ASEC Report 11월

® ASEC Report

2003. 12

안철수연구소의 시큐리티대응센터(Ahnlab - Security E-response Center)는 악성 코드 및 보안위협으로부터 고객을 안전하게 지키기 위하여 바이러스와 보안 전문가들로 구성되어 있는 조직이다.

이 리포트는 ㈜안철수연구소의 ASEC에서 국내 인터넷 보안과 고객에게 보다 다양한 정보를 제공하기 위하여 바이러스와 시큐리티의 종합된 정보를 매월 요약하여 리포트 형태로 제공하고 있다.

SUMMARY

AgoBot 웜 변형 다수 발견으로 웜 발견이 트로이목마보다 높아….

작년초부터 시작된 신종 트로이목마의 발견 건수가 이번달은 AgoBot 웜 변형이 다수 발견되어 그 순위가 바뀌는 현상이 발생했다. 메일이 아닌 네트워크라고 함축되는 전파경로를 가진 이 웜들은 변형이 많이 발견되고 있으며 또한 이와 유사한 아류작의 웜들도 계속 출현하고 있어 사용자들의 주의가 요구된다.

과거에는 웜이 메일로만 전파되는줄 알았지만 모두 옛이야기가 되버렸다. 웜은 이제 자신을 복제할 수 있는 곳이라면 어디든지 사용자의 관리소홀과 취약점을 이용하여 메일보다 빠르게, 사용자들이 눈치채지도 못하게 보안이 허술한 시스템을 감염시킬 수 있게 되었다. 즉, 과거의 웜이 수동적이였다면 현재의 웜들은 능동적으로 자신을 복제할 시스템을 찾고 보안이 허술한 시스템을 감염시키는 것이다.

안철수연구소를 비롯한 다양한 보안 및 안티 바이러스 업체가 윈도우 NT 기반 시스템의 관리소홀과 취약점으로 발생할 수 있는 문제점을 언급하고 있지만 여전히 많은 사용자들은 관리지식의 부족으로 AgoBot 과 같은 악성코드에 감염된 시스템을 안고 살아가고 있다.

이번달 ASEC Report 에서는 AgoBot 웜의 변형들의 다수 발견으로 인한 소식과 왜 감염이 많은지에 대한 문제점을 알아보고 신규보안 취약점에서는 Workstation 서비스 취약점, Linux Kernel 의 특정취약점을 이용하여 메모리 조작을 통한 시스템 Crash, Root 권한 획득의 문제점에 대하여 알아본다. 끝으로 테크니컬 칼럼에서는 요즘 문제시되고 있는 애드웨어의 설치확인과 제거를 통하여 대처할 수 있는 방법을 알아 보기로 한다.

I. 11월 악성코드 Top 10

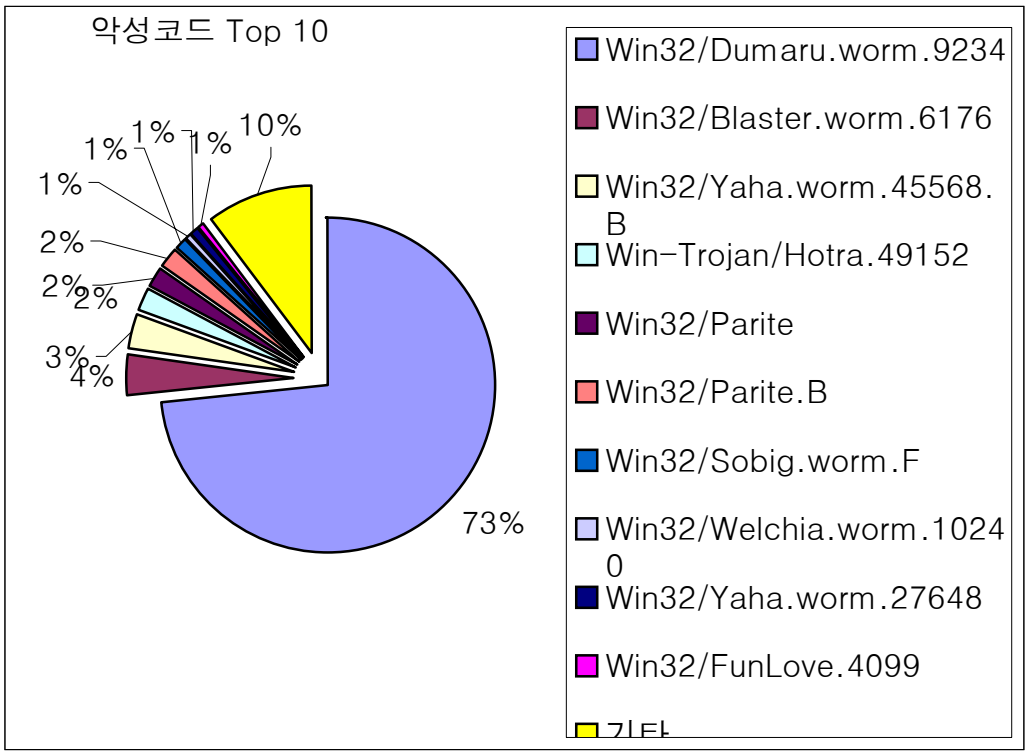
작성자 : 정진성 연구원

바이러스명	건수	%
Win32/Dumaru.worm.9234	9,796	73.2%
Win32/Blaster.worm.6176	547	4.1%
Win32/Yaha.worm.45568.B	445	3.3%
Win-Trojan/Hotra.49152	280	2.1%
Win32/Parite	275	2.1%
Win32/Parite.B	246	1.8%
Win32/Sobig.worm.F	139	1.0%
Win32/Welchia.worm.10240	103	0.8%
Win32/Yaha.worm.27648	81	0.6%
Win32/FunLove.4099	80	0.6%
기타	1,388	10.4%
합계	13,380	100

[표1]

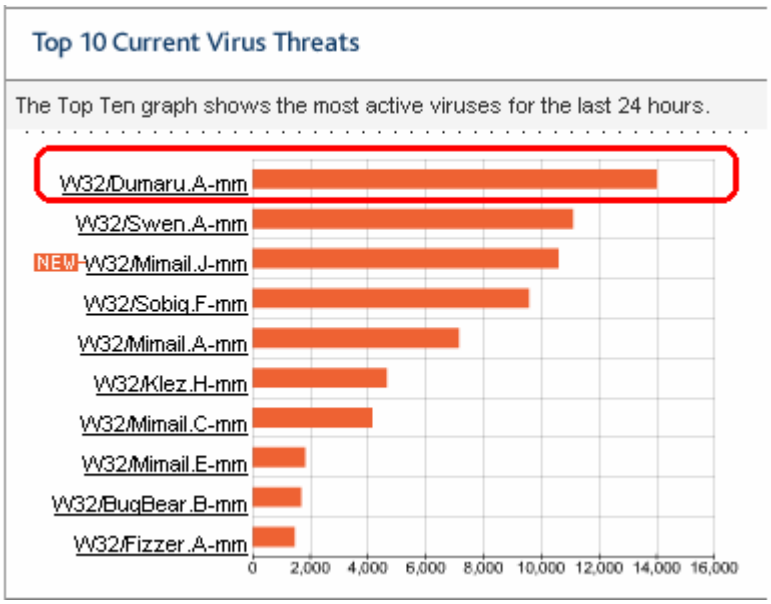
이번달은 9월과 10월을 비교해서 볼 때 9, 10월에 Top 10 에 포함된 몇몇 악성코드들이 빠지고 기존에 알려진 구종의 악성코드들이 다시 Top 10 에 포함되었다. 그 만큼 다시 이 해당 악성코드의 문의가 많았다는 것이다. 그 예로 Win32/FunLove.4099 , Win32/Sobig.worm.F 등을 들 수가 있겠다.

또한 Win32/Dumaru.worm.9234 의 경우 이상할 만큼 문의 건수가 높아졌다. 이 건수는 실제 감염된 시스템에서 (발송 대상 시스템의 IP 를 확인하기는 어려웠다.) 직접 연구소의 바이러스 신고를 받는 계정으로 접수된 수치이다. 즉, 고객의 문의도 포함된 경우도 있겠지만 실제로는 감염된 시스템에서 해당 계정으로 보낸량이 더 많다는 얘기이다. 이 웜의 건수가 높은건 비단 연구소의 통계뿐만은 아니다. [표1]의 차트로 정리된 것을 보면 다음과 같다.



[표2]

다음은 본 문서를 편집한 12월 4일 현재 MessageLab 의 Top 10 현황을 보자.



[표3]

Dumaru 웜의 수치가 높은 것을 알 수가 있다. 이 웜은 자체 SMTP 기능을 이용하며 다음과

같은 확장자에서 메일주소를 수집하여 발송하게 된다.

- htm, .wab, .html, .dbx, .tbb, .abd

전파방법으로 볼 때는 그리 특이할만한 점은 없다. 단지 위 확장자에서 메일주소를 수집할 경우 윈도우 주소록(아웃룩 주소록)에서 수집된 것보다는 더 많은 불특정 다수에게 발송할 수 있게 된다. 하지만 이 방법은 Dumaru 만의 고유 전파방법은 아니다. 참고로 웜은 마이크로소프트사의 패치로 위장하고 있기도 하다.

위 글에서 기술한 것처럼 10월과 비교해보면 다음과 같은 악성코드들이 Top 10 에 포함되었다.

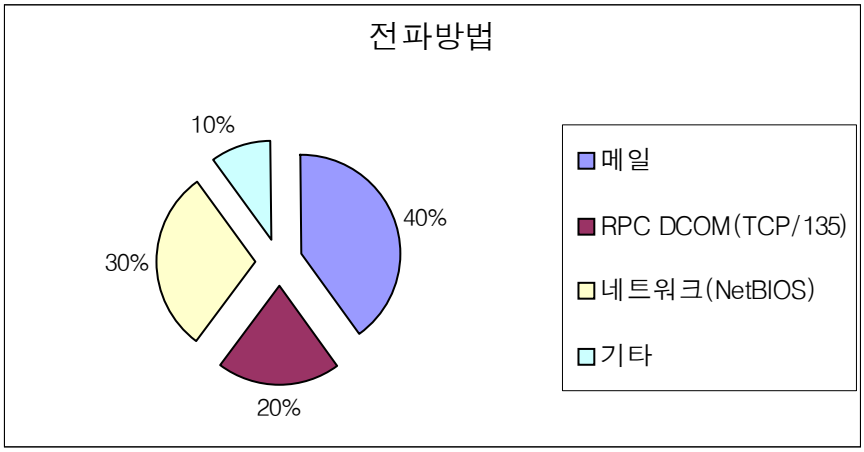
- Win32/Sobig.worm.F
- Win32/FunLove.4099

여기서 짚고 넘어가야 할 현상이 하나 있다. 바로 Win32/Sobig.worm.F 가 그것이다. 이 웜은 2003년 9월 10일 이후로는 실행은 되지만 자신을 전파시키는 루틴은 동작이 안되도록 되어있다. 하지만 10월, 11월에도 이 웜이 꾸준히 발견되고 있는 원인은 무엇일까? 대다수의 안티 바이러스 전문가들은 시스템 날짜가 잘못된 것을 우선으로 꼽고 있다.
9월 10일이란 날짜는 현재 날짜를 체크 하는것은 아니고 감염된 시스템의 날짜로 체크하기 때문에 현재 감염되어 웜을 발송하는 시스템들은 모두 날짜가 잘못 설정되었다는 얘기이다.

그러면 Top 10 에 속해 있는 악성코드들의 전파방법은 어떠한 유형을 가지고 있을까?
이번달 경우 크게 다음과 같이 분류되며

- 메일
- RPC DCOM 취약점 (TCP/135)
- 네트워크 (NetBIOS), (null Session)
- 기타 (감염파일 직접실행 등)

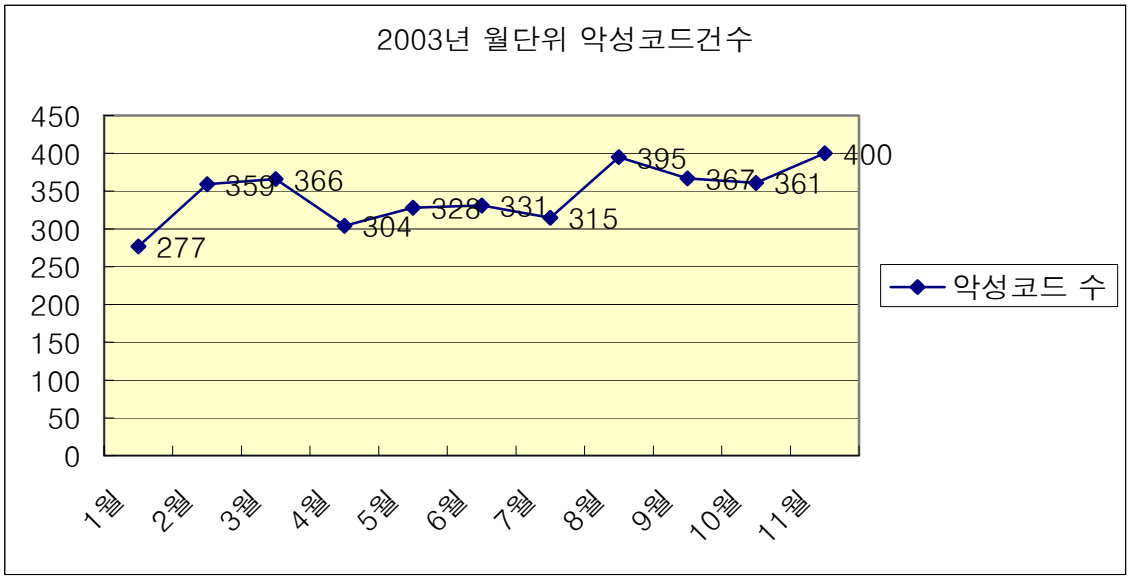
이를 표로 나타내면 [표4] 와 같다.



[표4]

[표4]처럼 11월달의 악성코드의 전파형태는 크게 '메일' 과 '네트워크' 로 나누어 지고 있다. 특히 현재는 메일로 전파되는 신종 악성코드의 발견건수는 그리 많지가 않다. Win32/Dumaru.worm.9234 처럼 구종의 악성코드가 그 순위를 차지 하고 있을 뿐이다. 대다수의 악성코드들은 메일보다는 RPC DCOM 관련 취약점이나 null session 을 이용한 전파형태가 더 많이 보고되고 있다. 더 깊은 얘기는 신종 악성코드 동향 부분에서 하기로 한다.

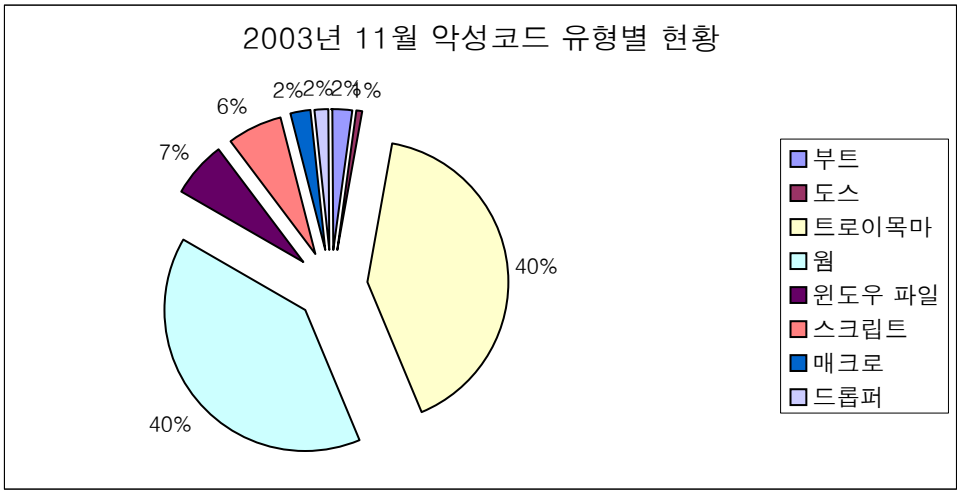
11월 문의된 총 악성코드의 숫자는 400건이다. 이는 10월과 비교하면 약 50건 정도가 늘어난 수치이다. 이는 곧 그 만큼 다양한 종류의 악성코드들이 사용자로부터 보고되고 있고 또한 그 피해문의도 다양하다는 것이다. 올 1월부터 11월까지의 문의된 악성코드의 종류수를 나타내보도록 하겠다. [표5] 와 같다.



[표5]

평균적으로 매달 345 종류의 다양한 악성코드의 문의가 접수된 것을 알 수가 있다. 대부분이 Top 10 또는 20 내의 악성코드 관련 문의가 대부분이겠지만 매달 문의되는 악성코드 수가 평균 345 종류라면 정말로 다양한 악성코드들이 사용자들에게 피해를 입히고 있다고 볼 수 있겠다.

그렇다면 이러한 악성코드들은 주로 어떤 유형들인지 [표6]을 통해서 알아보자.



[표6]

전반적으로 피해문의의 대다수가 '웜과 트로이목마' 에 집중되어 있는 것을 볼 수가 있다. 이들 대부분은 IRCBot 류의 웜 또는 트로이목마들이 대부분이다. 위 전파방법에도 설명했듯

이 현재 악성코드 제작자들 사이에서 RPC DCOM 관련 취약점이나 관리목적 공유폴더의 null session 을 이용한 전파 방법의 인기는 식을 줄을 모른다. 안타까운 현실이지만 이것은 여전히 많은 사용자들이 보안패치나 로그인 암호에 대하여 소홀히 하고 있다는 것이다.

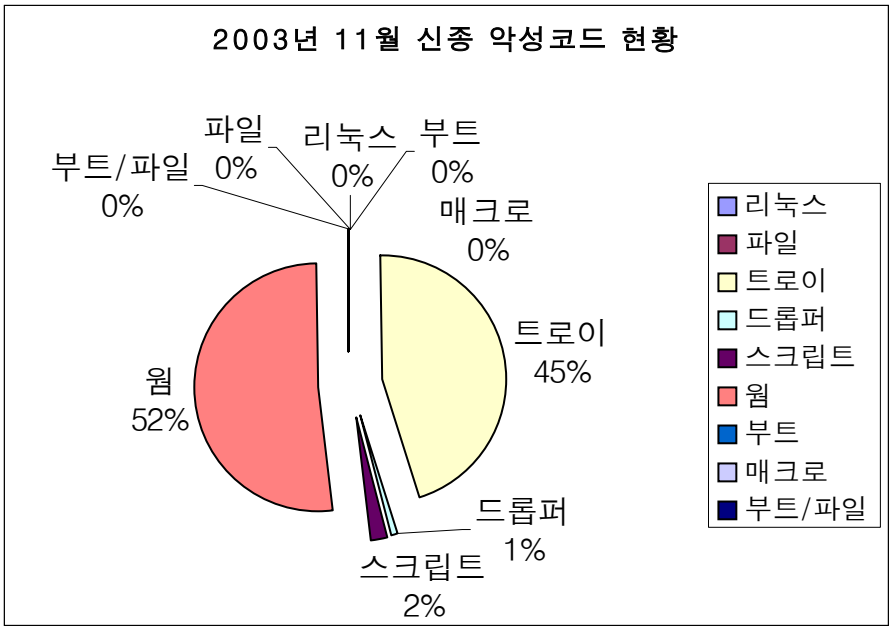
II. 11월 국내 신종 악성 코드 발견 동향

작성자 : 정진성 연구원

11월 한달 동한 접수된 신종 악성코드의 건수는 [표7, 8]과 같다.

리눅스	파일	트로이	드롭퍼	스크립트	웜	부트	매크로	부트/파일	합계
0	0	50	1	2	58	0	0	0	111

[표7]



[표8]

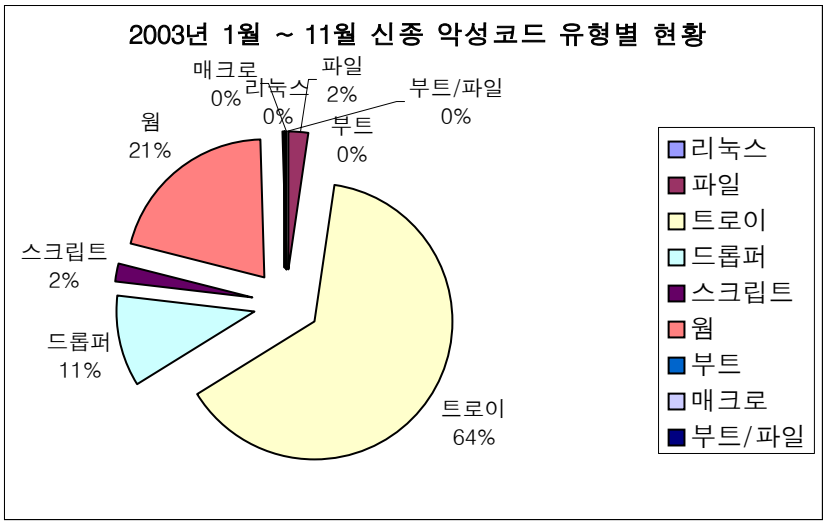
이번달 신종 악성코드 동향은 올해의 어느 달과는 조금 다르다. 그것은 바로 10월까지는 발견된 악성코드들 (대부분 웜과 트로이목마들)중 매번 트로이목마가 발견건수 1위를 차지하였는데 이번 달은 웜이 트로이목마에 비하여 약간 더 많이 발견, 보고된 것이다. 또한 이것은 올해 신종 웜의 발견 건수로는 Top 을 차지한 것 이다. [표10]을 보면 자세히 알 수가 있다.

월	리눅스	파일	트로이	드롭퍼	스크립트	웜	부트	매크로	부트/파일	합계
1월		7	50	18	3	7				85
2월		2	78	15	3	13	1	1		113
3월	2	3	76	24	1	12				118
4월		1	46	11	3	11				72
5월		4	39	14	2	13				72
6월		2	52	6	4	21				85
7월		3	59	4	1	10				77
8월		2	92	13	3	20				130
9월		1	78	7	2	28				116
10월			57	3		29				89
11월			50	1	2	58				111
합	2	25	677	116	24	222	1	1	0	868

[표9]

이번달에 웜이 많았던 이유는 발견된 웜의 종류 중 대부분을 차지하는 것은 Win32/AgoBot.worm 변형들이였다. 아울러 보고된 다른 웜들 대부분들이 모두 이와 유사한 IRCBot 기반의 웜들이라는 것이다.

다음은 [표9]를 기반으로 한 그래프이다.



[표10]

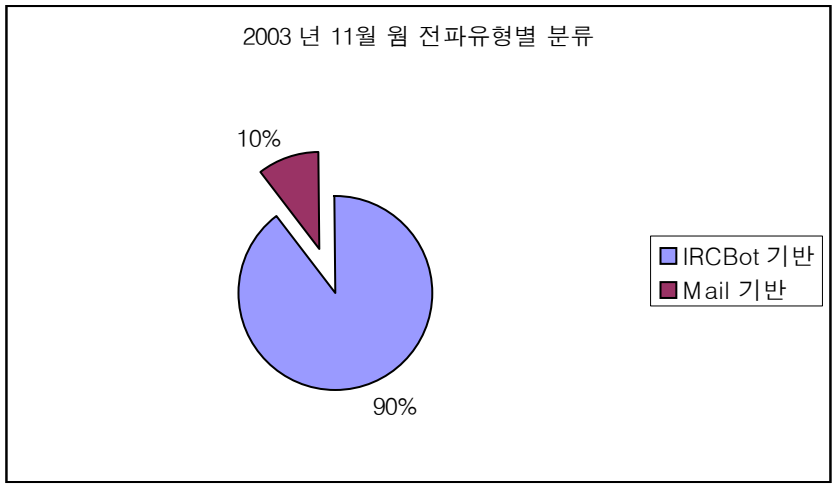
위 글에서도 언급한 것 처럼 이번달의 전체 악성코드 피해문의 통계와 현재 기술중인 신종

악성코드의 통계는 비슷한 점이 있는데 그것은 바로 트로이목마의 건수와 웜의 건수가 대략 비슷해졌다라는는 점이다. 올해는 어느달과 비교해봐도 웜이 트로이목마보다 많이 발견된 적은 없었다. 필자의 기억으로는 메일로 퍼지는 Mass Mailer 가 맹위를 떨쳐던 때 처럼 다시금 (IRCBot 기반의)웜의 전성기 돌아오지는 않았나 생각이 들 정도이니 말이다. 그 만큼 AgoBot 류의 변형이 많아지고 있다는 것이다.

전파유형은 그때 처럼 Mass Mailer 형태가 아닌 네트워크로 전파되는 IRCBot 형태라는게 다르며 주목할 만 점이라 하겠다. 우리는 [표8]에서 신종 악성코드의 유형을 알아보았다. 그렇다면 가장 많은 분포를 보이는 웜에 대한 자세한 전파방법에 따른 유형별 분류를 나누어 보자.

* 총 58 개의 신종(변형 포함) 웜이 보고되었고 다음과 같이 분류된다.

- IRCBot 기반의 웜
- Mail 기반의 웜

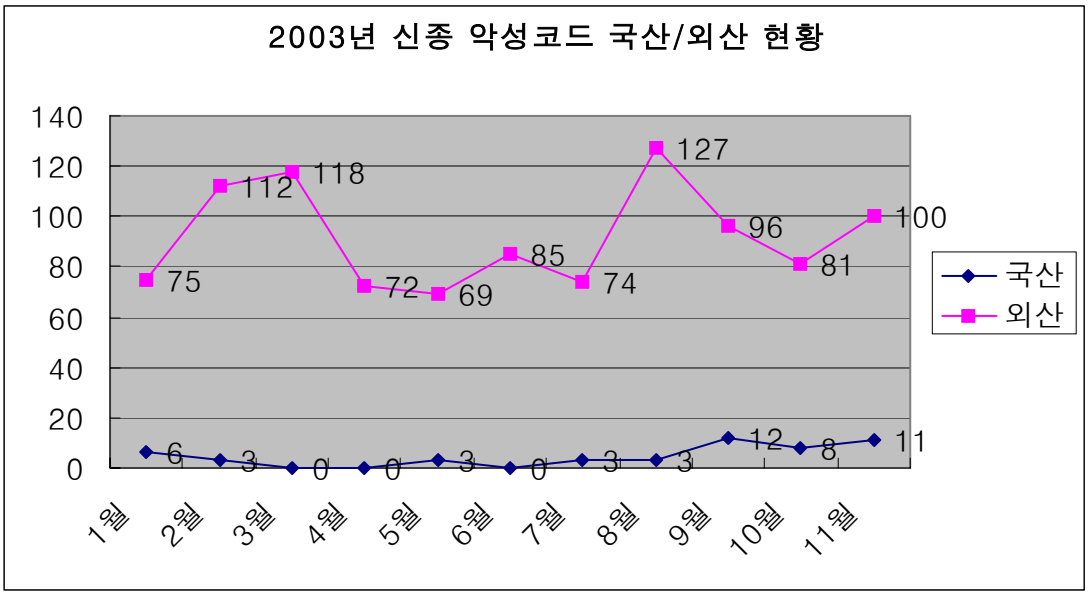


[표11]

위 표에서도 볼 수 있듯이 현재 웜의 경향은 '둘 중에 하나'라는 것인데 이전처럼 P2P 웜, 메신저 웜, 등 다양한 형태는 볼 수는 없다는 것이다. 어떻게 생각해 보면 그 만큼 해당 응용 프로그램 사용자의 리스크가 줄어들었다고도 볼 수 있지만 실은 그렇지 않을 것으로 본다. 왜냐하면 해당 웜들에 대한 리스크가 줄어들었을지는 몰라도 해당 응용 프로그램을 사용하지 않아도 보안패치가 안된 윈도우 환경이라면 어떤 IRCBot 가 침입하려고 할지 모르기 때문이다. 대다수의 사용자들이 윈도우 2000 이상 기반의 OS 를 사용하고 있으며 감염된 대부분의 사용자는 관리지식의 부족으로 인하여 보안패치나 암호설정등에 소홀히 하고 있고

제작자들은 바로 이러한 것을 놓치지 않기 때문으로 본다.

끝으로 11월달 신종 악성코드의 국/외산의 분포는 [표12] 와 같다.



[표12]

이번 달에도 역시 국산제작의 악성코드가 지난달과 비교하여 약간 늘었다. 지난달에도 설명했듯이 모두 국산 스팸 메일러 변형들의 영향으로 건수가 약간 증가하였다.

이 스팸 메일러는 국내 유명 채팅 사이트의 게시판에 클라이언트와 서버 파일을 올려두고 현재 정확한 경로는 알려지지 않았지만(광고 메일 또는 이전에 설치된 Sinmsn, Smibag 웜 등) Active X 를 이용하여 파일을 설치하고, 변형된 파일을 계속 게시판등에 업로드하면서 릴리즈 되고 있다.

과거에 스팸 메일은 단지 1회성 광고만을 위한 수단으로 사용되었는데 요즘 스팸 메일은 해당 메일을 클릭 했을 때 Active X 를 이용한 설치나 IFRAME 태그등을 이용하여 창을 최소화하여 특정 사이트를 오픈 후 역시 Active X 를 이용하여 광고 프로그램을 (소위 애드웨어 불리우는) 설치하게 하여 사용자에게 불편을 줄 수도 있는 수단으로도 변화되었다.

스팸메일은 메일함에서 메일을 삭제하면 되기에 일반 사용자도 쉽게 제거 할 수 있었지만 위와 같은 프로그램 설치로 인한 광고노출로 인하여 업무 생산성 저하 및 원한지 않은 사이트로의 이동으로 인한 심리적인 불쾌감을 유발하는등이 문제시 되고 있다. 또한 사용자는 이런 상황에 대처하기 어려우므로 안티 바이러스 업체들은 '애드웨어'라는 진단명으로 이런류

의 프로그램을 쉽게 진단하고 제거할 수 있도록 엔진에 추가하고 있는 실정이다.

III. 11월 신규 보안 취약점

작성자 : 조경원 연구원

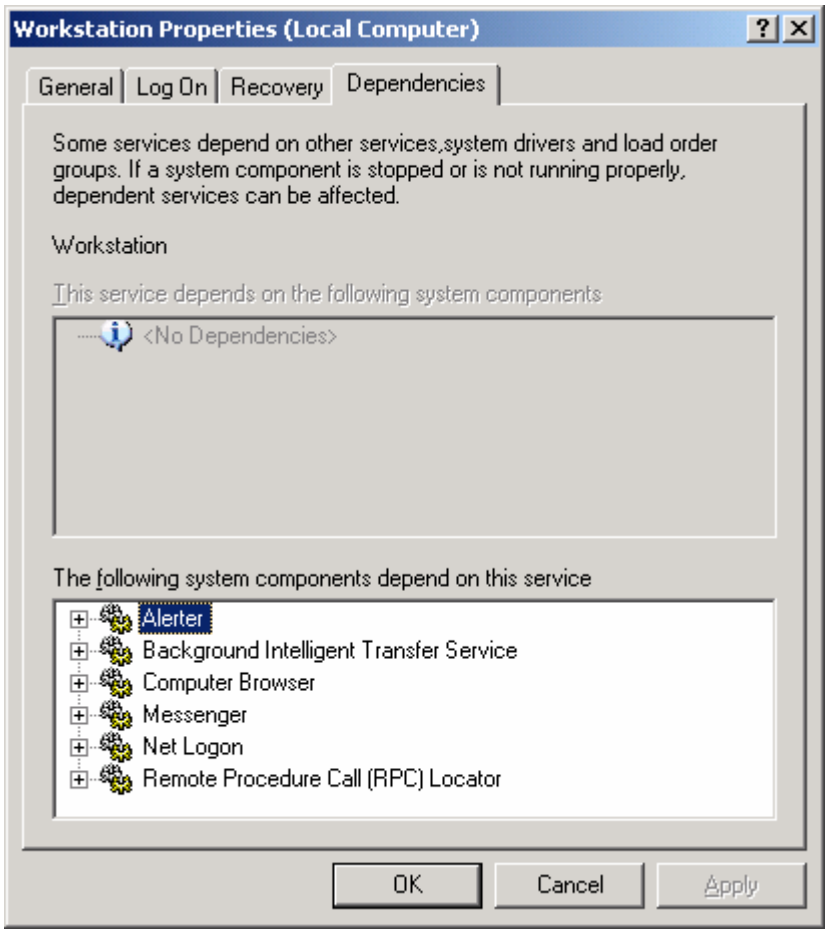
- Workstation 서비스 취약점

개요

11월 12일 MS03-049의 이름으로 MS에서는 위험 등급은 "긴급"의 Windows XP, 2000에 해당되는 취약점 및 패치를 발표하였다. Workstation서비스는 2000, XP 시스템에서 기본적으로 실행되는 서비스로 TCP 포트 139, 445 를 사용하여 접근이 가능하다. 공격자는 이 포트를 사용하여 악의적인 코드를 전송할 경우 Buffer Overflow 취약점이 발생하며 이를 이용하여 시스템에 장애를 주거나 시스템 내부에 명령을 실행 시킬 수 있다.

Workstation 서비스란...

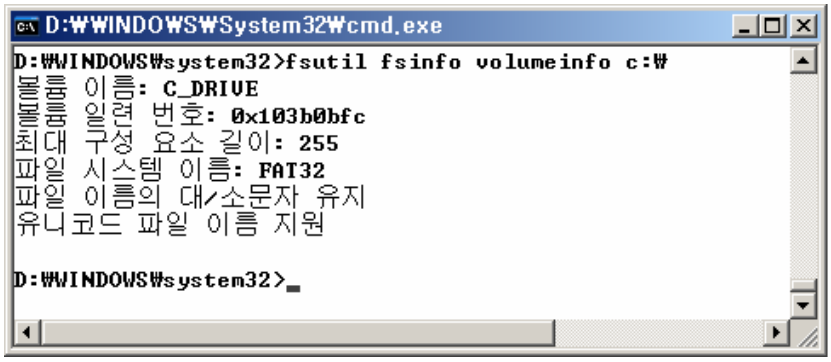
Windows Workstation 서비스는 인터넷에 연결된 공유파일, 네트워크 프린터등의 외부에 연결된 자원에 대한 연결을 지원하는 서비스이다. 주변 Windows시스템과 파일공유, 프린터 등을 사용하지 않더라도 다른 많은 서비스와 프로그램이 이 Workstation서비스와 연관성을 갖고 있어 Windows시스템에서는 반드시 사용되어지는 서비스라 할 수 있다. 인터넷에 연결되어 있지 않는 환경에서는 이 Workstaion서비스를 중지(Disable)시켜도 상관없지만 실제 이럴경우 많은 프로그램에서 오동작이 발생할 수 있다.
Workstaion서비스에 종속적인 서비스는 다음의 [그림1] 처럼 Workstation서비스의 "종속성" 탭을 통하여 확인할 수 있다.



[그림1]

취약점 발생원인

Workstation 서비스는 WKSSVC.DLL에서 지원하며 TCP 135, 139포트의 DCE/RPC 프로토콜을 통해 접근할 수 있다. WKSSVC.DLL에서 제공하는 몇몇 네트워크 관리 함수는 오류 발생시 %SYSTEM%₩debug 디렉토리에 로그파일을 생성하며 알려지지 않은 특정 RPC call을 비정상적으로 실행시에 vsprintf()함수를 사용하여 로그파일을 기록하게 된다. 이때 문자열이 지정된 버퍼보다 클 경우 Buffer Overflow가 발생하게 된다.
로그파일 생성은 시스템 디렉토리가 NTFS인 경우에는 ACL에 의하여 생성되지 않으므로 실제 공격은 다음의 [그림2]와 같은 FAT32를 사용하는 시스템에서 가능하다.



[그림2]

알려진 공격 코드

현재 두가 지의 알려진 공격코드가 존재하며 영문 2000 SP1과 영문 2000 SP4에 대한 내부 명령 실행 코드가 있으며 Workstation 서비스를 중지시키는 DoS 공격 코드가 알려져 있다. 공격코드를 확장하면 기타 버전의 OS에 대한 공격코드를 만들 가능성이 있다.

해결방법

Workstation 서비스를 Stop시키는 것으로 막을 수 있지만 이 경우에는 시스템이 비정상적으로 동작할 수 있다.
근본적인 취약점 제거를 위해서는 MS03-049 패치를 적용하여야 한다.
http://www.microsoft.com/korea/technet/security/bulletin/MS03-049.asp

참고URL

CERT Advisory CA-2003-28: Buffer Overflow in Windows Workstation Service
http://www.cert.org/advisories/CA-2003-28.html

Vulnerability Note VU#567620: Microsoft Windows Workstation service vulnerable to buffer overflow when sent specially crafted network message
http://www.kb.cert.org/vuls/id/567620

워크스테이션 서비스의 버퍼 오버런으로 인한 코드 실행 문제(828749)
http://www.microsoft.com/korea/technet/security/bulletin/MS03-049.asp

Buffer Overrun in the Workstation Service Could Allow Code Execution (828749)
http://www.microsoft.com/technet/security/Bulletin/MS03-049.asp

ASEC Advisory
http://info.ahnlab.com/securityinfo/user_seccontent.jsp?seq=5212

- Linux kernel do_brk() 취약점

개요

9월경 Linux kernel 2.4버전 대에서 Kernel 함수인 do_brk()함수의 문제점이 발견되었다. 해당 문제점은 2.4.23버전에서 Fix되었으며 보안취약점이 아닌 일반적인 잘못된 코딩으로 처리되었으며 기타 외국 Advisory에도 해당 부분이 보고되지 않았다. 11월 24일 Linux 벤더인 Debian의 몇몇 서버가 해킹당하여 조사되는 과정중 12월 1일 do_brk() 함수의 문제를 사용하여 공격한 것이 밝혀 지면서 이에 대하여 알려지게 되었다.
이 취약점은 Linux Kernel 내부코드의 잘못된 설계로 인한 취약점으로 일반유저가 Kernel 메모리에 직접 접근할 수 있다.
Kernel 메모리의 접근을 통하여 시스템을 Crash시키거나 메모리조작을 통한 root권한 획득이 가능하다. 현재까지 알려진 공격방법은 Local상에서만 가능하며 remote에서는 불가능하므로 일반계정을 통해 Login을 하여야만 이 공격 가능하다.

취약점 발생원인

Linux Kernel에는 brk()라는 시스템 콜이 있으며 해당 시스템 콜에서는 do_brk()하는 함수가 존재한다. do_brk()함수는 ELF, a.out등의 실행파일을 실행시에 메모리에 로딩하는 역활을 하며 do_brk()함수내의 처리부분에서 메모리크기를 적절하게 검사하지 못하여 Kernel영역의 메모리까지 접근 가능할 수 있다. Kernel메모리는 OS자체의 코드들과 정보가 포함되어 있어 일반유저는 접근이 불가능하며 이 취약점을 사용하여 일반 유저가 메모리에 write할 경우 시스템이 crash되거나 root획득 등의 작업을 할 수 있다.

알려진 공격 코드

현재 rebooting을 유도하는 공격코드가 알려져 있으나 Debian 사의 시스템을 크래킹한 사례가 있으므로 실제 공격코드가 존재하는 것으로 추정된다.

해결방법

Kernel자체를 Upgrade하여야 하며 2.4.23이상 버전의 Kernel에서 취약점이 제거된다.

Linux Kernel

http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.23.tar.bz2

RedHat Linux
http://rhn.redhat.com/errata/RHSA-2003-392.html

참고URL

취약점 CVE
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0961

ASEC Advisory
http://info.ahnlab.com/securityinfo/user_seccontent.jsp?seq=52128

Ⅳ. 테크니컬 컬럼 – 애드웨어 확인/제거

작성자 : 차민석 연구원

1. 애드웨어

2003년 11월 8일 발생한 Win-Trojan/Hotra.49152(http://info.ahnlab.com/smart2u/virus_detail_1240.html)는 애드웨어의 문제점 중 하나를 보여줬다. 이 애드웨어의 오동작으로 많은 시스템의 웹 브라우저 속도가 느려지는 문제가 발생했다. 이미 ASEC 리포트 Vol.04(2003년 10월호)에서 애드웨어에 대해 알아봤고 현재 대다수의 백신에서 애드웨어 진단/치료(삭제) 기능이 없는 상태에서 사용자가 수작업으로 애드웨어를 제거해야 하는 경우가 많다.

2. 애드웨어 설치 확인/제거

인터넷 익스플로러의 시작홈페이지 주소를 변경한 후에도 특정 사이트가 지속적으로 연결되거나, 특정 사이트 오픈 시 여러 개의 웹 브라우저 창이 동시에 오픈 되는 경우에는 다음의 사항을 확인하면 된다.

1. 애드웨어 확인 및 제거

1) 최신 엔진으로 업데이트 된 V3제품으로 검사하여 바이러스, 웜, 트로이목마와 같은 악성 코드가 있는지 확인한다. 수동 검사의 '검사 파일 형식'은 반드시 '모든 파일'로 설정한다. V3에서 진단되는 파일이 있다면 치료(삭제) 한다.

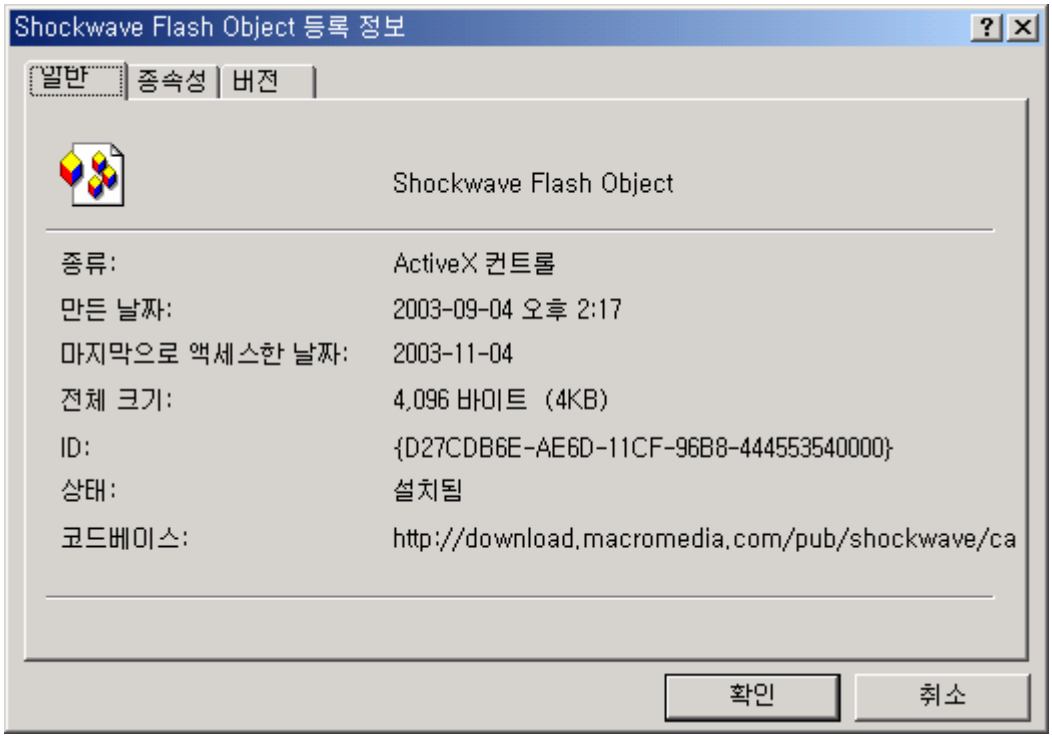
2) [시작]-[설정]-[프로그램 추가/제거]에서 시스템과 관련이 없고 본인이 설치한 적이 없는 프로그램이 설치되어 있는지 살펴본 후 삭제한다.

3) 임시 인터넷 파일을 모두 제거한다. 제거방법은 [인터넷 익스플로러 실행]-[도구]-[인터넷 옵션]-[임시 인터넷 파일]에서 '파일 삭제', '쿠키 삭제'를 선택하고 삭제하면 된다. '쿠키 삭제' 버튼이 바로 보이지 않는다면 [임시 인터넷 파일]-[설정]-[파

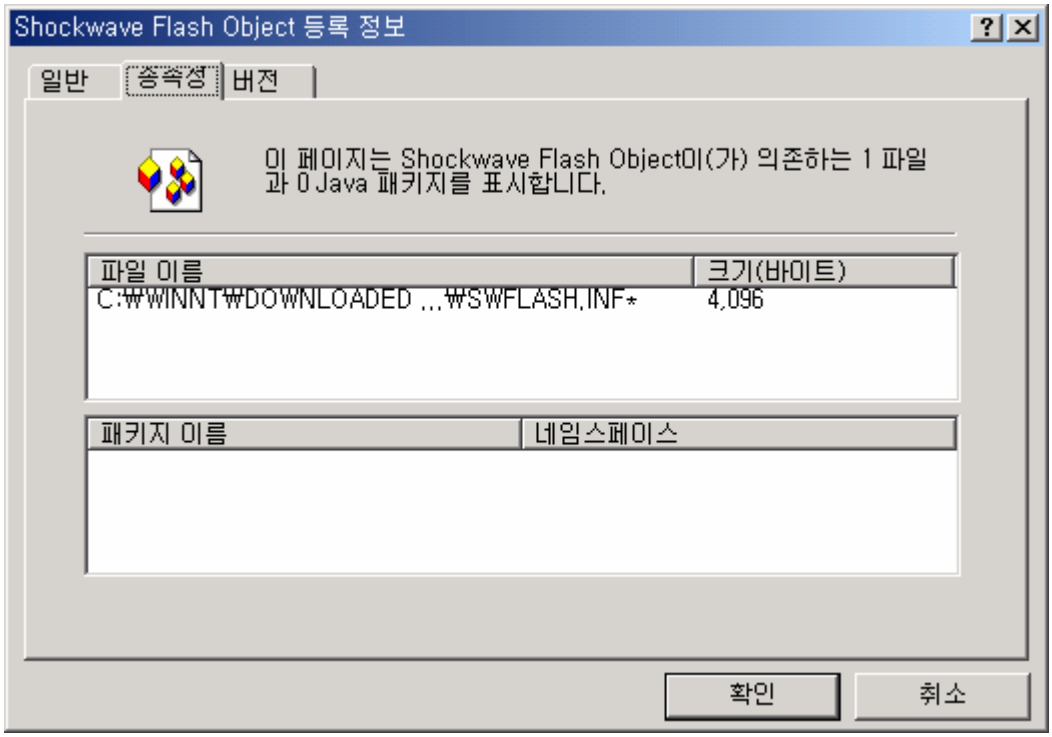
일보기]에서 열린 탐색기 창 내의 모든 파일을 제거해 하면 된다.

4) 윈도우(일반적으로 C:₩Windows나 C:₩WinNT)의 'Downloaded Program Files' 폴더에서 불필요하게 설치된 프로그램을 찾아 삭제한다. '프로그램 파일'에서 오른쪽 마우스 버튼을 눌러 [속성(R)]을 선택하면 '코드베이스' 항목에 프로그램 설치 위치를 알 수 있다. 출처를 정확히 알지 못할 경우 오른쪽 마우스 버튼을 눌러 '제거(R)'를 통해 삭제한다.

주 : 그림에서 사용된 내용은 정상 액티브 X로 애드웨어와 관련이 없다.



[그림3] 코드베이스를 통해 원본 위치를 확인



[그림4] [종속성]을 통해 관련된 프로그램 확인 가능

[그림5] 버전을 통해서도 출처 확인 가능

5) 실행 중인 프로세스에서 불필요한 프로그램이 존재한다면 종료하고 해당 파일을 삭

제한다. 윈도우 부팅 시 자동으로 시작하게 등록할 수 있는 레지스트리인 HKEY_LOCAL_MACHINE₩Software₩Microsoft₩Windows₩Currentversion₩run 등에서 등록된 항목들을 살펴보면 특정 파일이 심어져 있는 것을 확인할 수 있다. 윈도우 2000이라면 [Ctrl]+[Alt]+[Del]키를 누른 후 관련 프로세스를 종료시키고 해당 파일을 지우면 된다.

6) 보안 취약점이 존재해 감염되는 경우도 있으므로 윈도우 업데이트를 통해 자동으로 감염되는 것을 예방 할 수 있다. [시작]-[Windows Update]나 [인터넷 익스플로러 실행]-[도구]-[Windows Update]-[업데이트 검색]-[업데이트 검토 및 설치]를 통해 보안 패치를 적용한다

이와 같은 과정에도 문제를 해결하지 못할 경우에는 안리포트(AhnReport) 프로그램을 이용해 결과를 안철수연구소(v3sos@ahnlab.com)로 보내면 된다. 안철수연구소에서 제공하는 안리포트는 사용자의 시스템 정보를 수집하는 역할을 수행하는 프로그램으로 이를 통해 문제 원인과 신종 악성 코드를 추적하는 목적으로 사용된다. 안철수연구소 고객지원(http://info.ahnlab.com/customer/ahnreport.html) 혹은 기업고객지원(http://b2b.ahnlab.com/customer/ahnreport.html)에서 파일을 다운로드 받을 수 있다.

2. 추가 조치 방법

애드웨어를 삭제했는데도 애드웨어에서 변경한 값들이 그대로 존재한다. 이때 다음 레지스트리의 내용을 자신에 맞게 수정하는 게 좋다.

1) 웹 브라우저 홈페이지 변경

(1) [시작]-[실행]을 선택한 후 'regedit' 입력하고 확인을 누른다.
(2)HKEY_CURRENT_USER₩Software₩Microsoft₩Internet explorer₩Main₩Start page = '등록되어 있는 값 삭제 후 원하는 값으로 설정'

2) 애드웨어에서 자주 변경하는 레지스트리 값

애드웨어는 다음 레지스트리의 내용을 주로 변경하므로 이들 내용도 확인해 불필요한 내용이 존재하면 지워준다.

HKEY_CURRENT_USER₩Software₩Microsoft₩Internet Explorer₩Main]
"Start Page"=

[HKEY_LOCAL_MACHINE₩Software₩Microsoft₩Internet Explorer₩Main]
"Start Page"=

[HKEY_CURRENT_USER₩Software₩Microsoft₩Internet Explorer₩Main]
"Search Page"=

[HKEY_CURRENT_USER₩Software₩Microsoft₩Internet Explorer₩Main]
"Search Bar"=

[HKEY_CURRENT_USER₩Software₩Microsoft₩Internet Explorer]
"SearchURL"=

[HKEY_CURRENT_USER₩Software₩Microsoft₩Internet Explorer₩Search]
"CustomizeSearch"=

[HKEY_CURRENT_USER₩Software₩Microsoft₩Internet Explorer₩Search]
"SearchAssistant"=

[HKEY_LOCAL_MACHINE₩Software₩Microsoft₩Internet Explorer₩Main]
"Search Page"=

[HKEY_LOCAL_MACHINE₩Software₩Microsoft₩Internet Explorer₩Main]
"Search Bar"=

[HKEY_LOCAL_MACHINE₩Software₩Microsoft₩Internet Explorer]
"SearchURL"=

[HKEY_LOCAL_MACHINE₩Software₩Microsoft₩Internet Explorer₩Search]
"CustomizeSearch"=

[HKEY_LOCAL_MACHINE₩Software₩Microsoft₩Internet Explorer₩Search]
"SearchAssistant"=

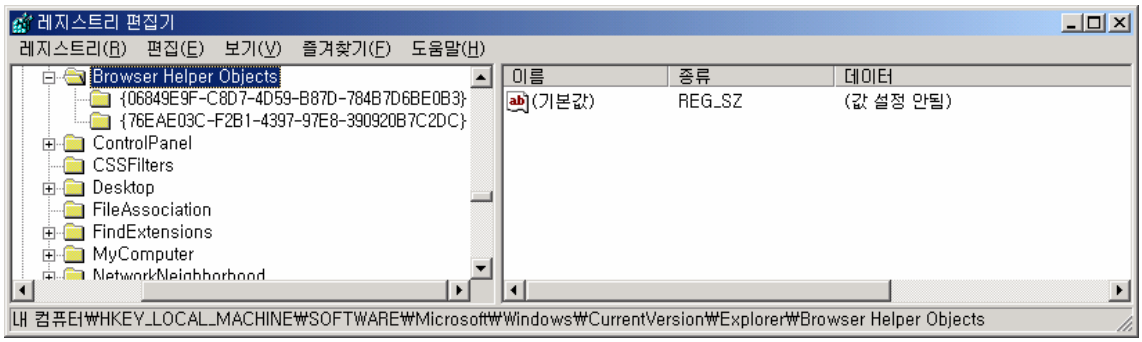
[HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Internet Explorer/Main]
"Default_Page_URL"=

[HKEY_CURRENT_USER/Software/Microsoft/Internet Explore/Main]
"Start Page"=

3) Browser Helper Objects

A. Browser Helper Objects 확인

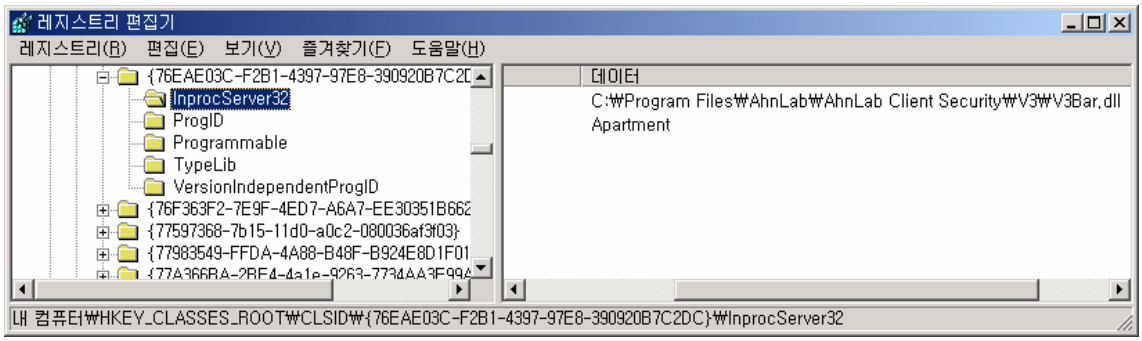
많은 애드웨어가 인터넷 익스플로러의 'Browser Helper Objects'(이하 BHO) 기능을 이용한다. BHO를 사용하면 인터넷 익스플로러의 여러 행동을 감시하고 다른 행동을 할 수 있다. 예를 들어 사용자가 특정 사이트 주소를 입력할 때 중간에서 가로채 다른 웹사이트로 이동 할 수도 있다. 특정 사이트 노출로 광고를 해야 하는 애드웨어로써는 유용한 기능이다. BHO 사용 여부는 레지스트리 에디터(regedit.exe)를 실행 해 'HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩Browser Helper Objects'에 등록된 CLSID 값을 확인한다. [그림6] 에서는 {06849E9F-C8D7-4D59-B87D-784B7D6BE0B3}와 {76EAE03C-F2B1-4397-97E8-390920B7C2DC}가 사용 중임을 알 수 있다.



[그림6] Browser Helper Objects 확인

B. CLSID 내용 확인

HKEY_CLASSES_ROOT₩CLSID₩{CLSID 값}의 "InprocServer32"키 값을 통해 해당 기능을 사용하는 파일 이름을 알 수 있다. 그림에서는 V3Bar.dll 파일이 사용하고 있음을 알 수 있다. 참고로 해당 파일은 V3에서 사용하는 파일이다.



[그림7] 해당 CLSID 값을 통해 사용 프로그램 확인

C. 불필요한 CLSID 삭제

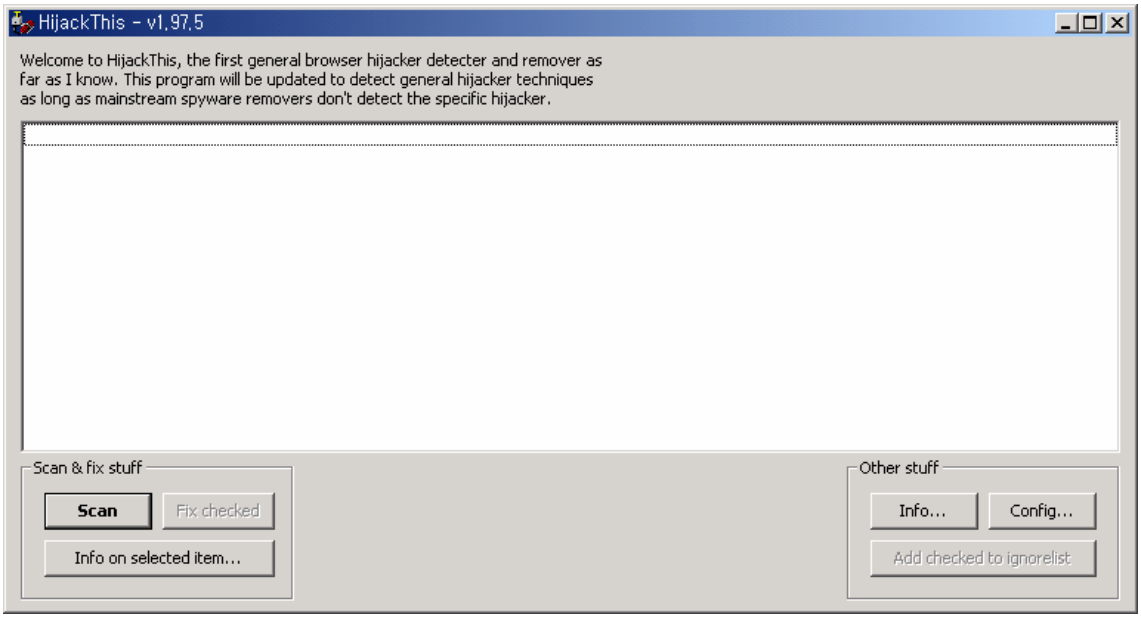
CLSID를 반복해서 찾아 해당 CLSID 값을 사용하는 프로그램이 불필요한 파일이라면
'HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩Browser Helper Objects'에 등록된 CLSID 값을 삭제 하면 된다.

3. 툴 사용법

1) HijackThis

HijackThis는 애드웨어 혹은 사용자 행동을 조사하는 프로그램의 설치 유무를 쉽게 찾을 수 있게 도와주는 프로그램이다. 단, 이 프로그램은 이들 프로그램을 직접 진단하는 기능은 없고 일반적으로 설치되는 위치의 정보를 알려줘 사용자가 판단 할 수 있도록 도와준다. 또한 결과에 나오는 프로그램이 모두 애드웨어 같은 유해가능 프로그램은 아니다.

이 프로그램은 다음 주소에서 다운로드 받을 수 있다.
- http://www.spywareinfo.com/~merijn/files/hijackthis.zip
- http://www.spywareinfo.com/~merijn/index.html



[그림8] HijackThis

[Scan] 버튼을 누르면 애드웨어가 주로 설치되는 위치 정보가 나온다. 비록 애드웨어 진단 기능은 없지만 사용자들에게 애드웨어 같은 유해가능 프로그램 뿐 아니라 웜, 트로이목마 등의 악성 코드가 설치된 위치를 쉽게 찾을 수 있게 도와준다.

4. 주의점

1) 애드웨어 제거 전에 윈도우 업데이트를 한다.

일부 애드웨어는 보안취약점을 이용해 특정 웹사이트에 접속하면 자동으로 애드웨어를 설치한다. 이런 자동 설치는 윈도우 업데이트를 하면 예방할 수 있다. 만약 윈도우 업데이트가 되어 있지 않다면 애드웨어를 삭제하고 인터넷 익스플로러를 실행하면 애드웨어가 지정한 특정 웹 사이트로 시작되어 다시 애드웨어가 설치된다.

2) 홈페이지 변경은 애드웨어 제거 후에 한다.

일부 애드웨어는 특정 시간이나 특정 행동 시 홈페이지 주소를 확인해 자신이 지정하는 웹사이트로 변경한다. 따라서, 애드웨어를 삭제하지 않고 홈페이지를 변경할 경우 애드웨어가 다시 특정 사이트로 변경 할 수 있다. 따라서, 가급적 홈페이지 변경은 애드웨어 제거 후에 한다.

5. 참고자료

- BHO(Browser Helper Objects)

: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebgen/html/bho.asp