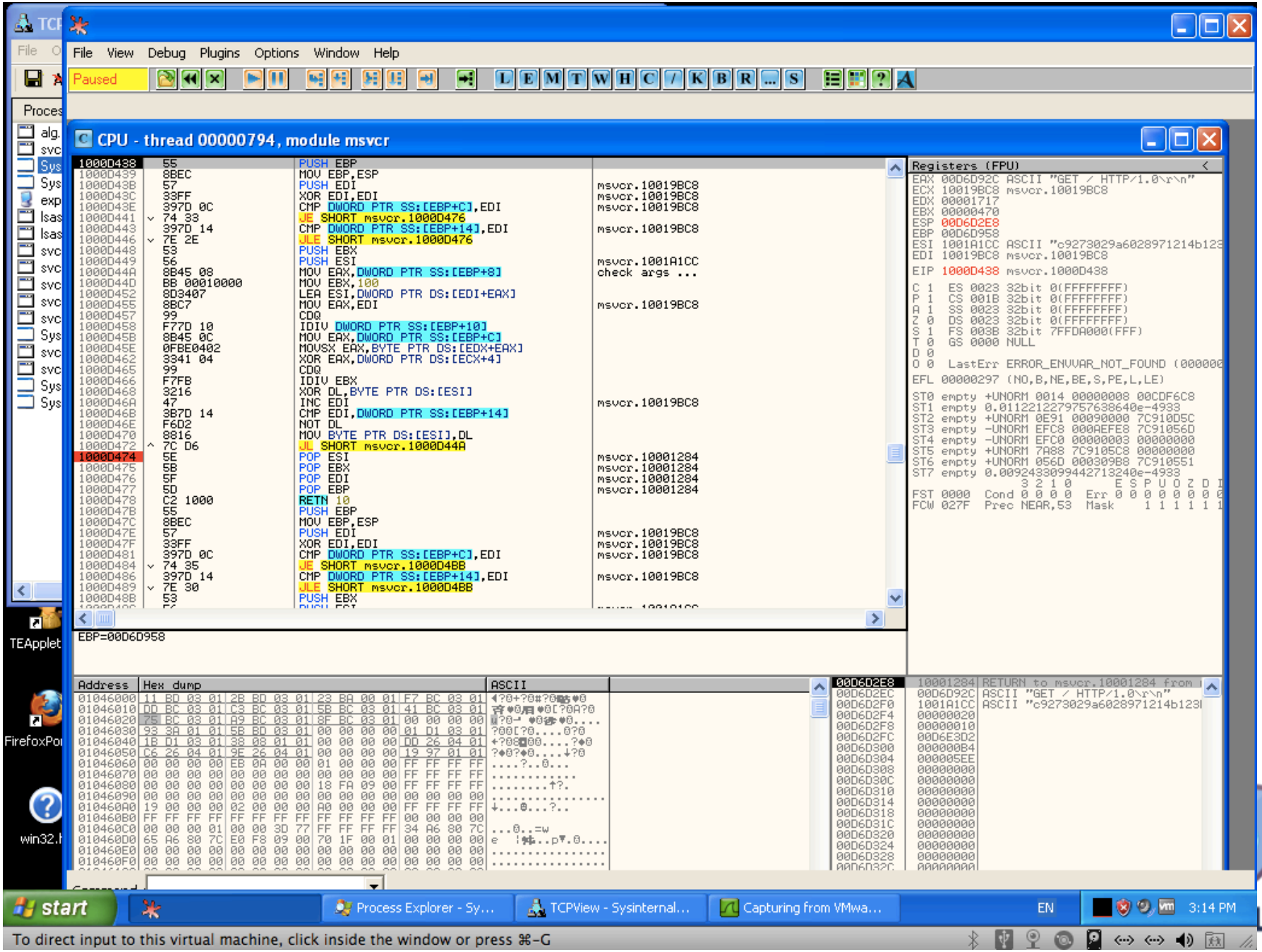


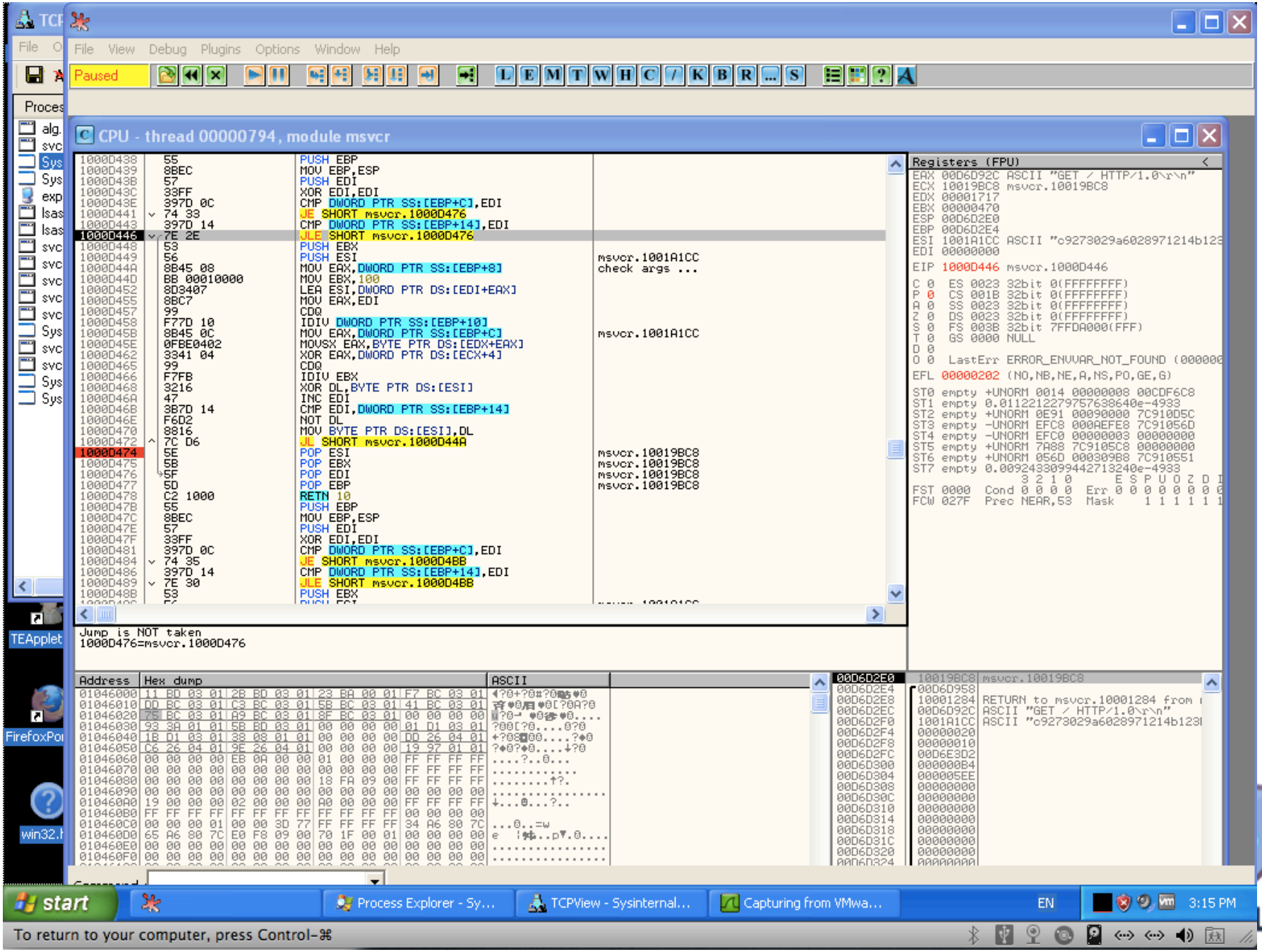
Infection Path

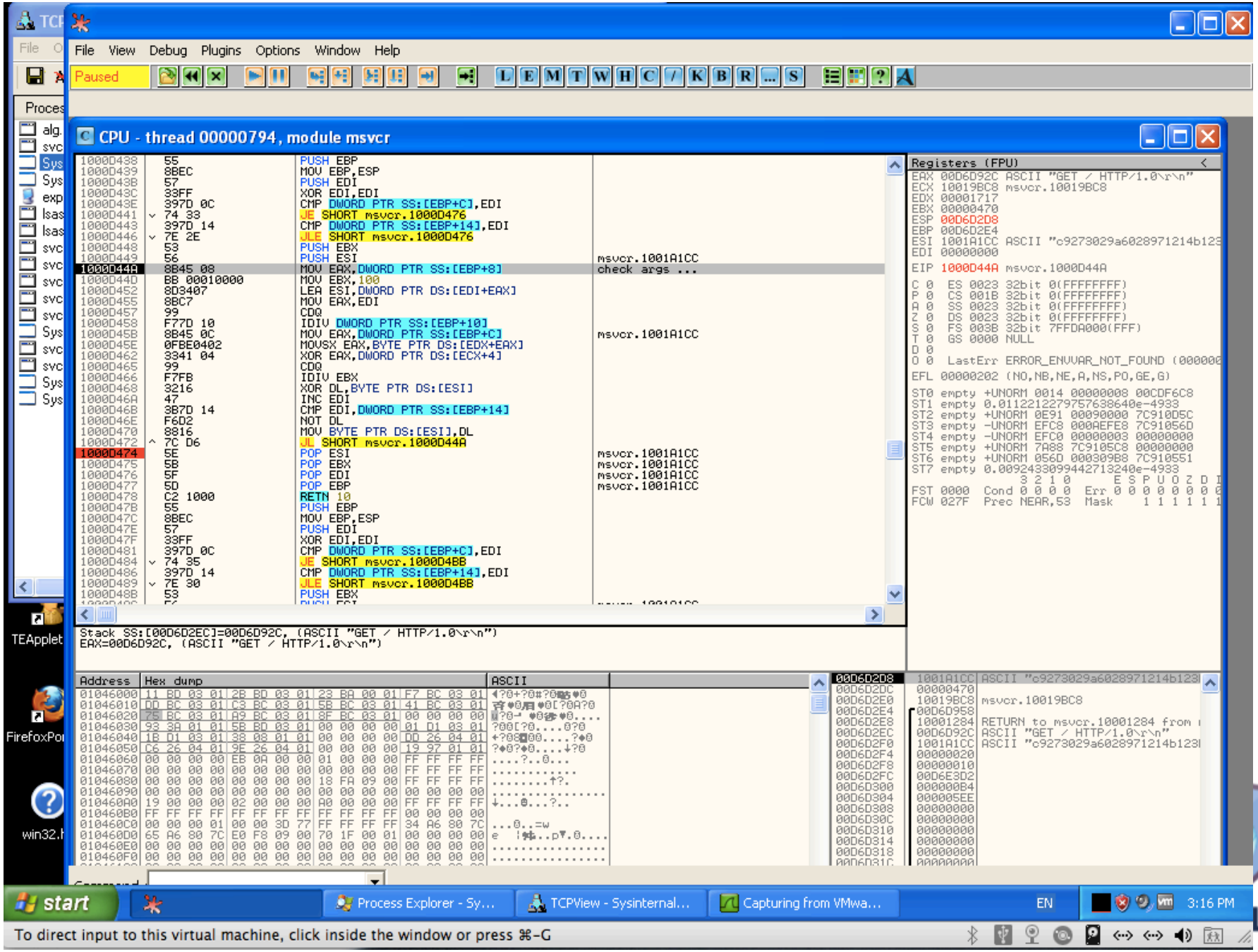
- Agenda.doc (Dropper)
  - Create IECheck.exe
  - Copy WS2Help.PNF to application data folder.
  - Change netstat.exe
  - Inject code to msvcr.dll and then to explorer.exe
  - Creat mutux (VistaDLL Running)
  - Detect anti-virus program including Kapersky
  - Target QQ, MSN, sina, foxmail and hotmail

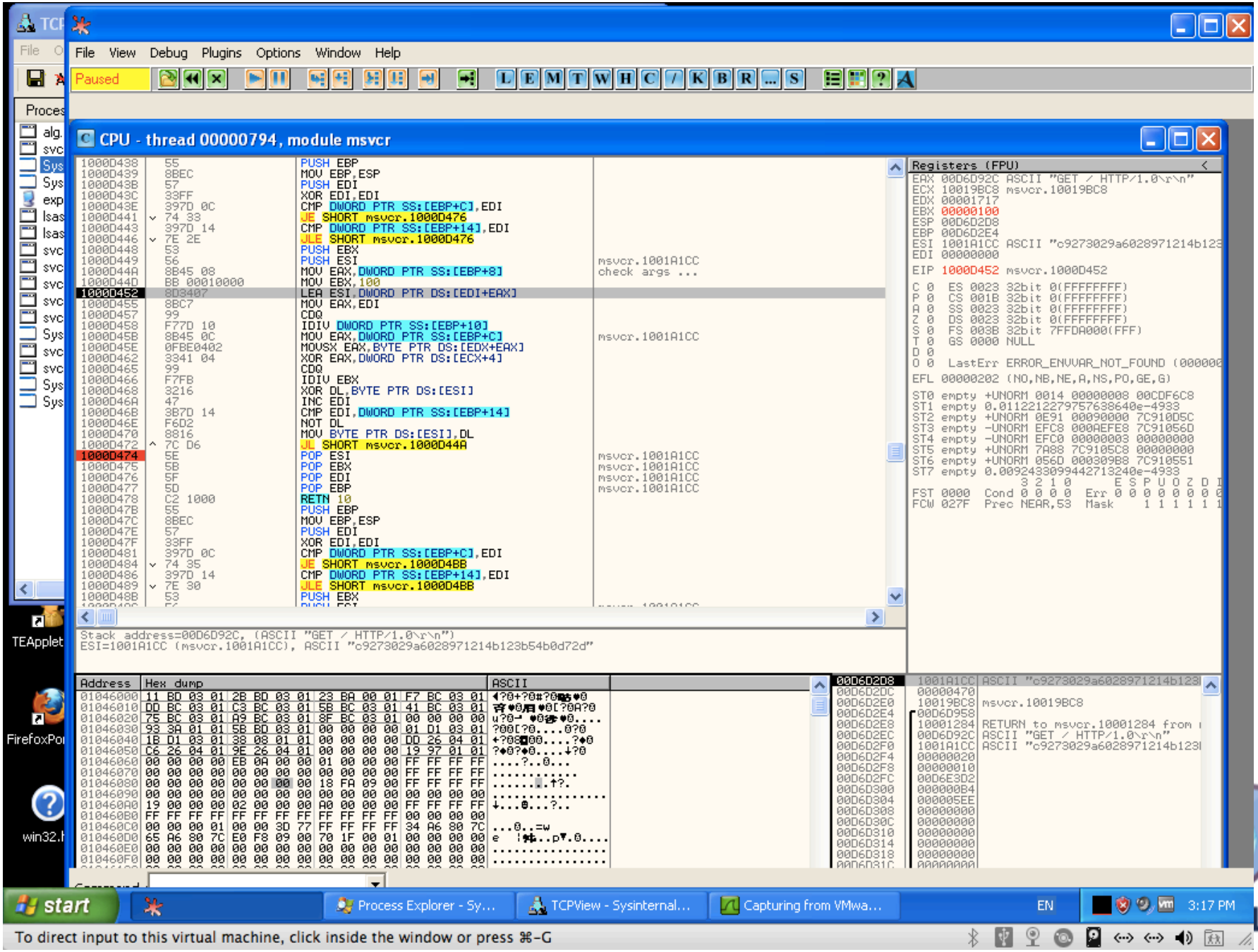
Analysis - Encoding Scheme

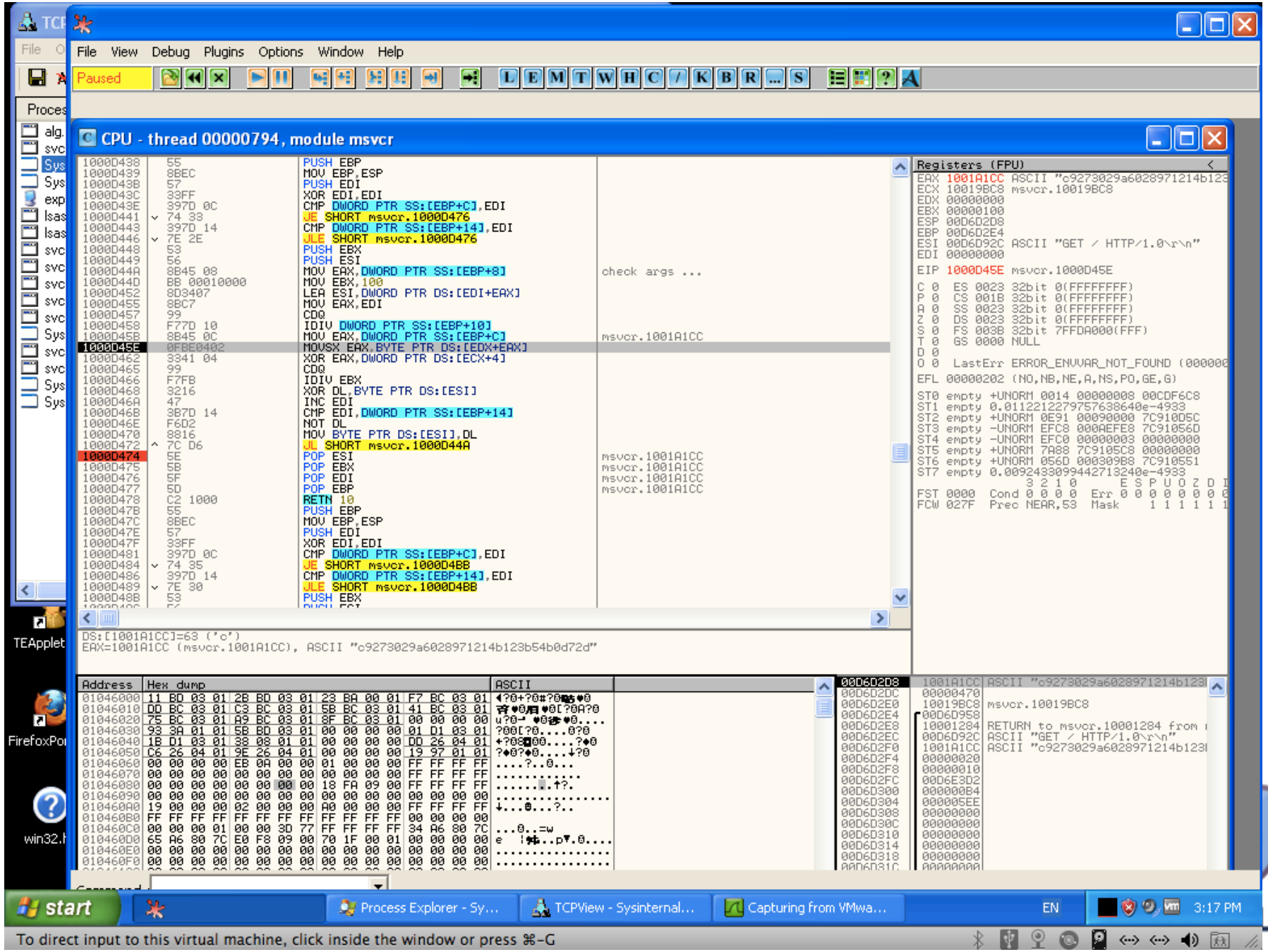
- XOR encoding only
- Encode and decode the traffic

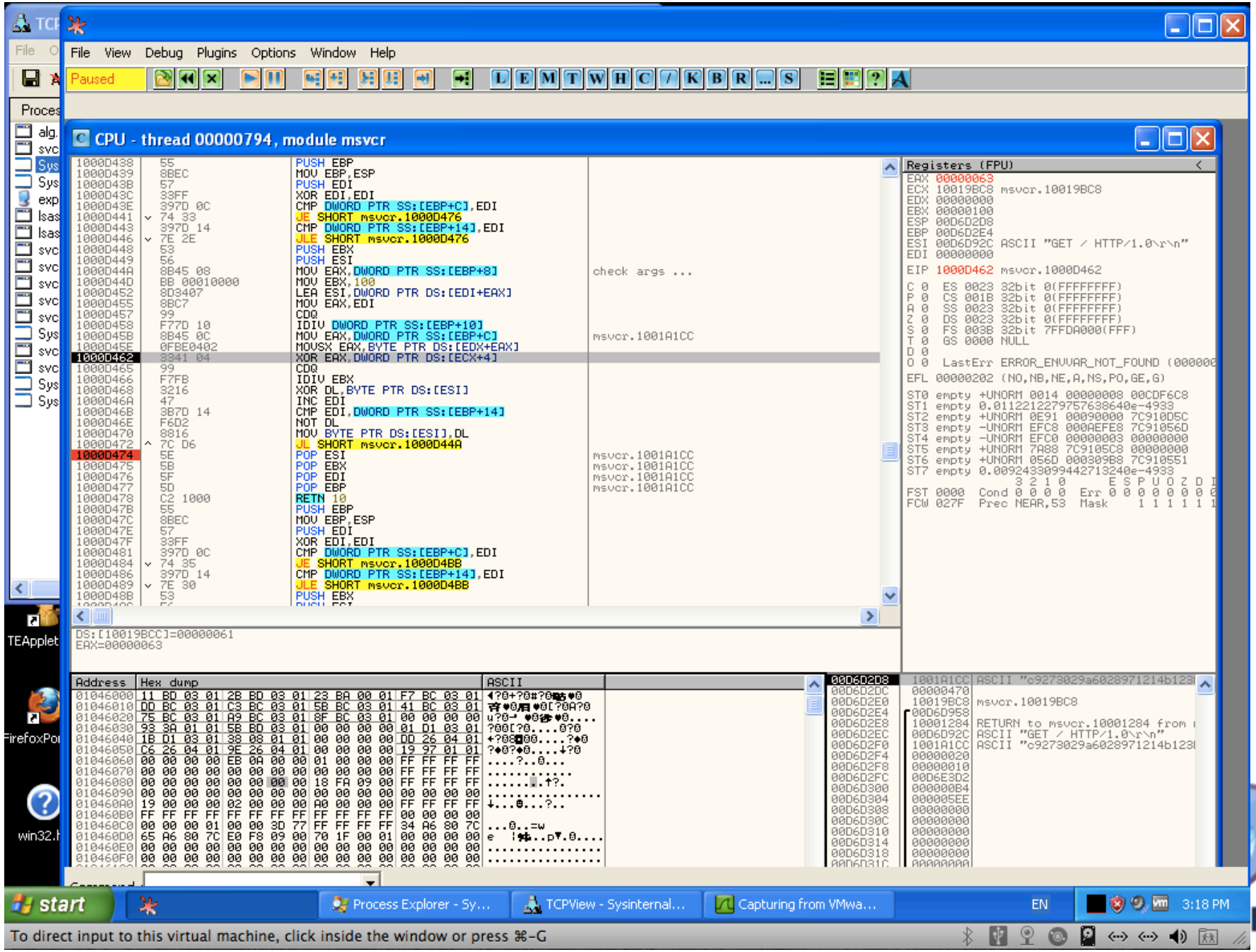

File View Debug Plugins Options Window Help
Paused
CPU - thread 00000794, module msvcr
1000D438 55 PUSH EBP
1000D439 8BEC MOV EBP,ESP
1000D43B 57 PUSH EDI
1000D43C 33FF XOR EDI,EDI
1000D43E 397D 0C CMP DWORD PTR SS:[EBP+C],EDI
1000D441 74 33 JE SHORT msvcr.1000D476
1000D443 397D 14 CMP DWORD PTR SS:[EBP+14],EDI
1000D446 7E 2E JLE SHORT msvcr.1000D476
1000D448 53 PUSH EBX
1000D449 56 PUSH ESI
1000D44A 8B45 08 MOV EAX,DWORD PTR SS:[EBP+8]
1000D44D BB 00010000 MOV EBX,100
1000D452 8D3407 LEA ESI,DWORD PTR DS:[EDI+EAX]
1000D455 8BC7 MOV EAX,EDI
1000D457 99 CDQ
1000D458 F77D 10 IDIV DWORD PTR SS:[EBP+10]
1000D45B 8B45 0C MOV EAX,DWORD PTR SS:[EBP+C]
1000D45E 0FBE0402 MOVSX EAX,BYTE PTR DS:[EDX+EAX]
1000D462 3341 04 XOR EAX,DWORD PTR DS:[ECX+4]
1000D465 99 CDQ
1000D466 F7FB IDIV EBX
1000D468 3216 XOR DL,BYTE PTR DS:[ESI]
1000D46A 47 INC EDI
1000D46B 3B7D 14 CMP EDI,DWORD PTR SS:[EBP+14]
1000D46E F6D2 NOT DL
1000D470 8816 MOV BYTE PTR DS:[ESI],DL
1000D472 7C D6 JL SHORT msvcr.1000D44A
1000D474 5E POP ESI
1000D475 5B POP EBX
1000D476 5F POP EDI
1000D477 5D POP EBP
1000D478 C2 1000 RETN 10
1000D47B 55 PUSH EBP
1000D47C 8BEC MOV EBP,ESP
1000D47E 57 PUSH EDI
1000D47F 33FF XOR EDI,EDI
1000D481 397D 0C CMP DWORD PTR SS:[EBP+C],EDI
1000D484 74 35 JE SHORT msvcr.1000D4BB
1000D486 397D 14 CMP DWORD PTR SS:[EBP+14],EDI
1000D489 7E 30 JLE SHORT msvcr.1000D4BB
1000D48B 53 PUSH EBX
check args ...
Registers (FPU)
EAX 00D6D92C ASCII "GET / HTTP/1.0\r\n"
ECX 10019BC8 msvcr.10019BC8
EDX 00001717
EBX 00000470
ESP 00D6D2E8
EBP 00D6D958
ESI 1001A1CC ASCII "c9273029a6028971214b123
EDI 10019BC8 msvcr.10019BC8
EIP 1000D438 msvcr.1000D438
C 1 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 1 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 1 FS 003B 32bit 7FFDA000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_ENVVAR_NOT_FOUND (000000
EFL 00000297 (NO,B,NE,BE,S,PE,L,LE)
ST0 empty +UNORM 0014 00000008 00CDF6C8
ST1 empty 0.011221227975763864 0e-4933
ST2 empty +UNORM 0E91 00090000 7C910D5C
ST3 empty -UNORM EFC8 000AEFE8 7C91056D
ST4 empty -UNORM EFC0 00000003 00000000
ST5 empty +UNORM 7A88 7C9105C8 00000000
ST6 empty +UNORM 056D 000309B8 7C910551
ST7 empty 0.009243309944271324 0e-4933
3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
EBP=00D6D958
Address Hex dump ASCII
00D6D2E8 10001284 RETURN to msvcr.10001284 from
00D6D2EC 00D6D92C ASCII "GET / HTTP/1.0\r\n"
00D6D2F0 1001A1CC ASCII "c9273029a6028971214b123
00D6D2F4 00000020
00D6D2F8 00000010
00D6D2FC 00D6E3D2
00D6D300 000000B4
00D6D304 000005EE
00D6D308 00000000
00D6D30C 00000000
00D6D310 00000000
00D6D314 00000000
00D6D318 00000000
00D6D31C 00000000
00D6D320 00000000
00D6D324 00000000
00D6D328 00000000
start
Process Explorer - Sy...
TCPView - Sysinternal...
Capturing from VMwa...
EN
3:14 PM
To direct input to this virtual machine, click inside the window or press ⌘-G

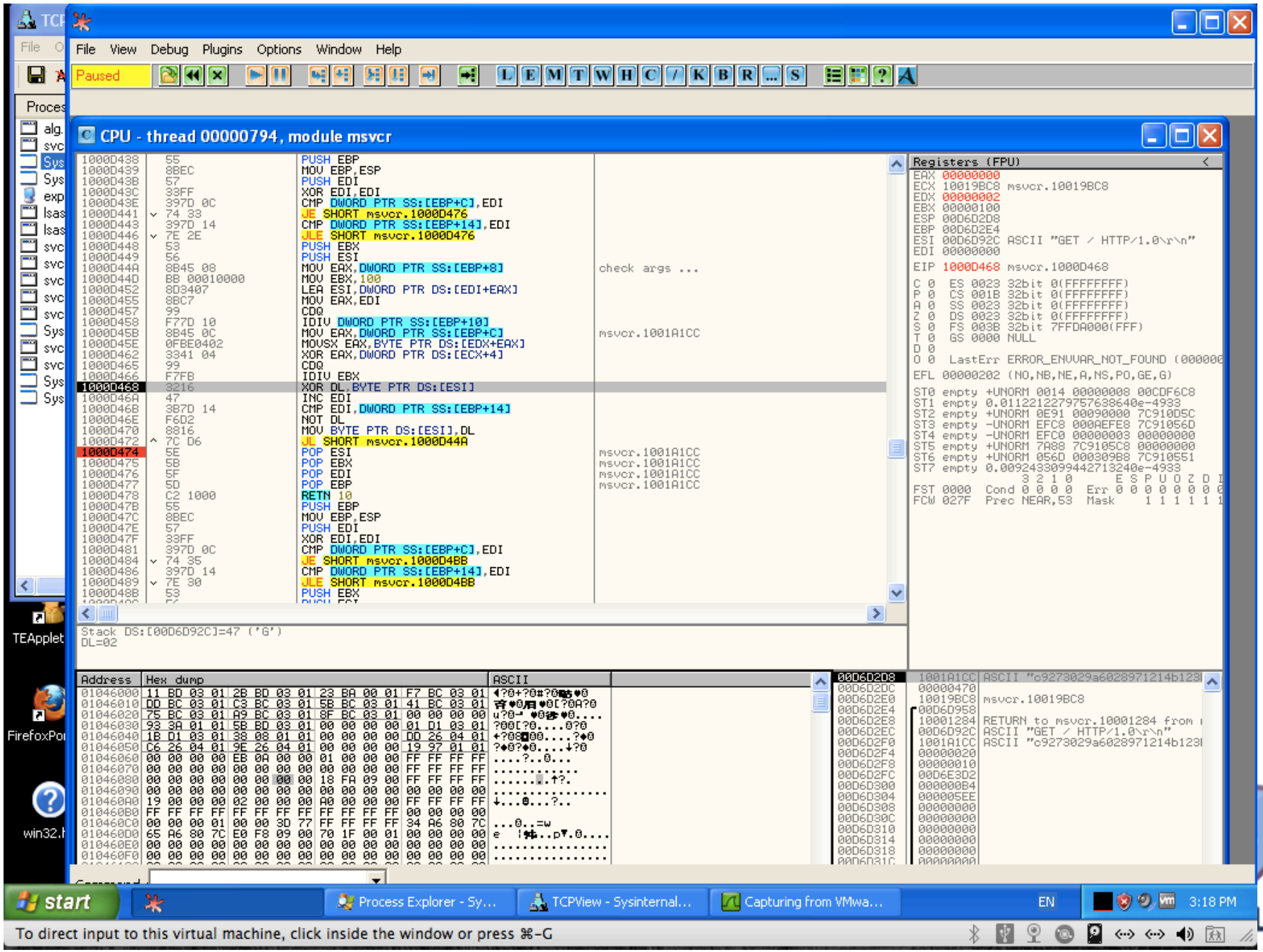

CPU - thread 00000794, module msvcr
Registers (FPU)
Jump is NOT taken
1000D476=msvcr.1000D476
Address
Hex dump
ASCII
start
Process Explorer - Sy...
TCPView - Sysinternal...
Capturing from VMwa...
EN
3:15 PM
To return to your computer, press Control-⌘

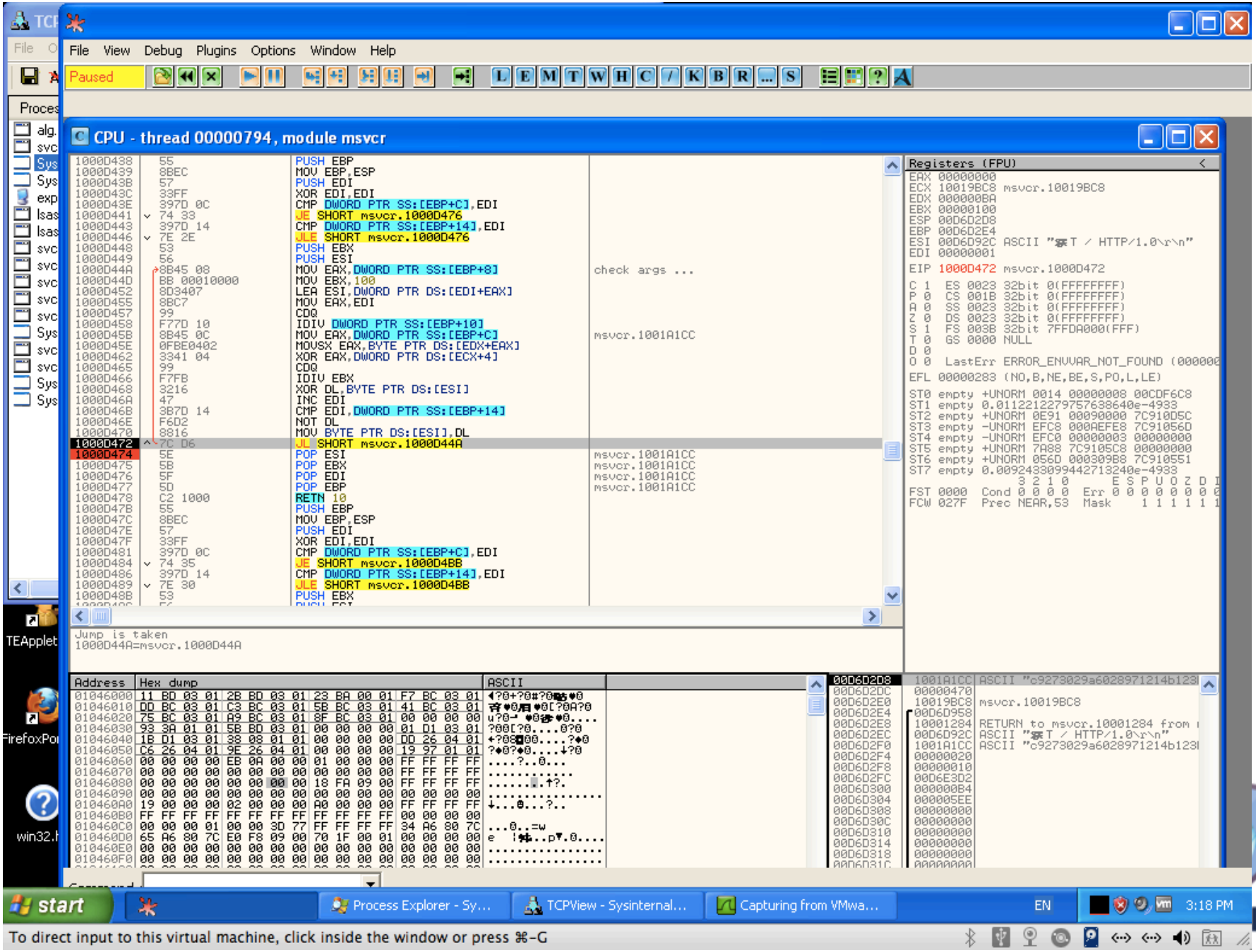

File View Debug Plugins Options Window Help
Paused
CPU - thread 00000794, module msvcr
1000D438 55 PUSH EBP
1000D439 8BEC MOV EBP,ESP
1000D43B 57 PUSH EDI
1000D43C 33FF XOR EDI,EDI
1000D43E 397D 0C CMP DWORD PTR SS:[EBP+C],EDI
1000D441 74 33 JE SHORT msvcr.1000D476
1000D443 397D 14 CMP DWORD PTR SS:[EBP+14],EDI
1000D446 7E 2E JLE SHORT msvcr.1000D476
1000D448 53 PUSH EBX
1000D449 56 PUSH ESI
1000D44A 8B45 08 MOV EAX,DWORD PTR SS:[EBP+8]
1000D44D BB 00010000 MOV EBX,100
1000D452 8D3407 LEA ESI,DWORD PTR DS:[EDI+EAX]
1000D455 8BC7 MOV EAX,EDI
1000D457 99 CDQ
1000D458 F77D 10 IDIV DWORD PTR SS:[EBP+10]
1000D45B 8B45 0C MOV EAX,DWORD PTR SS:[EBP+C]
1000D45E 0FBE0402 MOVSX EAX,BYTE PTR DS:[EDX+EAX]
1000D462 3341 04 XOR EAX,DWORD PTR DS:[ECX+4]
1000D465 99 CDQ
1000D466 F7FB IDIV EBX
1000D468 3216 XOR DL,BYTE PTR DS:[ESI]
1000D46A 47 INC EDI
1000D46B 3B7D 14 CMP EDI,DWORD PTR SS:[EBP+14]
1000D46E F6D2 NOT DL
1000D470 8816 MOV BYTE PTR DS:[ESI],DL
1000D472 7C D6 JL SHORT msvcr.1000D44A
1000D474 5E POP ESI
1000D475 5B POP EBX
1000D476 5F POP EDI
1000D477 5D POP EBP
1000D478 C2 1000 RETN 10
1000D47B 55 PUSH EBP
1000D47C 8BEC MOV EBP,ESP
1000D47E 57 PUSH EDI
1000D47F 33FF XOR EDI,EDI
1000D481 397D 0C CMP DWORD PTR SS:[EBP+C],EDI
1000D484 74 35 JE SHORT msvcr.1000D4BB
1000D486 397D 14 CMP DWORD PTR SS:[EBP+14],EDI
1000D489 7E 30 JLE SHORT msvcr.1000D4BB
1000D48B 53 PUSH EBX
check args ...
Registers (FPU)
EAX 00D6D92C ASCII "GET / HTTP/1.0\r\n"
ECX 10019BC8 msvcr.10019BC8
EDX 00001717
EBX 00000470
ESP 00D6D2D8
EBP 00D6D2E4
ESI 1001A1CC ASCII "c9273029a6028971214b123
EDI 00000000
EIP 1000D44A msvcr.1000D44A
C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDA000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_ENVVAR_NOT_FOUND (000000
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty +UNORM 0014 00000008 00CDF6C8
ST1 empty 0.011221227975763864 0e-4933
ST2 empty +UNORM 0E91 00090000 7C910D5C
ST3 empty -UNORM EFC8 000AEFE8 7C91056D
ST4 empty -UNORM EFC0 00000003 00000000
ST5 empty +UNORM 7A88 7C9105C8 00000000
ST6 empty +UNORM 056D 00030B8 7C910551
ST7 empty 0.009243309944271324 0e-4933
3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
Stack SS:[00D6D2EC]=00D6D92C, (ASCII "GET / HTTP/1.0\r\n")
EAX=00D6D92C, (ASCII "GET / HTTP/1.0\r\n")
Address Hex dump ASCII
01046000 11 BD 03 01 2B BD 03 01 23 BA 00 01 F7 BC 03 01
01046010 DD BC 03 01 C3 BC 03 01 5B BC 03 01 41 BC 03 01
01046020 75 BC 03 01 A9 BC 03 01 8F BC 03 01 00 00 00 00
01046030 93 3A 01 01 5B BD 03 01 00 00 00 00 01 D1 03 01
01046040 1B D1 03 01 38 08 01 01 00 00 00 00 DD 26 04 01
01046050 C6 26 04 01 9E 26 04 01 00 00 00 00 19 97 01 01
01046060 00 00 00 00 EB 0A 00 00 01 00 00 00 FF FF FF FF
01046070 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF
01046080 00 00 00 00 00 00 00 00 18 FA 09 00 FF FF FF FF
01046090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010460A0 19 00 00 00 02 00 00 00 A0 00 00 00 FF FF FF FF
010460B0 FF FF FF FF FF FF FF FF FF FF FF FF 00 00 00 00
010460C0 00 00 00 01 00 00 3D 77 FF FF FF FF 34 A6 80 7C
010460D0 65 A6 80 7C E0 F8 09 00 70 1F 00 01 00 00 00 00
010460E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010460F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00D6D2D8 1001A1CC ASCII "c9273029a6028971214b123
00D6D2DC 00000470
00D6D2E0 10019BC8 msvcr.10019BC8
00D6D2E4 00D6D958
00D6D2E8 10001284 RETURN to msvcr.10001284 from
00D6D2EC 00D6D92C ASCII "GET / HTTP/1.0\r\n"
00D6D2F0 1001A1CC ASCII "c9273029a6028971214b123
00D6D2F4 00000020
00D6D2F8 00000010
00D6D2FC 00D6E3D2
00D6D300 000000B4
00D6D304 000005EE
00D6D308 00000000
00D6D30C 00000000
00D6D310 00000000
00D6D314 00000000
00D6D318 00000000
TEApplet
FirefoxPor
win32.h
start
Process Explorer - Sy...
TCPView - Sysinternal...
Capturing from VMwa...
EN
3:16 PM
To direct input to this virtual machine, click inside the window or press ⌘-G


File View Debug Plugins Options Window Help
Paused
CPU - thread 00000794, module msvcr
1000D438 55 PUSH EBP
1000D439 8BEC MOV EBP,ESP
1000D43B 57 PUSH EDI
1000D43C 33FF XOR EDI,EDI
1000D43E 397D 0C CMP DWORD PTR SS:[EBP+C],EDI
1000D441 74 33 JE SHORT msvcr.1000D476
1000D443 397D 14 CMP DWORD PTR SS:[EBP+14],EDI
1000D446 7E 2E JLE SHORT msvcr.1000D476
1000D448 53 PUSH EBX
1000D449 56 PUSH ESI
1000D44A 8B45 08 MOV EAX,DWORD PTR SS:[EBP+8]
1000D44D BB 00010000 MOV EBX,100
1000D452 8D3407 LEA ESI,DWORD PTR DS:[EDI+EAX]
1000D455 8BC7 MOV EAX,EDI
1000D457 99 CDQ
1000D458 F77D 10 IDIV DWORD PTR SS:[EBP+10]
1000D45B 8B45 0C MOV EAX,DWORD PTR SS:[EBP+C]
1000D45E 0FBE0402 MOVSX EAX,BYTE PTR DS:[EDX+EAX]
1000D462 3341 04 XOR EAX,DWORD PTR DS:[ECX+4]
1000D465 99 CDQ
1000D466 F7FB IDIV EBX
1000D468 3216 XOR DL,BYTE PTR DS:[ESI]
1000D46A 47 INC EDI
1000D46B 3B7D 14 CMP EDI,DWORD PTR SS:[EBP+14]
1000D46E F6D2 NOT DL
1000D470 8816 MOV BYTE PTR DS:[ESI],DL
1000D472 7C D6 JL SHORT msvcr.1000D44A
1000D474 5E POP ESI
1000D475 5B POP EBX
1000D476 5F POP EDI
1000D477 5D POP EBP
1000D478 C2 1000 RETN 10
1000D47B 55 PUSH EBP
1000D47C 8BEC MOV EBP,ESP
1000D47E 57 PUSH EDI
1000D47F 33FF XOR EDI,EDI
1000D481 397D 0C CMP DWORD PTR SS:[EBP+C],EDI
1000D484 74 35 JE SHORT msvcr.1000D4BB
1000D486 397D 14 CMP DWORD PTR SS:[EBP+14],EDI
1000D489 7E 30 JLE SHORT msvcr.1000D4BB
1000D48B 53 PUSH EBX
msvcr.1001A1CC
check args ...
msvcr.1001A1CC
msvcr.1001A1CC
msvcr.1001A1CC
msvcr.1001A1CC
Registers (FPU)
EAX 00D6D92C ASCII "GET / HTTP/1.0\r\n"
ECX 10019BC8 msvcr.10019BC8
EDX 00001717
EBX 00000100
ESP 00D6D2D8
EBP 00D6D2E4
ESI 1001A1CC ASCII "c9273029a6028971214b123
EDI 00000000
EIP 1000D452 msvcr.1000D452
C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDA000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_ENVVAR_NOT_FOUND (000000
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty +UNORM 0014 00000008 00CDF6C8
ST1 empty 0.011221227975763864 0e-4933
ST2 empty +UNORM 0E91 00090000 7C910D5C
ST3 empty -UNORM EFC8 000AEFE8 7C91056D
ST4 empty -UNORM EFC0 00000003 00000000
ST5 empty +UNORM 7A88 7C9105C8 00000000
ST6 empty +UNORM 056D 00030B8 7C910551
ST7 empty 0.009243309944271324 0e-4933
3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
Stack address=00D6D92C, (ASCII "GET / HTTP/1.0\r\n")
ESI=1001A1CC (msvcr.1001A1CC), ASCII "c9273029a6028971214b123b54b0d72d"
Address Hex dump ASCII
01046000 11 BD 03 01 2B BD 03 01 23 BA 00 01 F7 BC 03 01
01046010 DD BC 03 01 C3 BC 03 01 5B BC 03 01 41 BC 03 01
01046020 75 BC 03 01 A9 BC 03 01 8F BC 03 01 00 00 00 00
01046030 93 3A 01 01 5B BD 03 01 00 00 00 00 01 D1 03 01
01046040 1B D1 03 01 38 08 01 01 00 00 00 00 DD 26 04 01
01046050 C6 26 04 01 9E 26 04 01 00 00 00 00 19 97 01 01
01046060 00 00 00 00 EB 0A 00 00 01 00 00 00 FF FF FF FF
01046070 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF
01046080 00 00 00 00 00 00 00 00 18 FA 09 00 FF FF FF FF
01046090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010460A0 19 00 00 00 02 00 00 00 A0 00 00 00 FF FF FF FF
010460B0 FF FF FF FF FF FF FF FF FF FF FF FF 00 00 00 00
010460C0 00 00 00 01 00 00 3D 77 FF FF FF FF 34 A6 80 7C
010460D0 65 A6 80 7C E0 F8 09 00 70 1F 00 01 00 00 00 00
010460E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010460F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00D6D2D8 1001A1CC ASCII "c9273029a6028971214b123
00D6D2DC 00000470
00D6D2E0 10019BC8 msvcr.10019BC8
00D6D2E4 00D6D958
00D6D2E8 10001284 RETURN to msvcr.10001284 from
00D6D2EC 00D6D92C ASCII "GET / HTTP/1.0\r\n"
00D6D2F0 1001A1CC ASCII "c9273029a6028971214b123
00D6D2F4 00000020
00D6D2F8 00000010
00D6D2FC 00D6E3D2
00D6D300 000000B4
00D6D304 000005EE
00D6D308 00000000
00D6D30C 00000000
00D6D310 00000000
00D6D314 00000000
00D6D318 00000000
start
Process Explorer - Sy...
TCPView - Sysinternal...
Capturing from VMwa...
EN
3:17 PM
To direct input to this virtual machine, click inside the window or press ⌘-G


File View Debug Plugins Options Window Help
Paused
CPU - thread 00000794, module msvcr
1000D438 55 PUSH EBP
1000D439 8BEC MOV EBP,ESP
1000D43B 57 PUSH EDI
1000D43C 33FF XOR EDI,EDI
1000D43E 397D 0C CMP DWORD PTR SS:[EBP+C],EDI
1000D441 74 33 JE SHORT msvcr.1000D476
1000D443 397D 14 CMP DWORD PTR SS:[EBP+14],EDI
1000D446 7E 2E JLE SHORT msvcr.1000D476
1000D448 53 PUSH EBX
1000D449 56 PUSH ESI
1000D44A 8B45 08 MOV EAX,DWORD PTR SS:[EBP+8] check args ...
1000D44D BB 00010000 MOV EBX,100
1000D452 8D3407 LEA ESI,DWORD PTR DS:[EDI+EAX]
1000D455 8BC7 MOV EAX,EDI
1000D457 99 CDQ
1000D458 F77D 10 IDIV DWORD PTR SS:[EBP+10]
1000D45B 8B45 0C MOV EAX,DWORD PTR SS:[EBP+C] msvcr.1001A1CC
1000D45E 0FBE0402 MOVSX EAX,BYTE PTR DS:[EDX+EAX]
1000D462 3341 04 XOR EAX,DWORD PTR DS:[ECX+4]
1000D465 99 CDQ
1000D466 F7FB IDIV EBX
1000D468 3216 XOR DL,BYTE PTR DS:[ESI]
1000D46A 47 INC EDI
1000D46B 3B7D 14 CMP EDI,DWORD PTR SS:[EBP+14]
1000D46E F6D2 NOT DL
1000D470 8816 MOV BYTE PTR DS:[ESI],DL
1000D472 7C D6 JL SHORT msvcr.1000D44A
1000D474 5E POP ESI msvcr.1001A1CC
1000D475 5B POP EBX msvcr.1001A1CC
1000D476 5F POP EDI msvcr.1001A1CC
1000D477 5D POP EBP msvcr.1001A1CC
1000D478 C2 1000 RETN 10
1000D47B 55 PUSH EBP
1000D47C 8BEC MOV EBP,ESP
1000D47E 57 PUSH EDI
1000D47F 33FF XOR EDI,EDI
1000D481 397D 0C CMP DWORD PTR SS:[EBP+C],EDI
1000D484 74 35 JE SHORT msvcr.1000D4BB
1000D486 397D 14 CMP DWORD PTR SS:[EBP+14],EDI
1000D489 7E 30 JLE SHORT msvcr.1000D4BB
1000D48B 53 PUSH EBX
Registers (FPU)
EAX 1001A1CC ASCII "c9273029a6028971214b123
ECX 10019BC8 msvcr.10019BC8
EDX 00000000
EBX 00000100
ESP 00D6D2D8
EBP 00D6D2E4
ESI 00D6D92C ASCII "GET / HTTP/1.0\r\n"
EDI 00000000
EIP 1000D45E msvcr.1000D45E
C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDA000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_ENVVAR_NOT_FOUND (000000
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty +UNORM 0014 00000008 00CDF6C8
ST1 empty 0.0112212279757638640e-4933
ST2 empty +UNORM 0E91 00090000 7C910D5C
ST3 empty -UNORM EFC8 000AEFE8 7C91056D
ST4 empty -UNORM EFC0 00000003 00000000
ST5 empty +UNORM 7A88 7C9105C8 00000000
ST6 empty +UNORM 056D 00030B8 7C910551
ST7 empty 0.0092433099442713240e-4933
3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
DS:[1001A1CC]=63 ('c')
EAX=1001A1CC (msvcr.1001A1CC), ASCII "c9273029a6028971214b123b54b0d72d"
Address Hex dump ASCII
01046000 11 BD 03 01 2B BD 03 01 23 BA 00 01 F7 BC 03 01
01046010 DD BC 03 01 C3 BC 03 01 5B BC 03 01 41 BC 03 01
01046020 75 BC 03 01 A9 BC 03 01 8F BC 03 01 00 00 00 00
01046030 93 3A 01 01 5B BD 03 01 00 00 00 00 01 D1 03 01
01046040 1B D1 03 01 38 08 01 01 00 00 00 00 DD 26 04 01
01046050 C6 26 04 01 9E 26 04 01 00 00 00 00 19 97 01 01
01046060 00 00 00 00 EB 0A 00 00 01 00 00 00 FF FF FF FF
01046070 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF
01046080 00 00 00 00 00 00 00 00 18 FA 09 00 FF FF FF FF
01046090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010460A0 19 00 00 00 02 00 00 00 A0 00 00 00 FF FF FF FF
010460B0 FF FF FF FF FF FF FF FF FF FF FF FF 00 00 00 00
010460C0 00 00 00 01 00 00 3D 77 FF FF FF FF 34 A6 80 7C
010460D0 65 A6 80 7C E0 F8 09 00 70 1F 00 01 00 00 00 00
010460E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010460F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00D6D2D8 1001A1CC ASCII "c9273029a6028971214b123
00D6D2DC 00000470
00D6D2E0 10019BC8 msvcr.10019BC8
00D6D2E4 00D6D958
00D6D2E8 10001284 RETURN to msvcr.10001284 from
00D6D2EC 00D6D92C ASCII "GET / HTTP/1.0\r\n"
00D6D2F0 1001A1CC ASCII "c9273029a6028971214b123
00D6D2F4 00000020
00D6D2F8 00000010
00D6D2FC 00D6E3D2
00D6D300 000000B4
00D6D304 000005EE
00D6D308 00000000
00D6D30C 00000000
00D6D310 00000000
00D6D314 00000000
00D6D318 00000000
TEApplet
FirefoxPor
win32.h
start
Process Explorer - Sy...
TCPView - Sysinternal...
Capturing from VMwa...
EN
3:17 PM
To direct input to this virtual machine, click inside the window or press ⌘-G


File View Debug Plugins Options Window Help
Paused
CPU - thread 00000794, module msvcr
1000D438 55 PUSH EBP
1000D439 8BEC MOV EBP,ESP
1000D43B 57 PUSH EDI
1000D43C 33FF XOR EDI,EDI
1000D43E 397D 0C CMP DWORD PTR SS:[EBP+C],EDI
1000D441 74 33 JE SHORT msvcr.1000D476
1000D443 397D 14 CMP DWORD PTR SS:[EBP+14],EDI
1000D446 7E 2E JLE SHORT msvcr.1000D476
1000D448 53 PUSH EBX
1000D449 56 PUSH ESI
1000D44A 8B45 08 MOV EAX,DWORD PTR SS:[EBP+8] check args ...
1000D44D BB 00010000 MOV EBX,100
1000D452 8D3407 LEA ESI,DWORD PTR DS:[EDI+EAX]
1000D455 8BC7 MOV EAX,EDI
1000D457 99 CDQ
1000D458 F77D 10 IDIV DWORD PTR SS:[EBP+10]
1000D45B 8B45 0C MOV EAX,DWORD PTR SS:[EBP+C] msvcr.1001A1CC
1000D45E 0FBE0402 MOVSX EAX,BYTE PTR DS:[EDX+EAX]
1000D462 3341 04 XOR EAX,DWORD PTR DS:[ECX+4]
1000D465 99 CDQ
1000D466 F7FB IDIV EBX
1000D468 3216 XOR DL,BYTE PTR DS:[ESI]
1000D46A 47 INC EDI
1000D46B 3B7D 14 CMP EDI,DWORD PTR SS:[EBP+14]
1000D46E F6D2 NOT DL
1000D470 8816 MOV BYTE PTR DS:[ESI],DL
1000D472 7C D6 JL SHORT msvcr.1000D44A
1000D474 5E POP ESI msvcr.1001A1CC
1000D475 5B POP EBX msvcr.1001A1CC
1000D476 5F POP EDI msvcr.1001A1CC
1000D477 5D POP EBP msvcr.1001A1CC
1000D478 C2 1000 RETN 10
1000D47B 55 PUSH EBP
1000D47C 8BEC MOV EBP,ESP
1000D47E 57 PUSH EDI
1000D47F 33FF XOR EDI,EDI
1000D481 397D 0C CMP DWORD PTR SS:[EBP+C],EDI
1000D484 74 35 JE SHORT msvcr.1000D4BB
1000D486 397D 14 CMP DWORD PTR SS:[EBP+14],EDI
1000D489 7E 30 JLE SHORT msvcr.1000D4BB
1000D48B 53 PUSH EBX
Registers (FPU)
EAX 00000063
ECX 10019BC8 msvcr.10019BC8
EDX 00000000
EBX 00000100
ESP 00D6D2D8
EBP 00D6D2E4
ESI 00D6D92C ASCII "GET / HTTP/1.0\r\n"
EDI 00000000
EIP 1000D462 msvcr.1000D462
C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDA000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_ENVVAR_NOT_FOUND (000000
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty +UNORM 0014 00000008 00CDF6C8
ST1 empty 0.011221227975763864 0e-4933
ST2 empty +UNORM 0E91 00090000 7C910D5C
ST3 empty -UNORM EFC8 000AEFE8 7C91056D
ST4 empty -UNORM EFC0 00000003 00000000
ST5 empty +UNORM 7A88 7C9105C8 00000000
ST6 empty +UNORM 056D 000309B8 7C910551
ST7 empty 0.009243309944271324 0e-4933
3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
DS:[10019BCC]=00000061
EAX=00000063
Address Hex dump ASCII
01046000 11 BD 03 01 2B BD 03 01 23 BA 00 01 F7 BC 03 01
01046010 DD BC 03 01 C3 BC 03 01 5B BC 03 01 41 BC 03 01
01046020 75 BC 03 01 A9 BC 03 01 8F BC 03 01 00 00 00 00
01046030 93 3A 01 01 5B BD 03 01 00 00 00 00 01 D1 03 01
01046040 1B D1 03 01 38 08 01 01 00 00 00 00 DD 26 04 01
01046050 C6 26 04 01 9E 26 04 01 00 00 00 00 19 97 01 01
01046060 00 00 00 00 EB 0A 00 00 01 00 00 00 FF FF FF FF
01046070 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF
01046080 00 00 00 00 00 00 00 00 18 FA 09 00 FF FF FF FF
01046090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010460A0 19 00 00 00 02 00 00 00 A0 00 00 00 FF FF FF FF
010460B0 FF FF FF FF FF FF FF FF FF FF FF FF 00 00 00 00
010460C0 00 00 00 01 00 00 3D 77 FF FF FF FF 34 A6 80 7C
010460D0 65 A6 80 7C E0 F8 09 00 70 1F 00 01 00 00 00 00
010460E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010460F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00D6D2D8 1001A1CC ASCII "c9273029a6028971214b123
00D6D2DC 00000470
00D6D2E0 10019BC8 msvcr.10019BC8
00D6D2E4 00D6D958
00D6D2E8 10001284 RETURN to msvcr.10001284 from
00D6D2EC 00D6D92C ASCII "GET / HTTP/1.0\r\n"
00D6D2F0 1001A1CC ASCII "c9273029a6028971214b123
00D6D2F4 00000020
00D6D2F8 00000010
00D6D2FC 00D6E3D2
00D6D300 000000B4
00D6D304 000005EE
00D6D308 00000000
00D6D30C 00000000
00D6D310 00000000
00D6D314 00000000
00D6D318 00000000
TEApplet
FirefoxPor
win32.h
start
Process Explorer - Sy...
TCPView - Sysinternal...
Capturing from VMwa...
EN
3:18 PM
To direct input to this virtual machine, click inside the window or press ⌘-G


File View Debug Plugins Options Window Help
Paused
CPU - thread 00000794, module msvcr
1000D438 55 PUSH EBP
1000D439 8BEC MOV EBP,ESP
1000D43B 57 PUSH EDI
1000D43C 33FF XOR EDI,EDI
1000D43E 397D 0C CMP DWORD PTR SS:[EBP+C],EDI
1000D441 74 33 JE SHORT msvcr.1000D476
1000D443 397D 14 CMP DWORD PTR SS:[EBP+14],EDI
1000D446 7E 2E JLE SHORT msvcr.1000D476
1000D448 53 PUSH EBX
1000D449 56 PUSH ESI
1000D44A 8B45 08 MOV EAX,DWORD PTR SS:[EBP+8] check args ...
1000D44D BB 00010000 MOV EBX,100
1000D452 8D3407 LEA ESI,DWORD PTR DS:[EDI+EAX]
1000D455 8BC7 MOV EAX,EDI
1000D457 99 CDQ
1000D458 F77D 10 IDIV DWORD PTR SS:[EBP+10]
1000D45B 8B45 0C MOV EAX,DWORD PTR SS:[EBP+C] msvcr.1001A1CC
1000D45E 0FBE0402 MOVSX EAX,BYTE PTR DS:[EDX+EAX]
1000D462 3341 04 XOR EAX,DWORD PTR DS:[ECX+4]
1000D465 99 CDQ
1000D466 F7FB IDIV EBX
1000D468 3216 XOR DL,BYTE PTR DS:[ESI]
1000D46A 47 INC EDI
1000D46B 3B7D 14 CMP EDI,DWORD PTR SS:[EBP+14]
1000D46E F6D2 NOT DL
1000D470 8816 MOV BYTE PTR DS:[ESI],DL
1000D472 7C D6 JL SHORT msvcr.1000D44A
1000D474 5E POP ESI msvcr.1001A1CC
1000D475 5B POP EBX msvcr.1001A1CC
1000D476 5F POP EDI msvcr.1001A1CC
1000D477 5D POP EBP msvcr.1001A1CC
1000D478 C2 1000 RETN 10
1000D47B 55 PUSH EBP
1000D47C 8BEC MOV EBP,ESP
1000D47E 57 PUSH EDI
1000D47F 33FF XOR EDI,EDI
1000D481 397D 0C CMP DWORD PTR SS:[EBP+C],EDI
1000D484 74 35 JE SHORT msvcr.1000D4BB
1000D486 397D 14 CMP DWORD PTR SS:[EBP+14],EDI
1000D489 7E 30 JLE SHORT msvcr.1000D4BB
1000D48B 53 PUSH EBX
Registers (FPU)
EAX 00000000
ECX 10019BC8 msvcr.10019BC8
EDX 00000002
EBX 00000100
ESP 00D6D2D8
EBP 00D6D2E4
ESI 00D6D92C ASCII "GET / HTTP/1.0\r\n"
EDI 00000000
EIP 1000D468 msvcr.1000D468
C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDA000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_ENVVAR_NOT_FOUND (000000
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty +UNORM 0014 00000008 00CDF6C8
ST1 empty 0.011221227975763864 0e-4933
ST2 empty +UNORM 0E91 00090000 7C910D5C
ST3 empty -UNORM EFC8 000AEFE8 7C91056D
ST4 empty -UNORM EFC0 00000003 00000000
ST5 empty +UNORM 7A88 7C9105C8 00000000
ST6 empty +UNORM 056D 00030B8 7C910551
ST7 empty 0.009243309944271324 0e-4933
3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
Stack DS:[00D6D92C]=47 ('G')
DL=02
Address Hex dump ASCII
01046000 11 BD 03 01 2B BD 03 01 23 BA 00 01 F7 BC 03 01
01046010 DD BC 03 01 C3 BC 03 01 5B BC 03 01 41 BC 03 01
01046020 75 BC 03 01 A9 BC 03 01 8F BC 03 01 00 00 00 00
01046030 93 3A 01 01 5B BD 03 01 00 00 00 00 01 D1 03 01
01046040 1B D1 03 01 38 08 01 01 00 00 00 00 DD 26 04 01
01046050 C6 26 04 01 9E 26 04 01 00 00 00 00 19 97 01 01
01046060 00 00 00 00 EB 0A 00 00 01 00 00 00 FF FF FF FF
01046070 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF
01046080 00 00 00 00 00 00 00 00 18 FA 09 00 FF FF FF FF
01046090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010460A0 19 00 00 00 02 00 00 00 A0 00 00 00 FF FF FF FF
010460B0 FF FF FF FF FF FF FF FF FF FF FF FF 00 00 00 00
010460C0 00 00 00 01 00 00 3D 77 FF FF FF FF 34 A6 80 7C
010460D0 65 A6 80 7C E0 F8 09 00 70 1F 00 01 00 00 00 00
010460E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010460F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00D6D2D8 1001A1CC ASCII "c9273029a6028971214b123
00D6D2DC 00000470
00D6D2E0 10019BC8 msvcr.10019BC8
00D6D2E4 00D6D958
00D6D2E8 10001284 RETURN to msvcr.10001284 from
00D6D2EC 00D6D92C ASCII "GET / HTTP/1.0\r\n"
00D6D2F0 1001A1CC ASCII "c9273029a6028971214b123
00D6D2F4 00000020
00D6D2F8 00000010
00D6D2FC 00D6E3D2
00D6D300 000000B4
00D6D304 000005EE
00D6D308 00000000
00D6D30C 00000000
00D6D310 00000000
00D6D314 00000000
00D6D318 00000000
TEApplet
FirefoxPor
win32.h
start
Process Explorer - Sy...
TCPView - Sysinternal...
Capturing from VMwa...
EN
3:18 PM
To direct input to this virtual machine, click inside the window or press ⌘-G

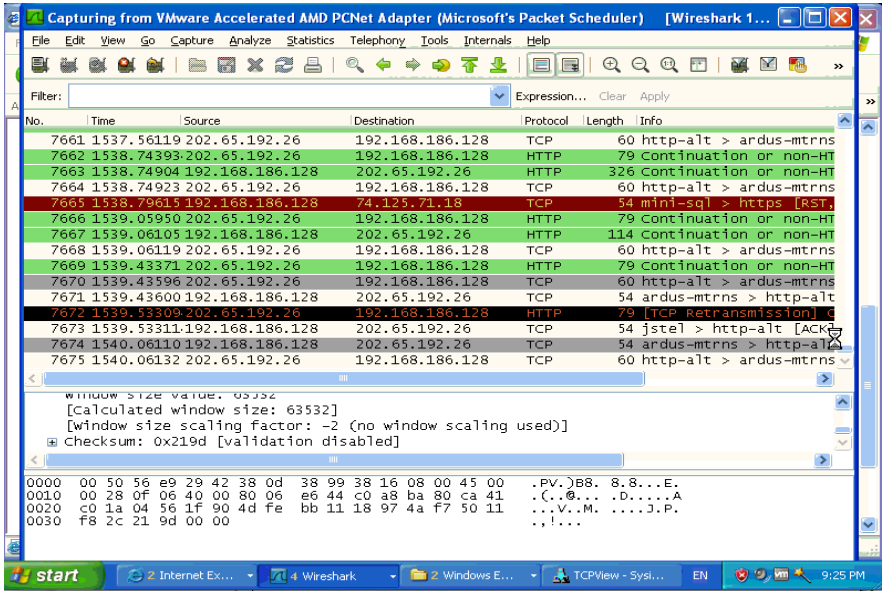

File View Debug Plugins Options Window Help
Paused
CPU - thread 00000794, module msvcr
1000D438 55 PUSH EBP
1000D439 8BEC MOV EBP,ESP
1000D43B 57 PUSH EDI
1000D43C 33FF XOR EDI,EDI
1000D43E 397D 0C CMP DWORD PTR SS:[EBP+C],EDI
1000D441 74 33 JE SHORT msvcr.1000D476
1000D443 397D 14 CMP DWORD PTR SS:[EBP+14],EDI
1000D446 7E 2E JLE SHORT msvcr.1000D476
1000D448 53 PUSH EBX
1000D449 56 PUSH ESI
1000D44A 8B45 08 MOV EAX,DWORD PTR SS:[EBP+8] check args ...
1000D44D BB 00010000 MOV EBX,100
1000D452 8D3407 LEA ESI,DWORD PTR DS:[EDI+EAX]
1000D455 8BC7 MOV EAX,EDI
1000D457 99 CDQ
1000D458 F77D 10 IDIV DWORD PTR SS:[EBP+10]
1000D45B 8B45 0C MOV EAX,DWORD PTR SS:[EBP+C] msvcr.1001A1CC
1000D45E 0FBE0402 MOVSX EAX,BYTE PTR DS:[EDX+EAX]
1000D462 3341 04 XOR EAX,DWORD PTR DS:[ECX+4]
1000D465 99 CDQ
1000D466 F7FB IDIV EBX
1000D468 3216 XOR DL,BYTE PTR DS:[ESI]
1000D46A 47 INC EDI
1000D46B 3B7D 14 CMP EDI,DWORD PTR SS:[EBP+14]
1000D46E F6D2 NOT DL
1000D470 8816 MOV BYTE PTR DS:[ESI],DL
1000D472 7C D6 JL SHORT msvcr.1000D44A
1000D474 5E POP ESI msvcr.1001A1CC
1000D475 5B POP EBX msvcr.1001A1CC
1000D476 5F POP EDI msvcr.1001A1CC
1000D477 5D POP EBP msvcr.1001A1CC
1000D478 C2 1000 RETN 10
1000D47B 55 PUSH EBP
1000D47C 8BEC MOV EBP,ESP
1000D47E 57 PUSH EDI
1000D47F 33FF XOR EDI,EDI
1000D481 397D 0C CMP DWORD PTR SS:[EBP+C],EDI
1000D484 74 35 JE SHORT msvcr.1000D4BB
1000D486 397D 14 CMP DWORD PTR SS:[EBP+14],EDI
1000D489 7E 30 JLE SHORT msvcr.1000D4BB
1000D48B 53 PUSH EBX
Registers (FPU)
EAX 00000000
ECX 10019BC8 msvcr.10019BC8
EDX 000000BA
EBX 00000100
ESP 00D6D2D8
EBP 00D6D2E4
ESI 00D6D92C ASCII "T / HTTP/1.0\r\n"
EDI 00000001
EIP 1000D472 msvcr.1000D472
C 1 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 1 FS 003B 32bit 7FFDA000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_ENVVAR_NOT_FOUND (000000
EFL 00000283 (NO,B,NE,BE,S,PO,L,LE)
ST0 empty +UNORM 0014 00000008 00CDF6C8
ST1 empty 0.011221227975763864 0e-4933
ST2 empty +UNORM 0E91 00090000 7C910D5C
ST3 empty -UNORM EFC8 000AEFE8 7C91056D
ST4 empty -UNORM EFC0 00000003 00000000
ST5 empty +UNORM 7A88 7C9105C8 00000000
ST6 empty +UNORM 056D 000309B8 7C910551
ST7 empty 0.009243309944271324 0e-4933
3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
Jump is taken
1000D44A=msvcr.1000D44A
Address Hex dump ASCII
01046000 11 BD 03 01 2B BD 03 01 23 BA 00 01 F7 BC 03 01
01046010 DD BC 03 01 C3 BC 03 01 5B BC 03 01 41 BC 03 01
01046020 75 BC 03 01 A9 BC 03 01 8F BC 03 01 00 00 00 00
01046030 93 3A 01 01 5B BD 03 01 00 00 00 00 01 D1 03 01
01046040 1B D1 03 01 38 08 01 01 00 00 00 00 DD 26 04 01
01046050 C6 26 04 01 9E 26 04 01 00 00 00 00 19 97 01 01
01046060 00 00 00 00 EB 0A 00 00 01 00 00 00 FF FF FF FF
01046070 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF
01046080 00 00 00 00 00 00 00 00 18 FA 09 00 FF FF FF FF
01046090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010460A0 19 00 00 00 02 00 00 00 A0 00 00 00 FF FF FF FF
010460B0 FF FF FF FF FF FF FF FF FF FF FF FF 00 00 00 00
010460C0 00 00 00 01 00 00 3D 77 FF FF FF FF 34 A6 80 7C
010460D0 65 A6 80 7C E0 F8 09 00 70 1F 00 01 00 00 00 00
010460E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010460F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00D6D2D8 1001A1CC ASCII "c9273029a6028971214b123
00D6D2DC 00000470
00D6D2E0 10019BC8 msvcr.10019BC8
00D6D2E4 00D6D958
00D6D2E8 10001284 RETURN to msvcr.10001284 from
00D6D2EC 00D6D92C ASCII "T / HTTP/1.0\r\n"
00D6D2F0 1001A1CC ASCII "c9273029a6028971214b123
00D6D2F4 00000020
00D6D2F8 00000010
00D6D2FC 00D6E3D2
00D6D300 000000B4
00D6D304 000005EE
00D6D308 00000000
00D6D30C 00000000
00D6D310 00000000
00D6D314 00000000
00D6D318 00000000
TEApplet
FirefoxPor
win32.h
start
Process Explorer - Sy...
TCPView - Sysinternal...
Capturing from VMwa...
EN
3:18 PM
To direct input to this virtual machine, click inside the window or press ⌘-G

Analysis – What information has been sent to CnC server?

- After decoding the network traffic
  - The host name
  - Installed OS type and patch level
- There should be more information sent to CnC server :)

Analysis – Found the .cab file

- We have found .bmp file in a compressed .cab file under application folder
- Screenshots are found. What the fxxk that our Wireshark screenshot is captured and sent back to CnC server :)



Xecure Lab

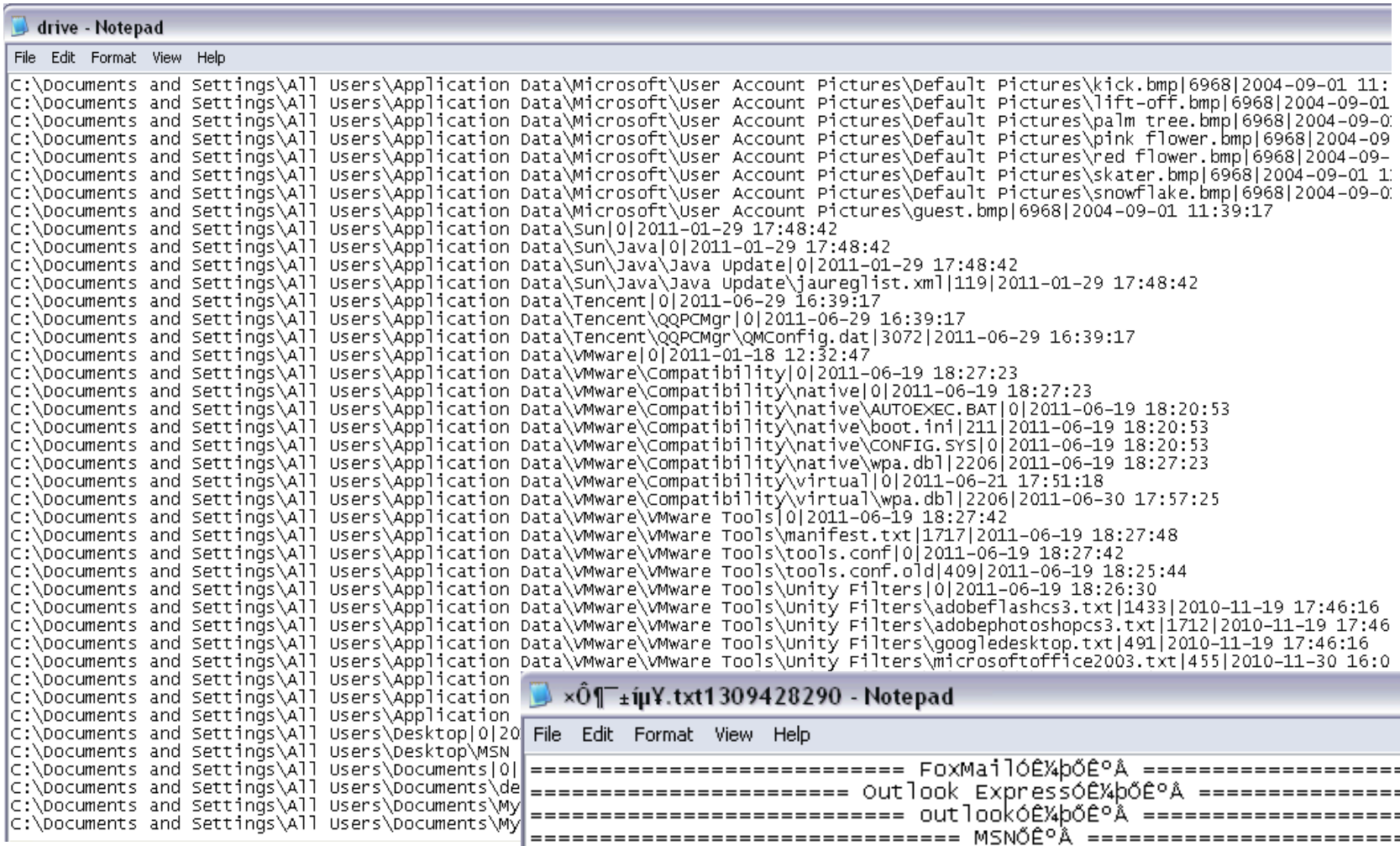
Digging into Tiger's Mouth ☺

- We have tried to install QQ, MSN and see what's going on:
  - Binaries are downloaded to the victim in C:\Windows\Debug folder
  - Malware creates more files in C:\Windows\Debug\Data folder
  - Those files are removed shortly.
  - Collected information are saved as file with .dll as extension and send it back to CnC server

What's going on?

- We have found that CnC server sent an instruction to the victim machine to compress files and send them back to the CnC server.
- There is a traffic sequence number set by the CnC server. Once the sequence number is used or wrong, the machine will not be infected again or CnC server will not send further instruction..
- The files iestorage.dll, SAM.dll and system.dll are actually cab compressed. Just rename the extension as "cab" and decompress them to get the following information.
  - The SAM and system kept the victim machines account information and registry information.
- The iestorage contains a file called "自动表单.txt987654321" which keeps the hacked email accounts and passwords.
- Another file, called drive, it keeps all filenames and time information on the hard disk
  - The APT task force really wants to know what information that the target kept in the victim machine.

Xecure Lab


drive - Notepad
File Edit Format View Help
C:\Documents and Settings\All Users\Application Data\Microsoft\User Account Pictures\Default Pictures\kick.bmp|6968|2004-09-01 11:
C:\Documents and Settings\All Users\Application Data\Microsoft\User Account Pictures\Default Pictures\lift-off.bmp|6968|2004-09-01
C:\Documents and Settings\All Users\Application Data\Microsoft\User Account Pictures\Default Pictures\palm tree.bmp|6968|2004-09-0
C:\Documents and Settings\All Users\Application Data\Microsoft\User Account Pictures\Default Pictures\pink flower.bmp|6968|2004-09
C:\Documents and Settings\All Users\Application Data\Microsoft\User Account Pictures\Default Pictures\red flower.bmp|6968|2004-09-
C:\Documents and Settings\All Users\Application Data\Microsoft\User Account Pictures\Default Pictures\skater.bmp|6968|2004-09-01 1
C:\Documents and Settings\All Users\Application Data\Microsoft\User Account Pictures\Default Pictures\snowflake.bmp|6968|2004-09-0
C:\Documents and Settings\All Users\Application Data\Microsoft\User Account Pictures\guest.bmp|6968|2004-09-01 11:39:17
C:\Documents and Settings\All Users\Application Data\Sun|0|2011-01-29 17:48:42
C:\Documents and Settings\All Users\Application Data\Sun\Java|0|2011-01-29 17:48:42
C:\Documents and Settings\All Users\Application Data\Sun\Java\Java Update|0|2011-01-29 17:48:42
C:\Documents and Settings\All Users\Application Data\Sun\Java\Java Update\jaureglist.xml|119|2011-01-29 17:48:42
C:\Documents and Settings\All Users\Application Data\Tencent|0|2011-06-29 16:39:17
C:\Documents and Settings\All Users\Application Data\Tencent\QQPCMgr|0|2011-06-29 16:39:17
C:\Documents and Settings\All Users\Application Data\Tencent\QQPCMgr\QMConfig.dat|3072|2011-06-29 16:39:17
C:\Documents and Settings\All Users\Application Data\VMware|0|2011-01-18 12:32:47
C:\Documents and Settings\All Users\Application Data\VMware\Compatibility|0|2011-06-19 18:27:23
C:\Documents and Settings\All Users\Application Data\VMware\Compatibility\native|0|2011-06-19 18:27:23
C:\Documents and Settings\All Users\Application Data\VMware\Compatibility\native\AUTOEXEC.BAT|0|2011-06-19 18:20:53
C:\Documents and Settings\All Users\Application Data\VMware\Compatibility\native\boot.ini|211|2011-06-19 18:20:53
C:\Documents and Settings\All Users\Application Data\VMware\Compatibility\native\CONFIG.SYS|0|2011-06-19 18:20:53
C:\Documents and Settings\All Users\Application Data\VMware\Compatibility\native\wpa.dbl|2206|2011-06-19 18:27:23
C:\Documents and Settings\All Users\Application Data\VMware\Compatibility\virtual|0|2011-06-21 17:51:18
C:\Documents and Settings\All Users\Application Data\VMware\Compatibility\virtual\wpa.dbl|2206|2011-06-30 17:57:25
C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools|0|2011-06-19 18:27:42
C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\manifest.txt|1717|2011-06-19 18:27:48
C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\tools.conf|0|2011-06-19 18:27:42
C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\tools.conf.old|409|2011-06-19 18:25:44
C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters|0|2011-06-19 18:26:30
C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\adobeflashcs3.txt|1433|2010-11-19 17:46:16
C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\adobephotoshopcs3.txt|1712|2010-11-19 17:46
C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\googledesktop.txt|491|2010-11-19 17:46:16
C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\microsoftoffice2003.txt|455|2010-11-30 16:0
C:\Documents and Settings\All Users\Application
C:\Documents and Settings\All Users\Application
C:\Documents and Settings\All Users\Application
C:\Documents and Settings\All Users\Desktop|0|20
C:\Documents and Settings\All Users\Desktop\MSN
C:\Documents and Settings\All Users\Documents|0|
C:\Documents and Settings\All Users\Documents\de
C:\Documents and Settings\All Users\Documents\My
C:\Documents and Settings\All Users\Documents\My
×Ô¶¯±¸¼ü¥.txt1309428290 - Notepad
File Edit Format View Help
========== FoxMailóÊ¼þõÊºÂ ==========
========== Outlook ExpressóÊ¼þõÊºÂ ==========
========== outlookóÊ¼þõÊºÂ ==========
========== MSNõÊºÂ ==========
========== ÆäËüÃô¸ÐÐÂÏ¢ÁÐ±í ==========
001
×ÊÔ´ÃûªÆ: Passport.Net
Öµ»òÓû§: donaldtsang_1699@hotmail.com
ÃÜ Âë: passi$me
002
×ÊÔ´ÃûªÆ: donaldtsang_1699@gmail.com
Öµ»òÓû§: donaldtsang_1699@gmail.com

- **Carrying out the dynamic analysis**
  - The *injected explorer.exe* downloads *fvcwin32.exe, acvcwin32.exe and avcwin32.exe* and kick started these programs.
    - ***fvcwin32.exe*** is responsible to collect all hard disk file information and create the file "*drive*" under *C:\windows\debug*
    - ***avcwin32.exe*** is responsible to collect email accounts and passwords, SAM, system info, keeping them under a *%AppData%\temp.* They are removed immediately after after compressed and saved under *C:\windows\debug\data*. In addition, it keeps capturing screen for every 1000 ms and saves the image under C*:\windows\debug\data* folder
    - **acvwin32.exe** is to capture screenshots for every 1000ms
  - The injected "*msrvc.dll*" keep on monitoring the *c:\windows\debug\data* folder and send out any new files under the folder to CnC server, immediately deleting sent files.

Case Summary (1)

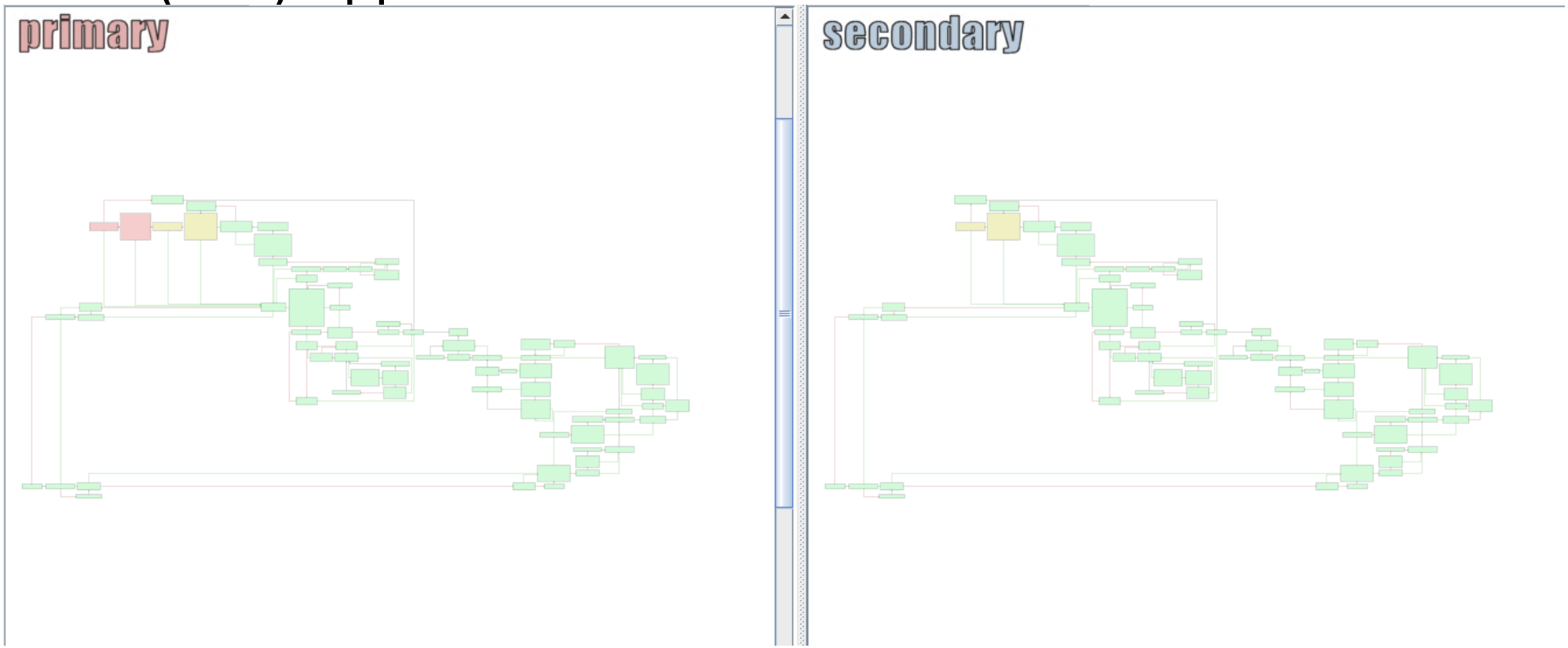
- Target political party in Hong Kong
- CnC server is in Hong Kong.
- The origin is from our mother country, China.
- **This "China-made" APT is NAPT (Non-Advanced Persistent Threat)** as we found some old routines for Win95/98. The "programmer" adds new features to it indeed and even use the same dropper in a separated collected .xls sample.

Case Summary (2)

- The ***agenda.doc*** is just packed with UPX.
- Dumping user credentials
- Using XOR instead of complicated encryption routine to encode/decode traffic to prevent from IPS/IDS detection.
- Download payload in different stages and each payload/executable is responsible for a single action.
- Use/Dependent on built-in Windows libraries
- With proper sequence number set up by CnC server to manage the victim,

Case Summary (3)

- **Same Generator** - The disassembled structure in agenda.doc matches the one in different APT sample (.exe) zipped inside a .chm file



Case Summary (4)

- This detailed case analysis is supplementary to reports published from:
  - Tracking Ghostnet http://www.infowar-monitor.net/2009/09/tracking-ghostnet-investigating-a-cyber-espionage-network/
  - Madiant http://www.princeton.edu/~yctwo/files/readings/M-Trends.pdf
- Feel free to reach me for the sample if you like.☺
- Meanwhile, do we still need to bother to do same analysis for various samples if they may come from the APT generator/taskforce? It drives our research indeed.

Case 2:
Calling from Mr. X Again

- Mr. X get many mails with suspicious attachment on or before 4 June, 1 July and LEGCO election and continue to make enquiry from me.
- The sender seems to be a staff in LEGCO council
- Anti-virus engine engaged by Gmail has not detected any issues.
- Filename written in Chinese is about “Official Reporters’ List for LEGCO Council News”

Hong Kong APT: Open it, man!

---------- Forwarded message ----------
From: Wor[redacted]i@legco.gov.hk>
Date: 2011/6/13
Subject: 責採訪立法會新聞的記者名單
To: [redacted]phk.org

謹此附上專責採訪立法會新聞的記者名單，以供參考。此名單在有需要時將予修訂。

公共資訊總主任

專責採訪立法會新聞的記者名單2011-6-12.xls
258K View Open as a Google spreadsheet Download

專責採訪立法會新聞的記者名單2011-6-12.xls
258K View Open as a Google spreadsheet Download

公義 Justice

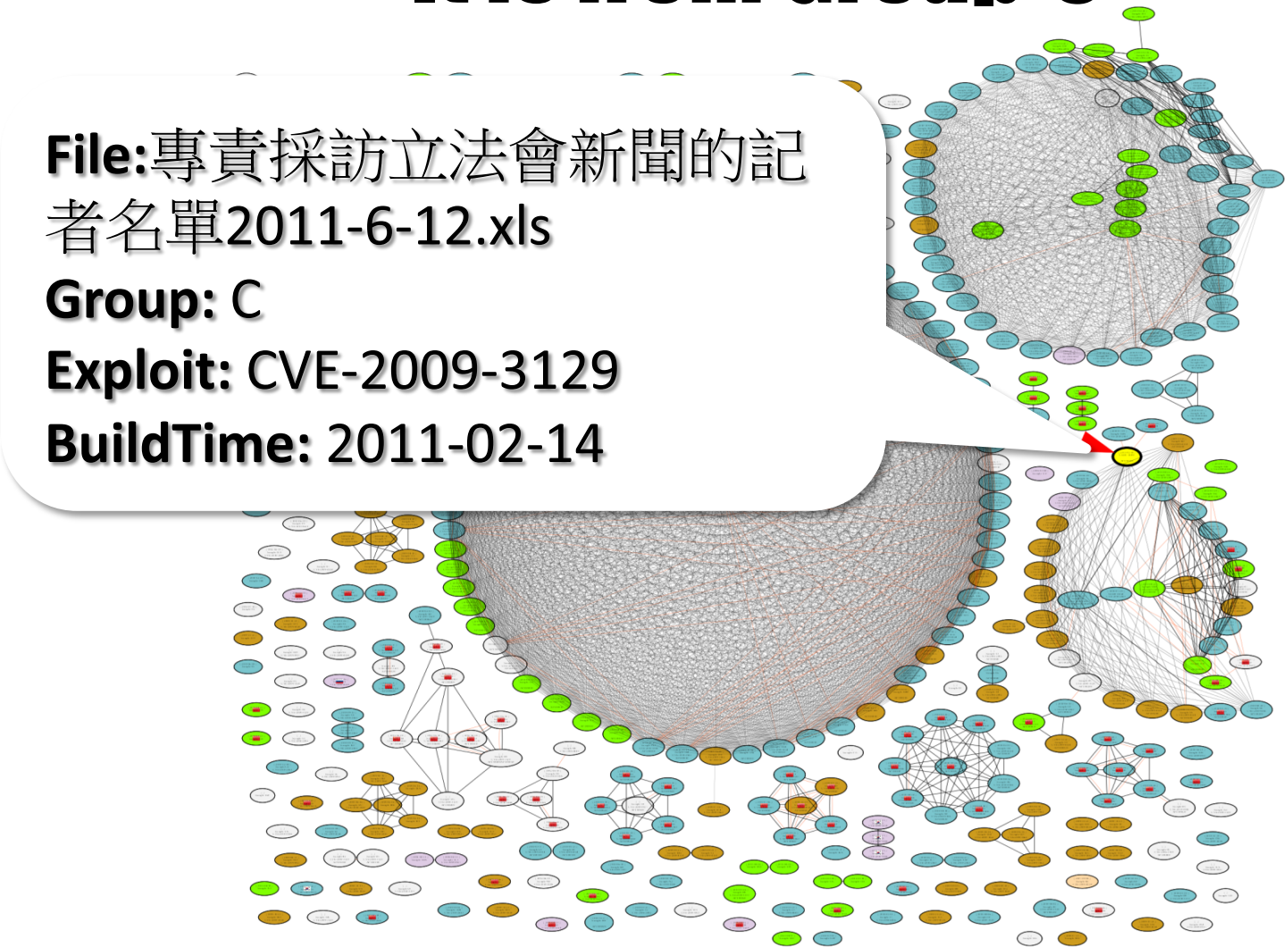
http://en.wikipedia.org/wiki/Guan_Yu

“All that is necessary for the triumph of evil is that good men do nothing” **– Edmund Burkle**

Let me take shout: “Grass Root Horse”!

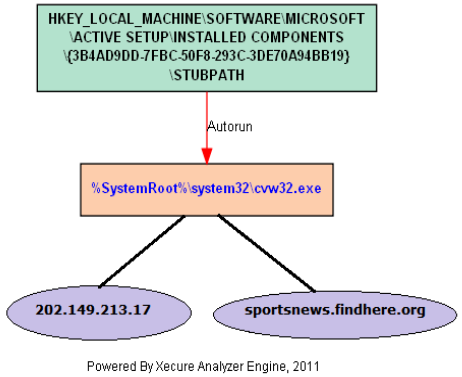
等我向他說聲”草泥馬”!

Automated Clustering: It is from Group-C



Malware of APT Group C

Malware Attack Graph



Malware Fix Suggestion

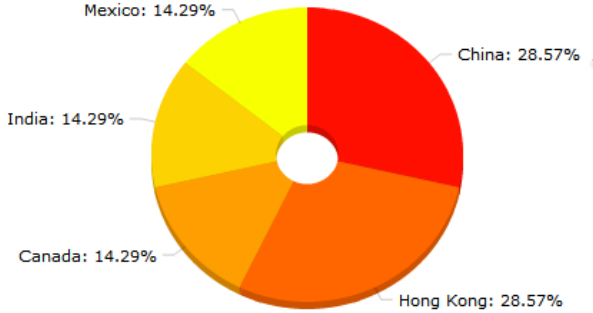
Malware Analysis Report

Time	2011-06-08 10:28:23
Duration	51 Seconds
Engine	2.9.1

%SystemRoot%\system32\cvw32.exe (8F80831DBF03CC6DECD06D82CE5E4E31)

Malware Family	
Build Time	
Malware Type	
Severity	
Behavior	• **This Malware has been identified the following behavior: Code-Injection (Target: IEXPLORE.EXE) functions.**
Modules	• Base=00140000 Size=00001000 IEXPLORE.EXE • Base=00150000 Size=00001000 IEXPLORE.EXE • Base=00E60000 Size=00001000 explorer.exe • Base=03060000 Size=00001000 explorer.exe
Files	• [EXE] **%SystemRoot%\system32\cvw32.exe** 8F80831DBF03CC6DECD06D82CE5E4E31
Autoruns	• HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\ACTIVE SETUP\INSTALLED COMPONENTS\{3B4AD9DD-7FBC-50F8-293C-3DE70A94BB19}\STUBPATH
Network	• 202.149.213.17 • sportsnews.findhere.org

C&C Location of APT Group C



28.5% C&C IP located in China

A Chinese Poem from Cao Zhi (曹植-七步成詩)

- 煮豆燃豆萁
- Cooking beans on a fire kindled with bean stalks,
- 豆在釜中泣。
- The beans weep in the pot.
- 本是同根生
- Originally born from the selfsame roots
- 相煎何太急！
- Why so eager to torture each other!

Xecure Lab

Special Thanks

• Special thanks to **Ran2 and DDL** to analyze those APT samples with me.
• Especially **Ran2** has worked on the analysis with me and got a lot juicy stuff from time to time ☺

Part 2:
Research Methodology

Research Direction (1/2)

- **We are not just focusing on a single one-off attack, we tend to observe the entire APT attack plan and trend**
  - Traditionally, we just focus on malware forensics or analyze a single victim's machine. We cannot understand the APT attack plan and its trend indeed.

Research Direction (2/2)

- **Analyze and extract features and characteristics of APT taskforce via:**
  - Malware features
  - Exploit
  - C&C Network
  - Speared Email
  - Victim's background
  - Time of attack

APT File Analysis and Grouping

- Theoretically, in an information system (i.e. malware analysis system), if we could collect all the attributes/properties of our malicious sample sets, we could identify whether the executable/ document/sample is malicious.
- However, the research issues are insufficient collection in attributes/ characteristics (for example, the malware has been packed and engage various anti-debugging capabilities), so that we get the indiscernibility relation

Standard Analysis Method

- Static Approach
  - Extract signature/features from file format
  - Reversing
- Dynamic Approach
  - Execute it under controlled environment and capture/log all the behaviors
  - Analyze networking traffic
- Challenge of Dynamic Analysis

We prefer using static analysis to prevent from Anti-VM, dormant functionality and side effect of master/bot interaction.

What APT Attributes we focused?

- We work on the analysis on multi-vector basis.

- Throughout static analysis:
  - Extract and review executable, Shellcode and PE header
  - Objects and abnormal structure in file

- Throughout dynamic analysis:
  - Install the system into Windows
    - Scan Process Memory to detect abnormal structure
    - Code-Injection, API Hooking …
  - Detect any known Code Snippet
    - Rootkit, KeyLogger, Password Collector, Anti-AV…
  - Suspicious strings: email address, domain, IP, URL

Extract Attributes from APT File

Static Analysis

Dynamic Analysis

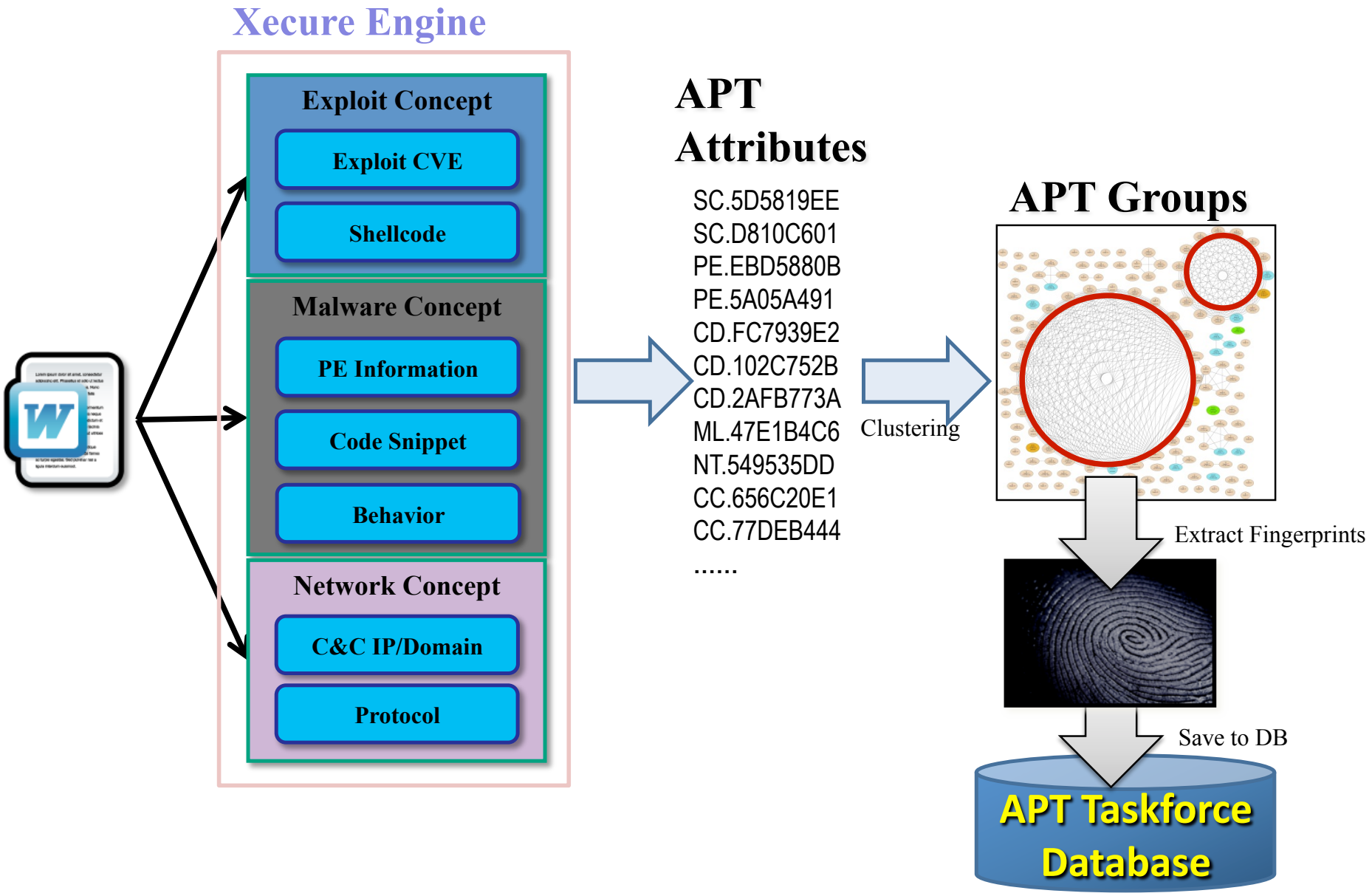
Concept	Data
CVE	CVE-2009-3129
Shellcode	Code=90903CFDEF CAPO=E2FE9071 PUCA=002191CB
Entropy	6.821483
Network	140.128.115.*** smtp.126.com test.3322.org.cn
Structure	JS=A103FE426E214CE JS=90C0C0C0C AS=32EF90183227
Malware 1	PE=EF024788 Entry=000B7324 Code=D7B5A0120987FE Code=83D2325AB5 Code=20BDCE Autorun=STARTUP_FOLDER Behavior=DLL-Injection, Password Collector
Malware 2	PE=EF93461A Entry=0003CAC0 Code=AC23109B Code=19EFAC21 Behavior=API-Hooking

Discretization

APT Attributes

SC.5D5819EE
SC.D810C601
PE.EBD5880B
PE.5A05A491
CD.FC7939E2
CD.102C752B
CD.2AFB773A
ML.47E1B4C6
NT.549535DD
CC.656C20E1
CC.77DEB444
.....

Clustering !


Xecure Engine
Exploit Concept
Exploit CVE
Shellcode
Malware Concept
PE Information
Code Snippet
Behavior
Network Concept
C&C IP/Domain
Protocol
APT Attributes
SC.5D5819EE
SC.D810C601
PE.EBD5880B
PE.5A05A491
CD.FC7939E2
CD.102C752B
CD.2AFB773A
ML.47E1B4C6
NT.549535DD
CC.656C20E1
CC.77DEB444
.....
Clustering
APT Groups
Extract Fingerprints
Save to DB
APT Taskforce Database

Part 3:
Analysis and Result

Experiment

- Mila's provided APT sample archives are confirmed to malicious
- Those archives are open to public for downloading and analysis (Collection1, 242 APT files)
- The sample archives are used by many researchers
- We highly credit to Mila’s samples

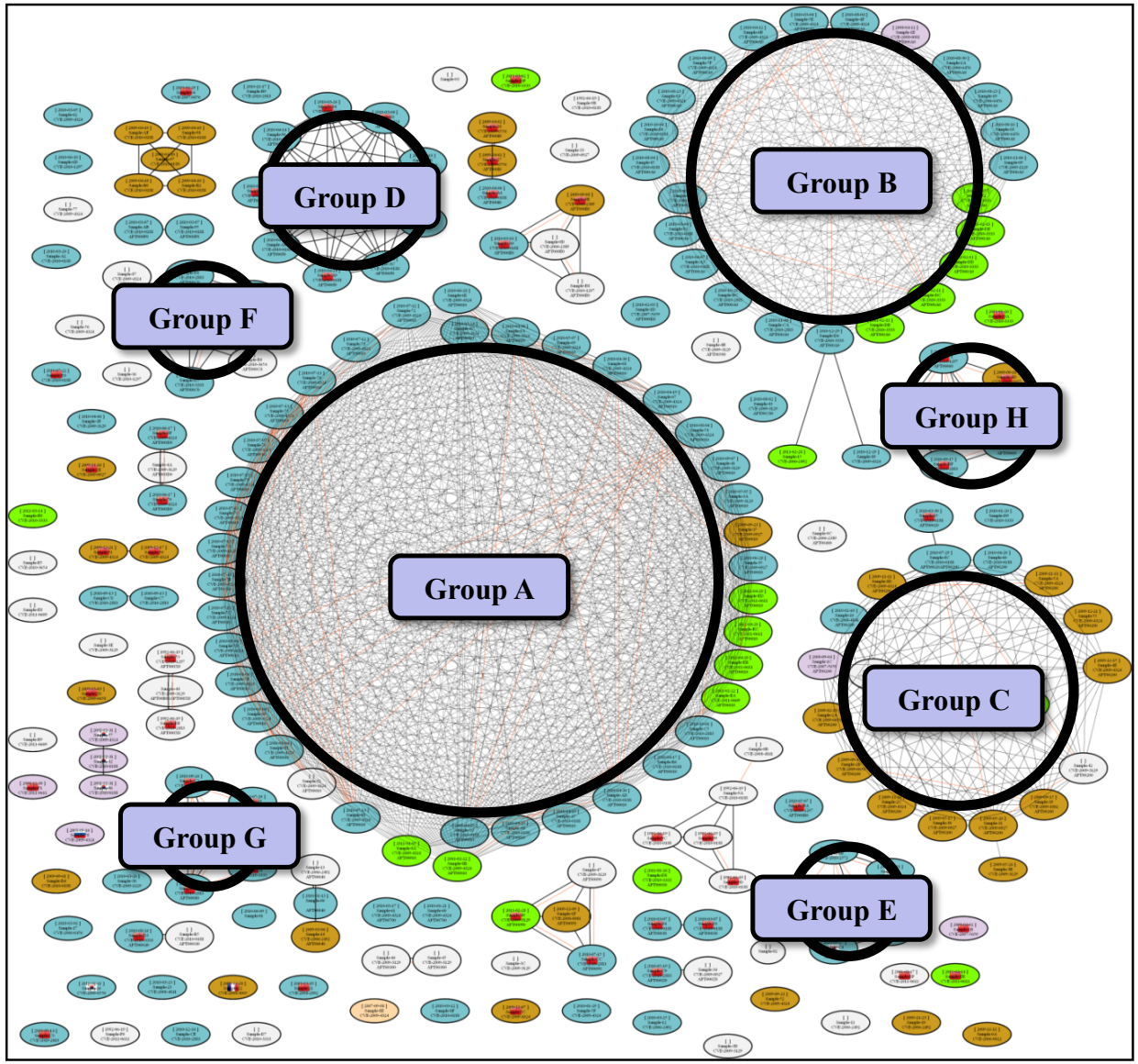
- http://contagiodump.blogspot.com/

Detection Rate

- **Xecure Inspector**
  - 94.6 % (229 / 242)

- Definition updated to 2011/6/11
  - **Microsoft Security Essentials**
    - 21.4 % (52 / 242)
  - **Sophos**
    - 35.9 % (87/242)
  - **AntiVir**
    - 56.6 % (137/242)

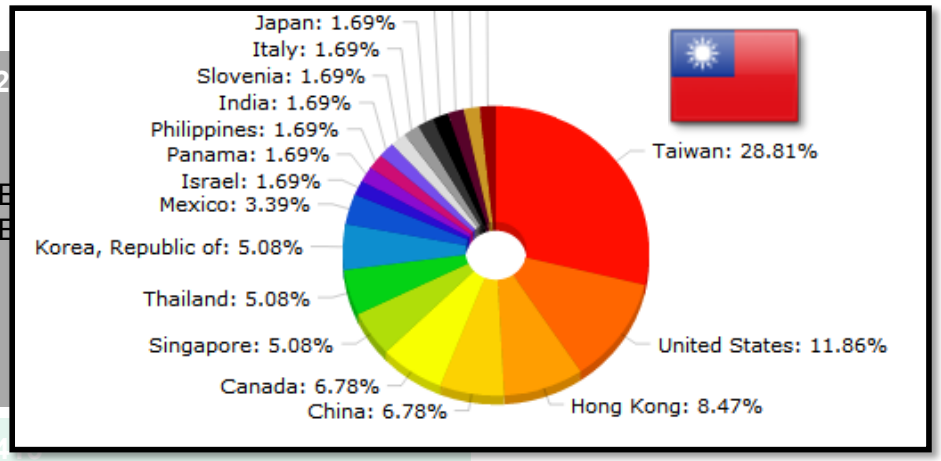
There are 8 major APT-Taskforce Groups



Groups of Mila Sample Set Collection1

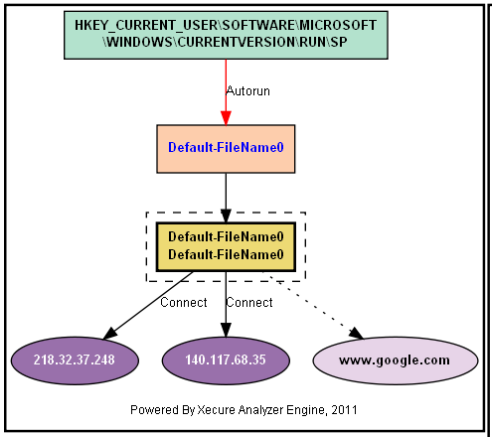
Top 3 APT Taskforce Groups

Group A	Active	2009-0923 ~ 2011-0420
	Number	40
	CVE	CVE-2009-4841, CVE-2009-0927, CVE-2009-3129, CVE-2009-4324, CVE-2010-0188, CVE-2010-2833, CVE-2011-0611, CVE-2011-0609
	Malware	APT00010
	C&C	IP:23, Domain: 5
Group B	Active	2008-0414 ~ 2011-02
	Number	26
	CVE	CVE-2006-6456, CVE CVE-2009-4324, CVE CVE-2010-3333
	Malware	APT000A0
	C&C	IP:23, Domain:4
Group C	Active	2008-0904 ~ 2011-04
	Number	21
	CVE	CVE-2007-5659, CVE-2008-4841, CVE-2009-1862, CVE-2009-3129, CVE-2009-4324, CVE-2009-0658, CVE-2009-0927,
	Malware	APT00200
	C&C	IP:5, Domain:11



Malware of APT Group A

Malware Attack Graph



Malware Fix Suggestion

Malware Analysis Report

Time	2011-06-08 09:49:41
Duration	84 Seconds
Engine	2.9.1

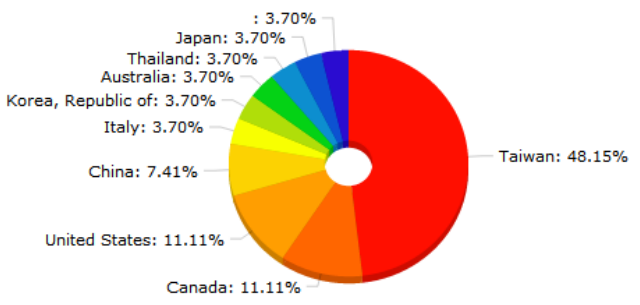
Default-FileName (6DE7186AAD5C3AA496B5BE8EAA2BC838)

Malware Family	
Build Time	2010-07
Malware Type	
Severity	★★
Behavior	• **This Malware has been identified the following behavior: Password Collection functions.**
Modules	• Base=00400000 Size=0000C000 Default-FileName
Files	• [EXE] **Default-FileName** 6DE7186AAD5C3AA496B5BE8EAA2BC838
Autoruns	• HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\SP
Network	• 140.117.68.35 • 218.32.37.248 • www.google.com

Bot Command

/get Remote Local
/rsh [SHELL FILE]
/shr [wins.exe]
/put Local Remote
/run Program
/sleep MINIUTES

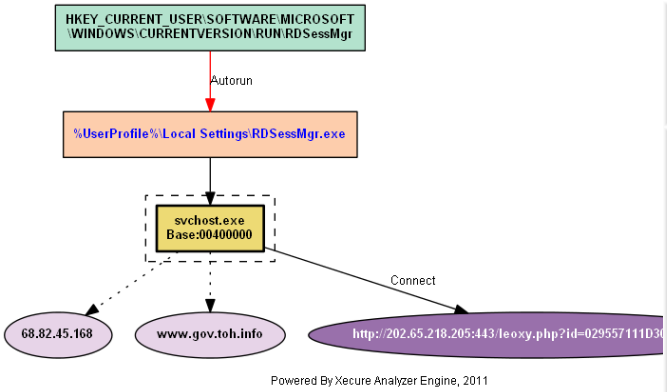
C&C Location of APT Group A



48.1% C&C IP located in Taiwan

Malware of APT Group B

Malware Attack Graph



Malware Fix Suggestion

Malware Analysis Report

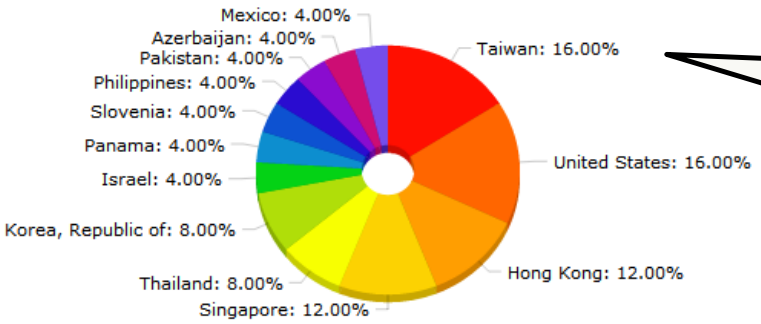
Time	2011-06-08 09:41:35
Duration	74 Seconds
Engine	2.9.1

%UserProfile%\Local Settings\RDSessMgr.exe (F23A421D1DD02D060F35D25341BAB003)

Malware Family	[redacted]
Build Time	2010-03
Malware Type	**China Spyware**
Severity	★★

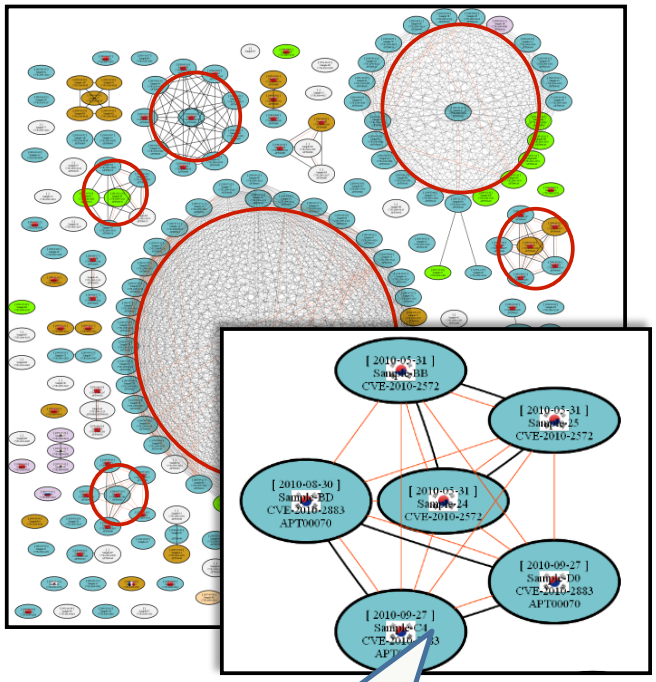
Behavior	• **This Malware has been identified the following behavior: Code-Injection (Target: svchost.exe) functions.**
Modules	• Base=00400000 Size=00005000 svchost.exe
Files	• [EXE] **%UserProfile%\Local Settings\RDSessMgr.exe** F23A421D1DD02D060F35D25341BAB003
Autoruns	• HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\RDSessMgr
Network	• 68.82.45[redacted] • http://202.65[redacted]3/leoxy.php?id=029[redacted]f4ee • www.gov.toh.info

C&C Location of APT Group B



16% C&C IP located in Taiwan

Malware of Group E



Group-E
Language = Korean

VIRUS TOTAL

Virustotal is a **service that analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

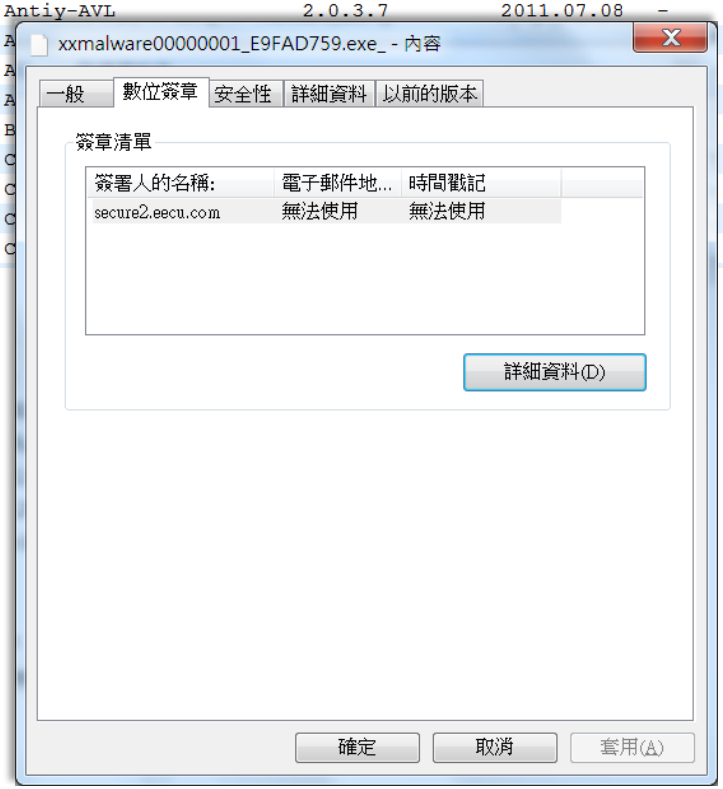
0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name: **xxmalware00000001_E9FAD759.exe_**
Submission date: **2011-07-08 08:00:23 (UTC)**
Current status: **finished**
Result: **1/ 42 (2.4%)**

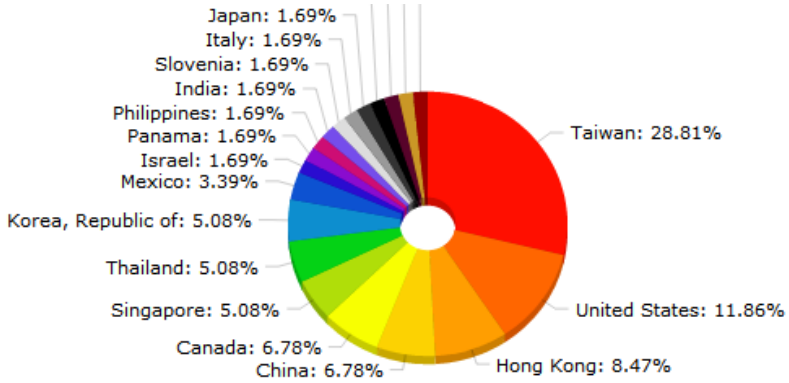
VT Community
not reviewed
Safety score: -

Compact | Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.07.08.01	2011.07.08	-
AntiVir	7.11.11.29	2011.07.08	TR/Dropper.Gen
Antiy-AVL	2.0.3.7	2011.07.08	-



All (A,B,C)


Japan: 1.69%
Italy: 1.69%
Slovenia: 1.69%
India: 1.69%
Philippines: 1.69%
Panama: 1.69%
Israel: 1.69%
Mexico: 3.39%
Korea, Republic of: 5.08%
Thailand: 5.08%
Singapore: 5.08%
Canada: 6.78%
China: 6.78%
Taiwan: 28.81%
United States: 11.86%
Hong Kong: 8.47%


Greenland
Suomi Finland
Sverige Sweden
Norge Norway
Россия Russia
United Kingdom
Polska
France
Україна Ukraine
Kazakhstan
Mongolia
España Spain
Italia Italy
Iraq
Iran
China
Japan
North Pacific Ocean
Canada
United States
North Atlantic Ocean
Algeria
Libya
مصر Egypt
Saudi Arabia
India
Thailand
Mali
Niger
Chad
Sudan
Nigeria
Ethiopia
Kenya
DR Congo
Tanzania
Angola
Namibia
Botswana
South Africa
Madagascar
Indian Ocean
Indonesia
Papua New Guinea
Australia
New Zealand
South Pacific Ocean
Venezuela
Colombia
Brasil Brazil
Perú
Bolivia
Chile
Argentina
South Atlantic Ocean

Findings from Mila Sample Set (1/2)

- Our analysis against Mila Sample set could identify 8 major APT taskforces.

- There are around 12 different CVEs and exploits are identified.

- We have found that even APT taskforce uses 8-9 different exploits, however, the type of malware used is limited to a few one. There is no surprise at all ☺

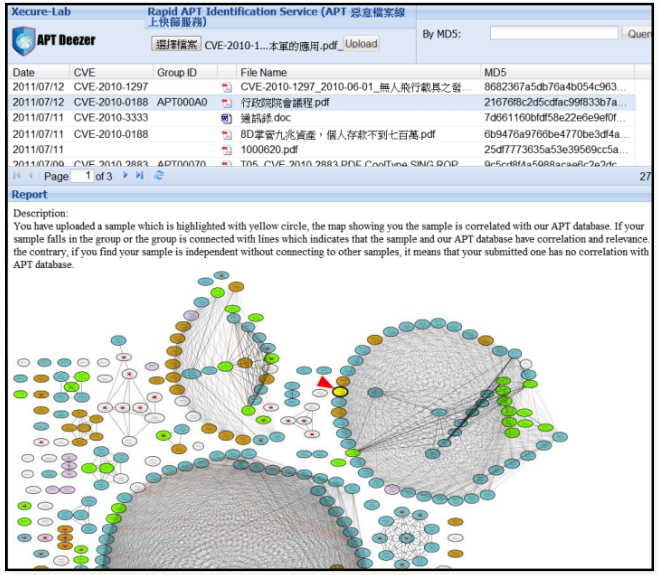
- We identify APT Taskforce based on CnC server location and malware they have used. The exploit the taskforce used is not very related to our analysis.

Findings from Mila Sample Set (2/2)

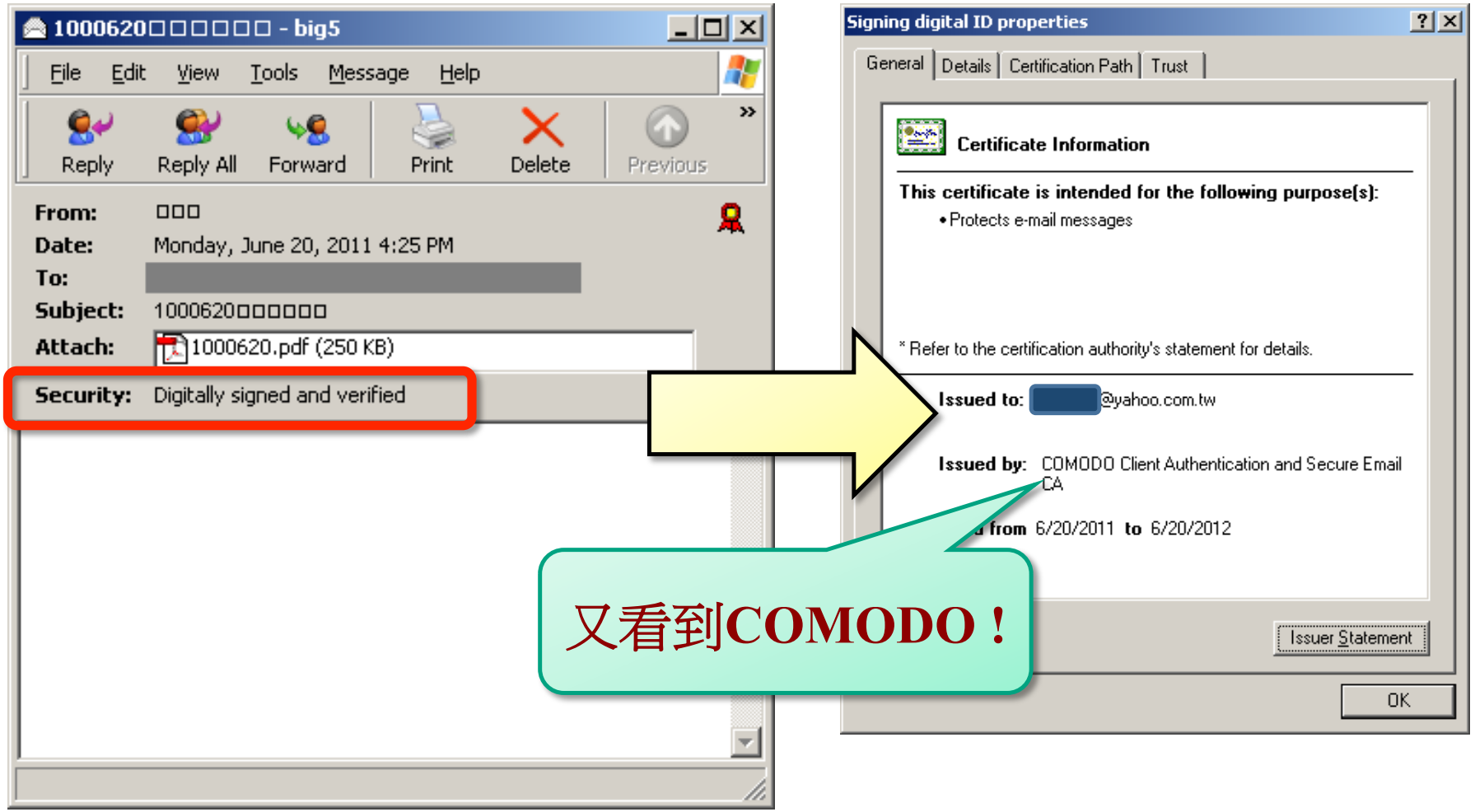
- Language used in APT sample：
  24% of the samples is from China 
- 3.9% of the samples is from Korean  ，
- We also found some are from Russia  與 France 
- APT CnC server location Top 3 Ranking:
  - Taiwan (28%) 
  - US
  - Hong Kong (HK is readily another CnC heaven, come on, babe ☺)

Xecure-Lab : APT-Deezer
Rapid APT Identification Service

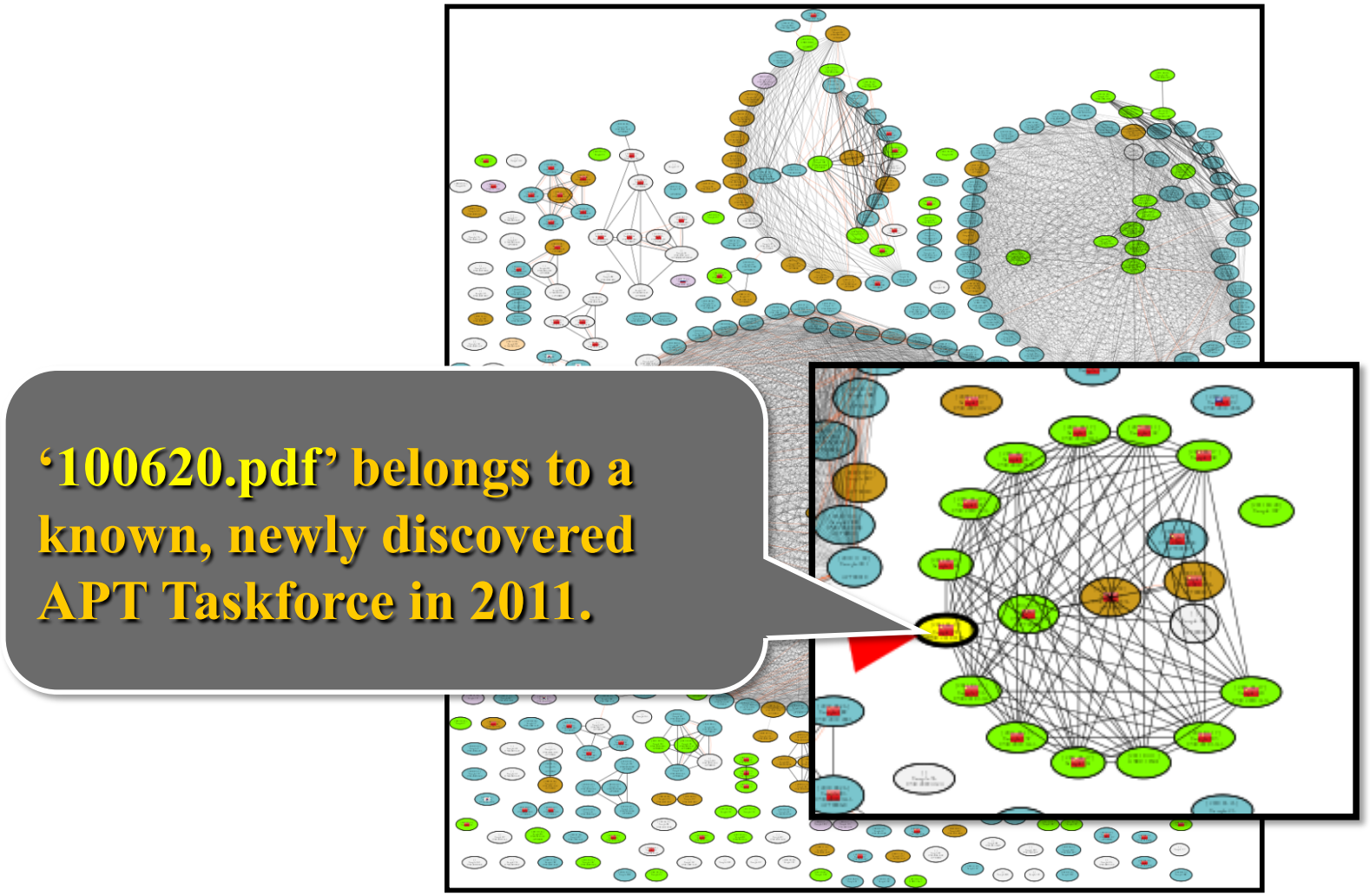
- **APT-Deezer provides a free online service to check whether your submitted sample whether it is an APT sample**
  - We tak Mila sample set as the base training set
  - Identify Exploit CVE and Malware family
  - Zero-Day Exploit detection and analysis
  - APT Malware sample DNA analysis and comparison
  - APT sample clustering and grouping
  - Support file formats including DOC,PPT,XLS,PDF,RTF
- URL: http://aptdeezer.xecure-lab.com



Case Study (1/3)
Target Attack Mail has been signed !?

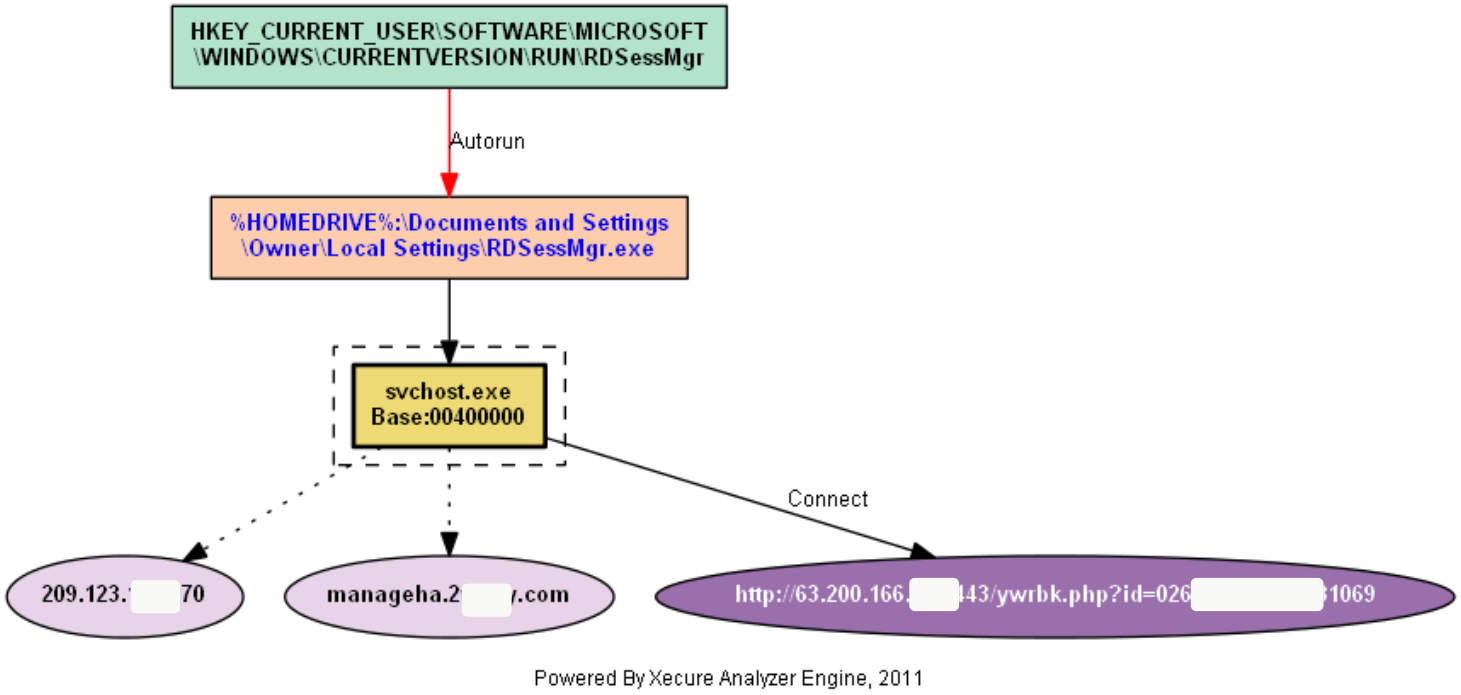


(2/3) Identify the APT Taskforce Group



(3/3) Identify the APT Taskforce Group

- But Malware is a known family, it is same as APT-Group-B !



Thank you for your listening

- Xecure Lab (http://www.xecure-lab.com)
- We keep collecting samples for analysis.
- Enhance the capability to analyze and observe APT DNA family in more accurate manner.
- It is an incremental efforts made to the Malware Analysis community.
- Together, we make homeland secured.

Special Thanks

- Every members in Xecure Research Team and Mila as well as everyone has contributed ideas to us.
- Our family and fellows

Finally

Blackhat review board members,

are you convinced yet? ☺