ASEC Report 7월

® ASEC Report

2007. 8

안철수연구소의 시큐리티대응센터(AhnLab Security Emergency response Center)는 악성코드 및 보안위협으로부터 고객을 안전하게 지키기 위하여 바이러스 분석 및 보안 전문가들로 구성되어 있는 조직이다.

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

I. ASEC 월간 통계

(1) 7월 악성코드 통계

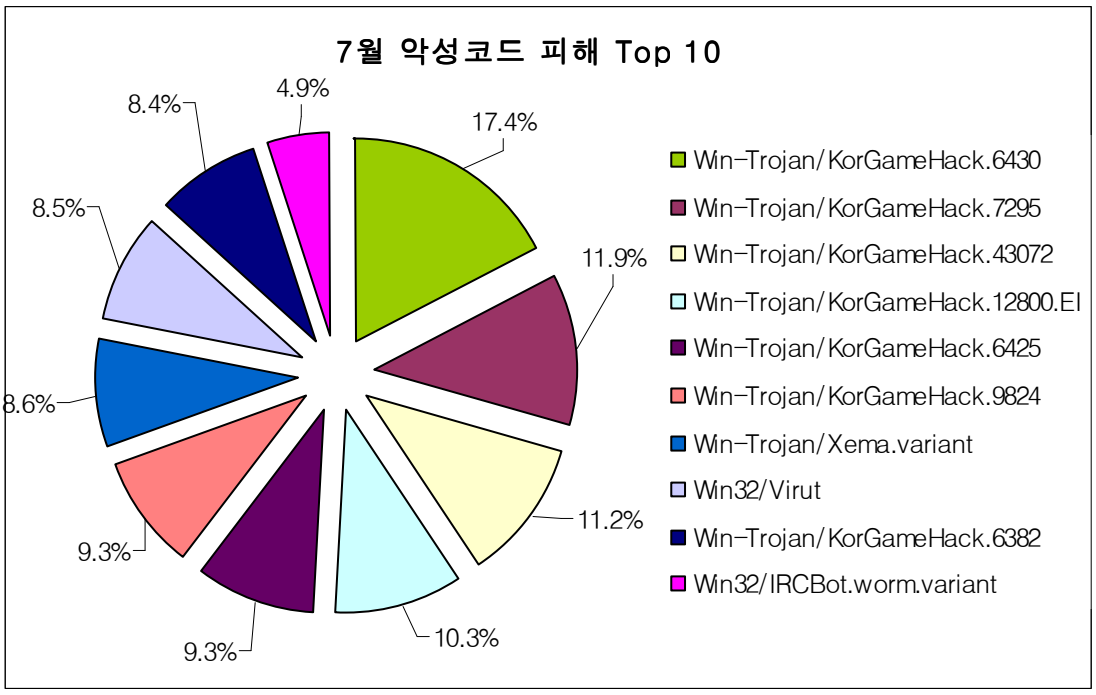
순위		악성코드명	건수	%
1	new	Win-Trojan/KorGameHack.6430	149	17.4%
2	new	Win-Trojan/KorGameHack.7295	102	11.9%
3	new	Win-Trojan/KorGameHack.43072	96	11.2%
4	new	Win-Trojan/KorGameHack.12800.EI	88	10.3%
5	new	Win-Trojan/KorGameHack.6425	80	9.3%
5	new	Win-Trojan/KorGameHack.9824	80	9.3%
6	↓6	Win-Trojan/Xema.variant	74	8.6%
7	↓1	Win32/Virut	73	8.5%
8	new	Win-Trojan/KorGameHack.6382	72	8.4%
9	↓7	Win32/IRCBot.worm.variant	42	4.9%
합계			856	100.0%

[표 1-1] 2007년 7월 악성코드 피해 Top 10

악성코드 피해 동향

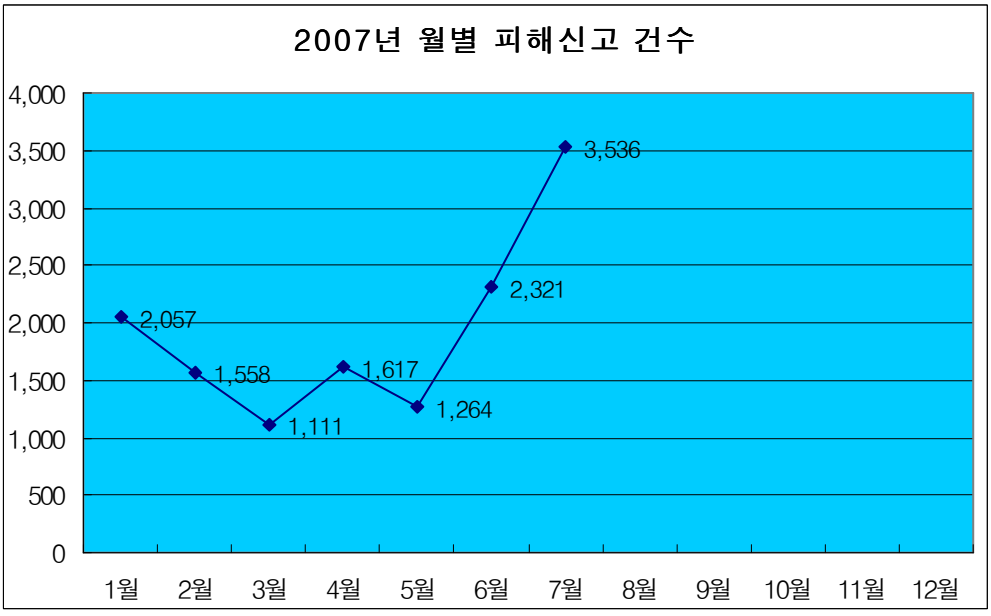
2007년 7월 악성코드 Top10에는 전월 1위였던 Win-Trojan/Xema.variant가 6계단 하락하였으며, 전월 3위였던 Win32/IRCBot.worm.variant은 9위로 순위가 7계단 하락하였다. Win-Trojan/Xema.variant와 바이럿(Win32/Virut), Win32/IRCBot.worm.variant을 제외하고는 모두 새로이 Top10에 진입하였다. 이는 다양한 악성코드들이 새로이 나타나고 있음을 단적을 보여주고 있다. 그 중, 트로이목마류는 8종이 포함되어 고객정보 탈취를 통한 금전적 이득을 목적으로 악성코드 제작이 진행되고 있음을 알 수 있다. 또한, 전월에 Top10에 4종이 포함되었던 아이알씨봇(IRCBOT)은 7월에는 약세를 보이며 9위권에 1개만 링크되었다.

7월의 악성코드 피해 Top 10을 도표로 나타내면 [그림 1-1]과 같다.



[그림 1-1] 2007년 7월 악성코드 피해 Top 10

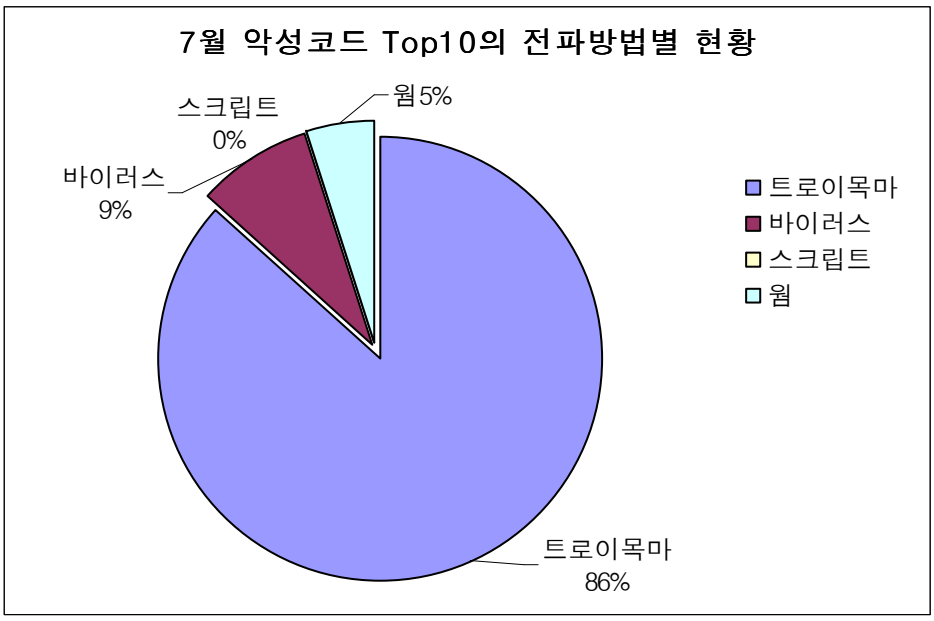
[그림 1-2]에서와 같이 1월부터 월별 피해신고 건수는 꾸준히 감소세를 보이다가 6월에는 전월보다 1,000건 이상 증가하였고, 7월에는 6월보다도 1,200건 이상 증가하였다. 이는 Arp-Spoofing등으로 인하여 GameHack 등의 확산과 같이 새로운 악성코드로 인한 피해 신고 증가의 영향을 받은 것으로 보인다.



[그림 1-2] 2007년 월별 피해신고건수

7월 악성코드 Top 10 전파방법 별 현황

[표 1-1]의 악성코드 피해 Top 10에서 확인된 악성코드의 전파방법은 아래 [그림 1-3]과 같다

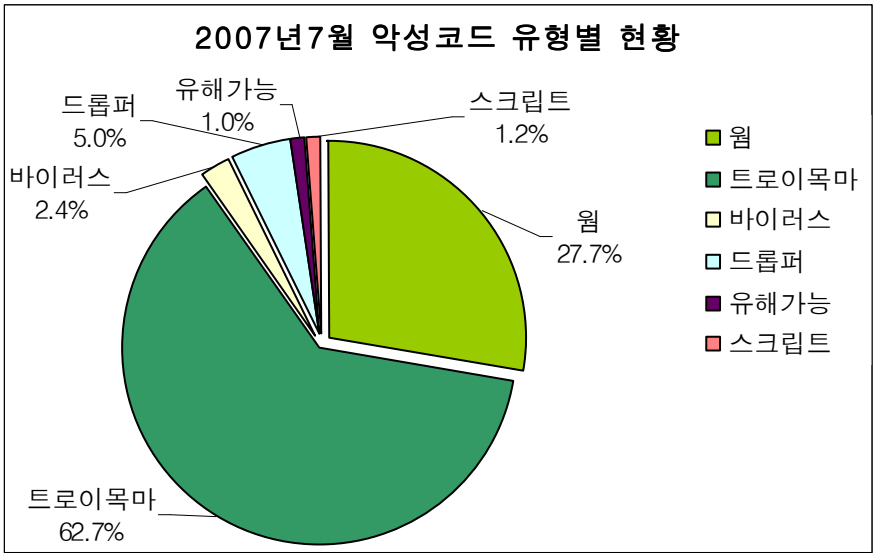


[그림 1-3] 2007년 7월 악성코드 Top 10의 전파방법 별 현황

7월에도 변함없이 트로이목마류가 가장 많은 피해를 발생시켰으며, 점유률은 86%로 전월(76%)에 비해 증가하였으며, 바이러스는 전월(5%)에 비해 소폭 증가하였다. 반면, 웜은(Worm)의 순위 하락으로 전월(17%)에 비해 점유율이 하락하였다. 또한, 스크립트는 Top10 한 건도 포함되지 않았다.

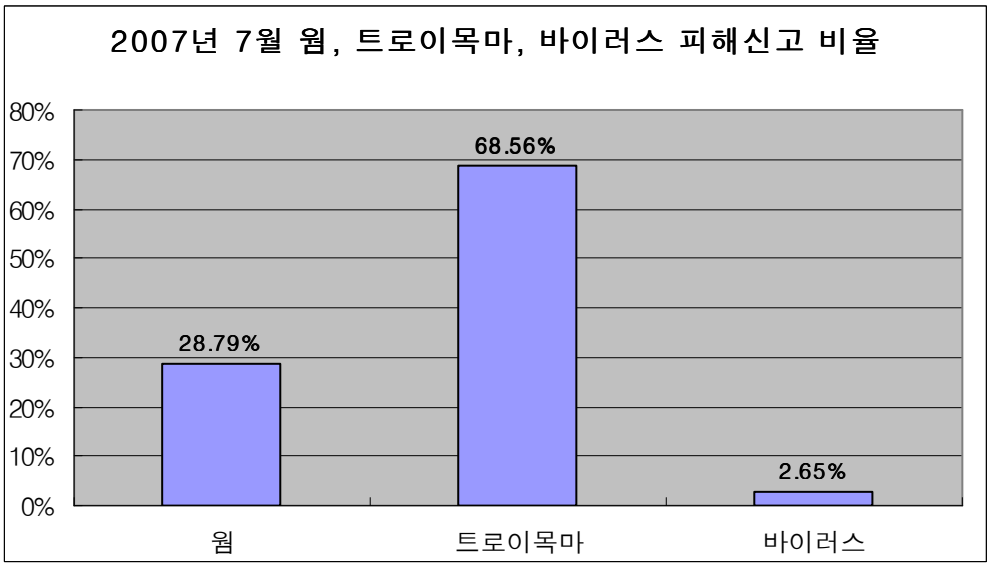
피해신고 된 악성코드 유형 현황

2007년 7월에 피해신고 된 악성코드의 유형별 현황은 [그림 1-4]와 같다.



[그림 1-4] 2007년 7월 피해 신고된 악성코드 유형별 현황

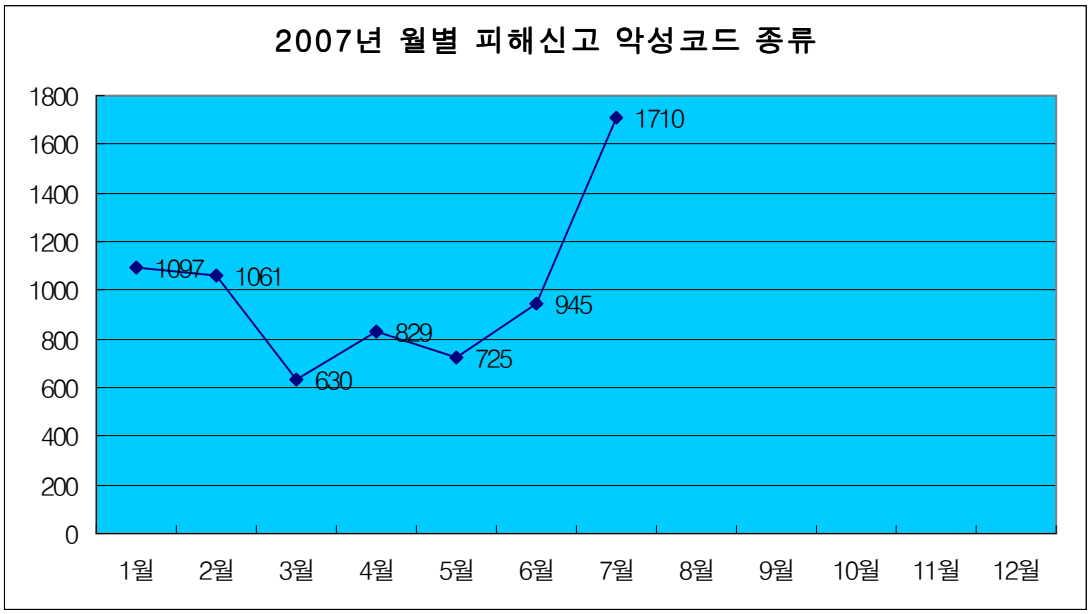
전체 피해 신고에서의 악성코드 유형을 확인해보면, Top10의 악성코드 유형과 동일한 양상을 띠고 있다. 트로이목마가 62.7%로 가장 많았으며, 그 뒤를 웜(27.7%)과 드롭퍼(5.0%)이 차지하였다. Top10으로 봤을 때 웜(4.9%)의 순위는 높지 않으나 전체 건수로 봤을 때 웜 변형이 다수 존재하였음을 알 수 있다. 그 외 바이러스는 2.4%, 뒤를 이어 스크립트가 1.2%, 유해가능프로그램이 1.0%였다. 이중 주요 악성코드 유형인 트로이목마, 바이러스, 웜에 대한 피해신고 비율을 따져보면 [그림 1-5]와 같다.



[그림 1-5] 2007년 7월 웜, 트로이목마 피해신고 비율

월별 피해신고 된 악성코드 종류 현황

악성 종류 현황은 국내에서 발견된 변종 및 신종 악성코드 증감을 나타내며, [그림 1-6]에서와 같이 2007년에는 2월에 급격한 감소세를 보인 이후에 다시 증가 추세를 보이고 있으며, 7월에는 전월 대비 약 2배 가까이 많은 수의 다양한 악성코드가 발견되었다.



[그림 1-6] 2007년 월별 피해신고 악성코드 종류 개수

국내 신종(변형) 악성코드 발견 피해 통계

7월 한달 동안 접수된 신종 (변형) 악성코드의 건수 및 유형은 [표 1-2]와 같다.

	웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
5 월	53	331	59	0	4	0	0	0	34	0	481
6 월	86	431	53	1	1	0	0	0	17	0	589
7 월	28	300	71	4	3	0	0	0	16	0	422

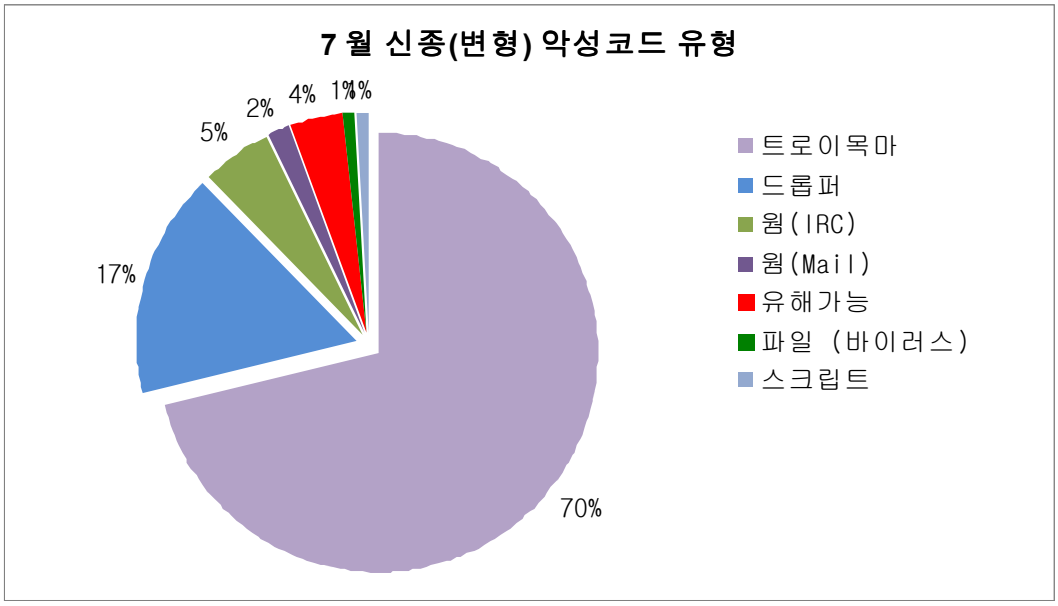
[표 1-2] 2007년 최근 3개월간 유형별 신종 (변형) 악성코드 발견현황

이번 달은 휴가철인 7월이어서 인지 발견된 신종(변형)악성코드 수가 전월 대비 28% 정도 감소하였다. 악성코드의 수가 계절적인 요인을 타는 경우는 중국산 악성코드 급증으로 인하여 중국 최대 명절인 춘절이 있는 2월 정도이지만 최근 2년간 (2005, 2006)의 7, 8월 악성코드의 수를 보면 그 해 평균보다 약 7% ~ 30% 정도 감소하였으며, 올해에도 같은 현상이 반복되었다. 감소 원인에 대해서는 명확하지는 않지만 중국산 악성코드로 인한 유입이 많은 우리나라의 경우에 한하여 발생하는 현상으로 추정된다.

이번 달 감소한 악성코드 유형은 다음과 같다.

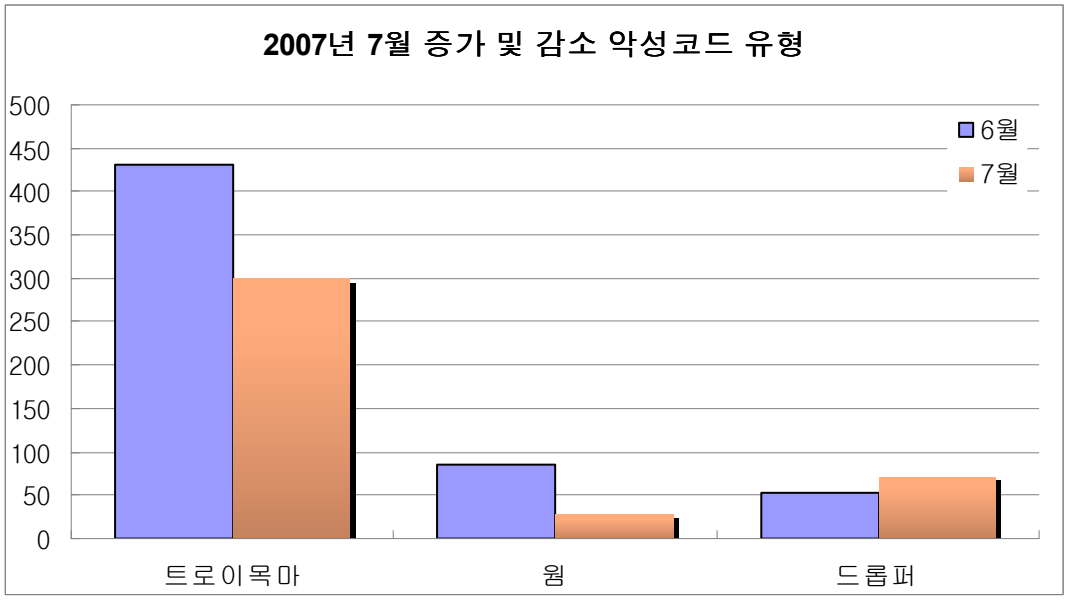
- 온라인 게임의 사용자 정보 탈취 트로이목마 – 전월 대비 36% 감소
- Win32/IRCBot.worm – 전월 대비 46% 감소
- 이메일 웜 감소 – 전월 대비 Stration 및 Allaple 변형 발견 되지 않음
- Win-Trojan/Zlob – 전월 대비 현저히 발견 건수 적음

특히 이번 달에는 Win32/Zhelatin.worm의 변형이 자주 보고되었는데, 모두 동일한 것으로 단지 해당 악성코드가 사용하는 다형성 코드가 달라서 엔진에 추가되었을 뿐이며, 이러한 샘플은 통계와 본 보고서의 데이터 자료에서는 제외되었다.



[그림 1-7] 2007년 7월 신종 및 변형 악성코드 유형

7월에는 트로이목마와 웜 유형은 큰폭으로 감소하였으나, 드롭퍼는 전월대비 25% 증가하였다. 증가한 드롭퍼는 대부분 온라인 게임의 사용자 데이터를 훔쳐내는 악성코드로서, 보통 이러한 악성코드는 드롭퍼(.exe)에서 트로이목마(.dll)를 생성하는데 트로이목마들은 대부분 기진단되는 경우가 많았고, 드롭퍼만 실행압축 프로그램을 변경하거나 코드를 약간 달리하여 진단 되지않도록 하는 경우가 종종 있었다. 따라서 온라인 게임의 사용자 데이터를 훔쳐내는 드롭퍼가 증가하였다고 하더라도 따라서 트로이목마가 함께 증가 되지는 않는다.



[그림 1-8] 2007년 7월 감소 및 증가 악성코드 유형

이번 달에는 전월에 1종 밖에 발견 되지 않은 바이러스가 3종 발견 되었다.

- Win32/Grum
- Win32/Klest.B
- Win32/Rungbu

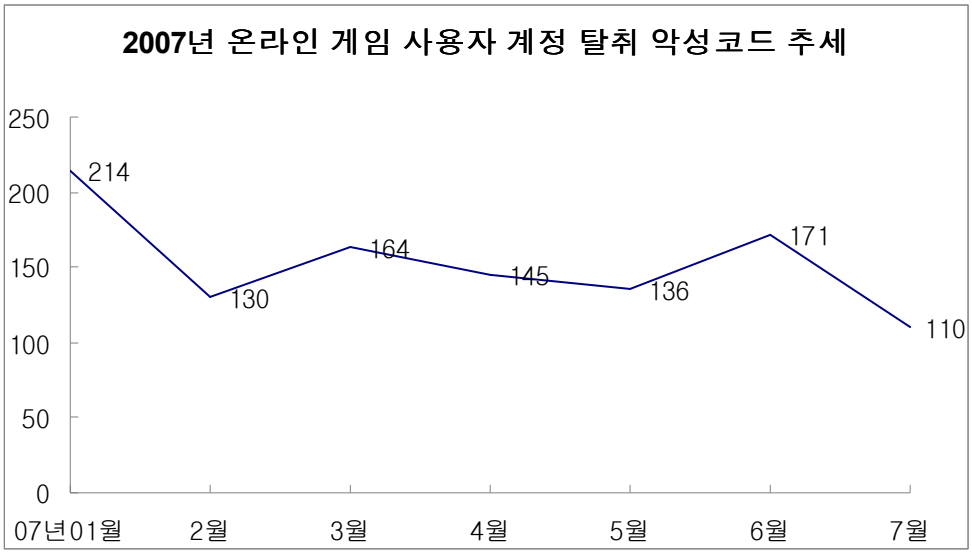
Win32/Grum 바이러스는 메일로 전파 되는 Win32/Grum.worm으로부터 감염될 수 있으며, 시스템에 있는 모든 *.exe 파일을 감염 시키지는 않고 다음 레지스트리에 등록된 실행파일만을 감염시키는 특징을 가지고 있다.

HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Run

Win32/Klest.B 바이러스는 글을 작성하는 현재 .C 형까지 변형이 발견된 후위형 바이러스로서 원본 파일에 섹션 하나를 추가하며 특정 호스트로부터 파일을 다운로드하는 작은 쉘코드 하나를 포함하고 있다.

Win32/Rungbu 바이러스는 MS 워드 문서인 *.DOC 문서를 감염키는 특징을 가지며, 정상적인 *.DOC 문서 앞 부분에 자신을 위치시킨다. 감염된 워드 문서는 확장자가 EXE로 변경 되며 해당 문서를 실행하면 원래 *.DOC 가 분리 되어서 문서가 오픈 된다.

다음은 트로이목마 및 드롭퍼의 전체 비중에서 상당한 비율을 차지 하는 온라인 게임의 사용자 계정을 탈취하는 트로이목마의 추세를 살펴보았다.



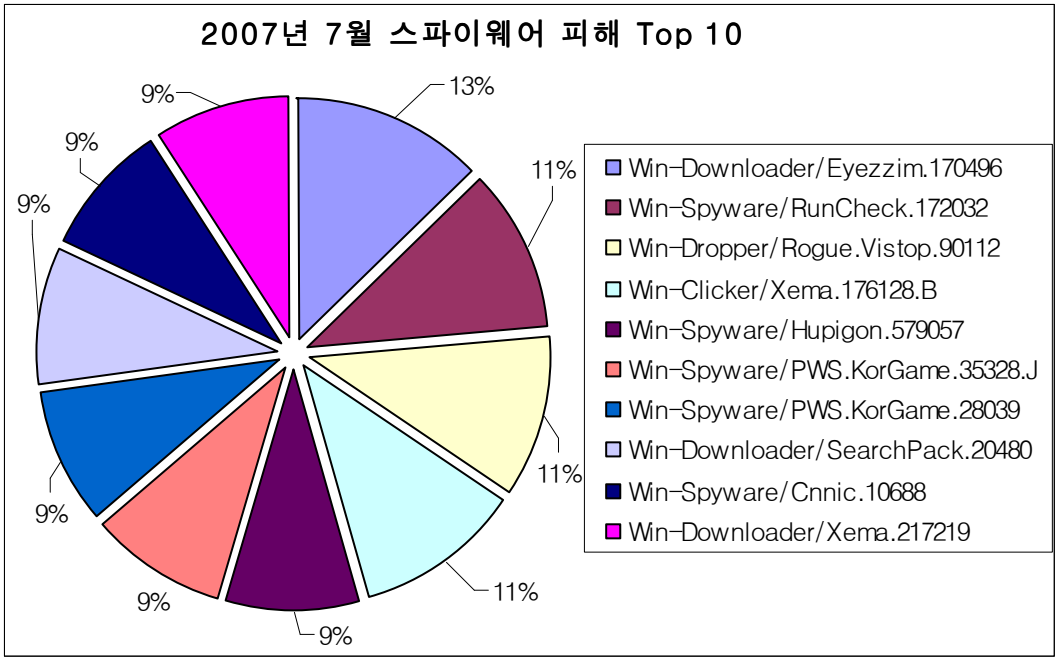
[그림 1-9] 온라인 게임 사용자 계정 탈취 트로이목마 현황[1]

이번 달은 온라인 게임의 사용자 데이터를 훔쳐내는 트로이목마가 전월 대비 36% 감소하였는데, 이는 기진단되는 트로이목마가 많았기 때문으로 추정된다. 일반적으로 이러한 악성코드는 자동화된 도구에 의해서 제작되어 실제 메인 기능을 수행하는 트로이목마 (*.DLL)의 핵심코드들은 대부분 유사하기 때문에 이러한 특징을 분석하여 엔진에 반영함으로써 기진단될 수 있다.

(2) 7월 스파이웨어 통계

순위		스파이웨어 명	건수	비율
1	New	Win-Downloader/Eyezzim.170496	7	1%
2	New	Win-Spyware/RunCheck.172032	6	1%
3	New	Win-Dropper/Rogue.Vistop.90112	6	1%
4	New	Win-Clicker/Xema.176128.B	6	1%
5	New	Win-Spyware/Hupigon.579057	5	1%
6	New	Win-Spyware/PWS.KorGame.35328.J	5	1%
7	New	Win-Spyware/PWS.KorGame.28039	5	1%
8	New	Win-Downloader/SearchPack.20480	5	1%
9	New	Win-Spyware/Cnnic.10688	5	1%
10	New	Win-Downloader/Xema.217219	5	1%
		기타	710	90.0%
합계			765	100%

[표 1-3] 2007년 7월 스파이웨어 피해 Top 10



[그림 1-10] 2007년 7월 스파이웨어 피해 Top 10

2007년 7월 스파이웨어 피해 통계를 살펴보면 6월과 마찬가지로 국내에서 제작 배포되는 스파이웨어의 피해가 지속되는 것을 알 수 있다. 스파이웨어 피해 Top 10의 절반 정도를 국내제작 스파이웨어가 차지하고 있으며, 나머지 절반은 중국에서 제작된 스파이웨어로 보인다.

가장 많은 피해 신고가 접수된 다운로더 아이찜(Win-Downloader/Eyezzim.170496)은 국내에서 제작 배포 되었으며, 7월 한 달에만 4종의 변형이 발견되었다. 다운로더 아이찜은 NT 서비스(Windows NT Service)로 실행되는데, 일반적으로 NT 서비스로 실행되는 스파이웨어는 자동실행 레지스트리에 등록된 스파이웨어보다 발견하기가 어렵다.

여전히 중국에서 제작되는 스파이웨어는 국내외 주요 온라인 게임 계정 유출을 목적으로 하고 있으며 이들에 의한 피해 신고 또한 꾸준히 접수되고 있다.

2007년 7월 유형별 스파이웨어 피해 현황은 [표 1-4]와 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
5월	320	109	22	122	2	10	2	9	0	596
6월	279	166	46	139	8	16	0	1	0	655
7월	261	183	55	232	10	20	3	1	0	765

[표 1-4] 2007년 7월 유형별 스파이웨어 피해 건수

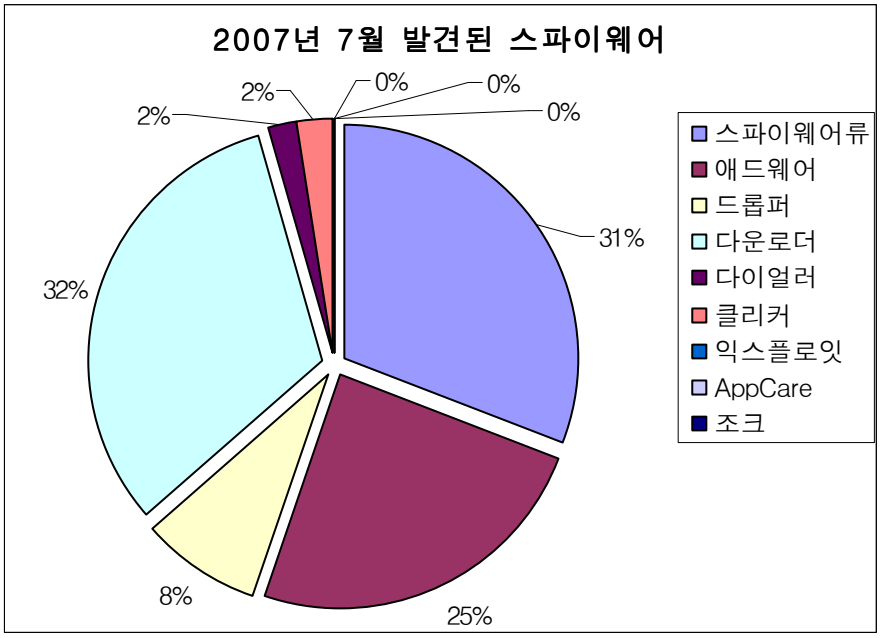
2007년 7월 스파이웨어 피해 신고 건수는 6월보다 약 100여 건 증가한 765건이 기록되었다. 7월 스파이웨어 피해 신고 접수 통계를 살펴보면 다운로더에 의한 피해 신고가 6월 139건에서 232건으로 크게 늘어난 것을 볼 수 있다. 다운로더의 피해 신고 증가는 아래 스파이웨어 동향에 언급된 '배포방식의 변화'와 연관이 있다. 설치 배당금을 목적으로 애드웨어 제작사는 번들 설치를 위한 다운로더를 이용하고 있으며, 이들 다운로더가 사용자 또는 안티-바이러스, 안티-스파이웨어 프로그램과 같은 보안 프로그램이 인지하지 못하도록 다양한 변형을 양산하고 있다. 또한 이들 다운로더의 코드 또한 정체를 숨기고 사용자를 속이기 위하여 점차 악성으로 변화하고 있다.

7월 스파이웨어 발견 현황

7월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 1-5], [그림 1-11]과 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
5월	143	29	5	46	1	4	1	3	0	232
6월	108	46	19	38	2	3	0	0	0	216
7월	63	50	17	65	4	5	0	0	0	204

[표 1-5] 2007년 7월 유형별 신종(변형) 스파이웨어 발견 현황

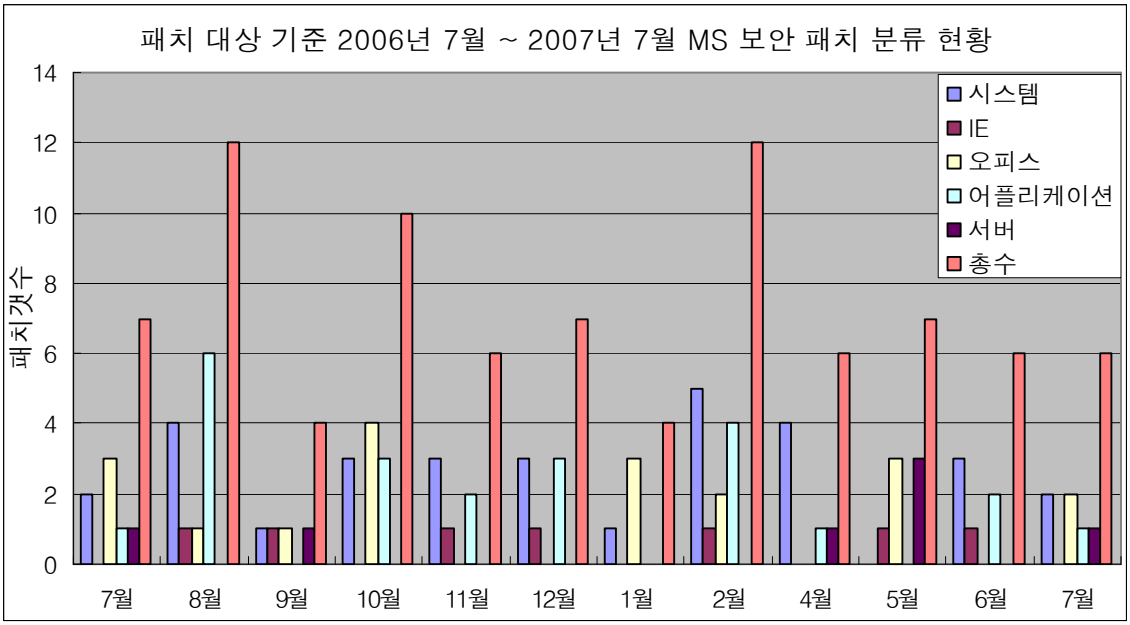


[그림 1-11] 2007년 7월 발견된 스파이웨어 프로그램 비율

5월과 6월에 이어 7월에도 신종 및 변형 스파이웨어 발견 건수는 감소세를 보이고 있다. 특히 스파이웨어류의 신종 및 변형 발견 건수는 거의 절반으로 감소하였으나, 신종 및 변형 다운로더는 거의 두 배 가까이 증가하였다. 위의 스파이웨어 피해 현황에서 언급한 국내 애드웨어 제작사의 다운로더 양산이 주요 원인으로 추정된다.

(3) 7월 시큐리티 통계

2007년 7월에는 마이크로소프트사에서 총 6개의 보안 업데이트를 발표하였으며, 긴급(Critical) 3개, 중요 2개, 보통 1개로 구성되어 있다. 이 중에서 서버군 제품(Windows 2000/2003 Server)의 공격에 사용될 수 있는 MS07-039, MS07-040에 대한 패치가 포함되었으며, 특이사항으로는 닷넷 프레임워크(.NET Framework)가 설치된 클라이언트 시스템을 공격할 수 있거나, ASP .NET 이 실행중인 웹 서버를 공격할 수 있는 MS07-040 에 대한 패치가 포함되어 있다.

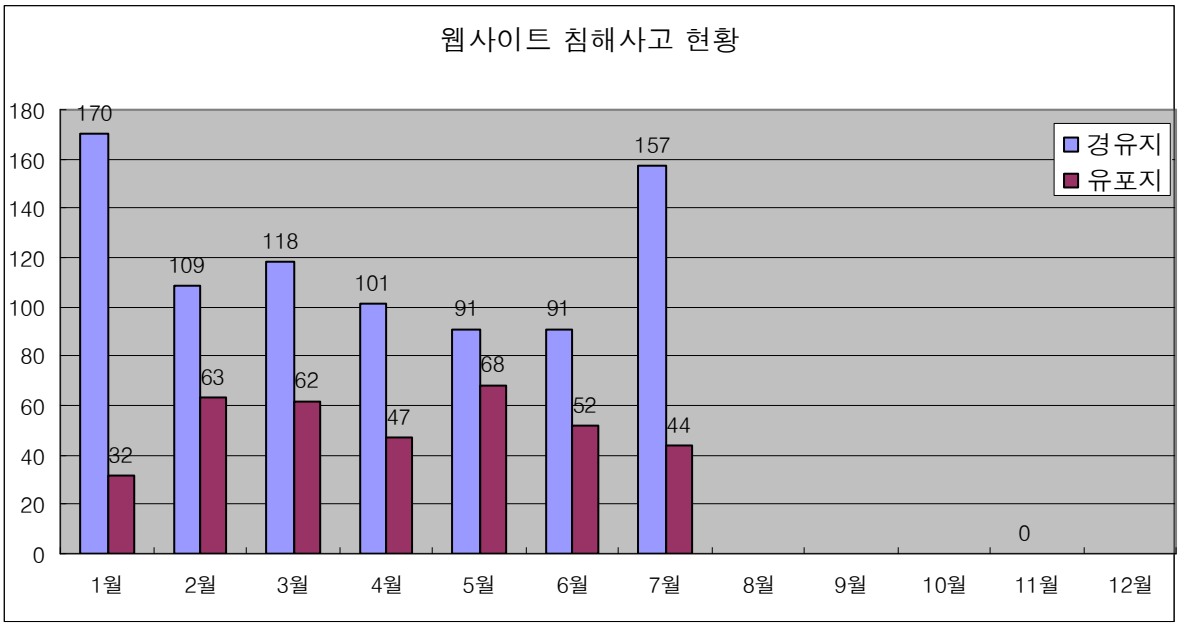


[그림 1-12] 최근 1년간 공격대상 기준 MS 보안 패치 현황

[그림 1-12]를 보면, 전반적으로 2007년에 들어와서, 오피스 및 IE 취약점이 증가 추세에 있는 것을 알 수 있다. 7월 달에도 엑셀 취약점(MS07-036)과 Microsoft Office Publisher의 취약점으로 인한 원격 코드 실행 문제점(MS07-037)에 대한 패치가 발표되었다. 엑셀 취약점(MS07-036)은 악성코드에서도 사용이 가능함으로, 반드시 오피스 홈페이지에서 보안 업데이트를 적용해야만, 클라이언트 시스템의 보안성을 강화할 수 있다.

윈도우 비스타(Windows Vista)에 포함된 윈도우 방화벽(Windows Firewall) 에는 기본적으로 여러 프로토콜 및 어플리케이션에 대한 보안 정책이 적용되어 있다. 그러나 Teredo 인터페이스에 대한 정책이 제대로 적용되어 있지 않아서, Teredo 관련 서비스에 대해 방화벽을 우회할 수 있게 된다. MS07-038 은 이러한 문제점을 해결할 수 있다.

2007년 7월 웹 침해사고 현황



[그림 1] 악성코드 배포를 위해 침해된 사이트 수/ 배포지 수

2007년 7월의 웹 사이트 경유지/유포지 개수는 167/44로 2007년 6월과 비교하여 경유지 개수가 크게 증가하였다. 새롭게 발표된 인터넷 익스플로러 관련 취약점의 공격 코드가 공개된 것이 없음에도 불구하고 침해된 사이트 수가 크게 증가한 이유는 취약점이 존재하는 국내 웹사이트가 중국 해커들의 공략 대상이 되어 중국발 해킹이 크게 증가한 것으로 추정된다. 국내 웹사이트의 근본적인 보안 정책의 점검 없이는 앞으로도 중국발 해킹은 계속 증가할 것으로 예상된다.

취약점별 현황을 살펴보면 여전히 MS07-017 취약점을 이용한 공격코드가 44%로 절반 가량을 차지하고 있다. 2007년 6월 통계에서 분석한 것처럼 새로운 취약점이 발표되지 않는 이상 2007년 8월의 경우도 크게 다르지 않을 것으로 보인다. 현재 조작된 ANI 파일은 대부분의 AV 제품에서 대응 가능하므로 일반 사용자는 AV제품의 업데이트와 주기적인 보안패치로 만약에 있을 보안 위협에 대비하여야 한다.

II. ASEC Monthly Trend & Issue

(1) 악성코드 – 비밀 채널로 통신하는 악성코드들

이번 달은 Covert Channels(비밀 채널)을 은밀하게 오픈하여 외부로 통신하는 악성코드인 Win-Trojan/Agent.20992.CK에 대해서 살펴 본다. 그리고 ransom ware 라고 불리우는 Gpcode 변형이 다시 발견 되었다는 소식을 전하며 해당 악성코드의 증상에 대해서 본다. 이번 달에 또 다시 다수의 변종이 발견된 Win32/Zhelatin.worm 변형의 메일 유형에 대해서 알아보며 끝으로 또 다시 발견된 MSN 메신저 소식을 전한다.

비밀채널로 통신하는 Win-Trojan/Agent.20992.CK

Funny.zip 이란 첨부 파일을 가진 메일이 국외에서 대량 유포 되었다. 메일은 다음과 같은 제목들을 일부 가지고 있는 것으로 확인 되었다.

- Action for pleasure
- Double energy
- life is beautiful!
- Life is good!
- Paradice in your bed
- Paradice in your bed
- Return sunrise to your life!
- View this price
- You can be young again

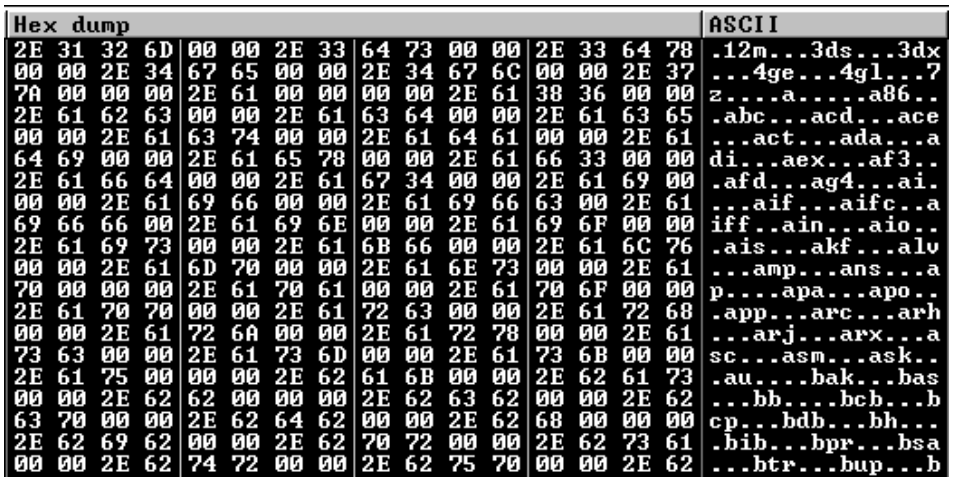
첨부된 파일을 실행하면 runtime.sys 가 생성되고 메모리에 로드 된다. 이후 인터넷 익스플로러를 유저모드에서 은폐시킨 후 실행하고 특정 호스트로 접속하게 해둔다. 이와 같은 증상은 다른 변형을 다운로드 하거나 스팸 메일을 발송하는 스팸 봇을 다운로드 해오기도 한다. 특히 해당 악성코드는 네트워크 관련 IRP(I/O Request Packets)를 후킹하여 외부와 통신을 은폐한다. IPR는 디바이스 드라이버가 파일을 읽고, 쓰거나 또는 네트워크를 패킷을 쓸 때 사용되며, 아래 [그림 2-1]과 같이 원래 드라이버의 콜을 가로채서 runtime.sys가 먼저 동작 하도록 한다.

[그림 2-1] Win-Trojan/Agent.20992.CK 가 후킹하는 IRP

돌아온 Ransom ware - GpCode

Ransom ware는 몸값을 뜻하는 Ransom 과 Software의 ware 가 결합된 신조어로써 사용자가 주로 접근하는 데이터를 암호화한 후 암호를 풀기를 원하면 일정금액의 돈을 지불해야만 암호화된 데이터를 복호화 할 수 있는 도구를 제공하는 류의 악성코드를 일컫는 용어로 사용 되고 있다. GpCode 라고 명명된 악성코드는 작년에 첫 발견, 보고 되었고 이후 변형이 몇 개 더 보고 되었다. 이후 올 7월에 발견된 변형은 올해 첫 발견된 변형이라 할 수 있다.

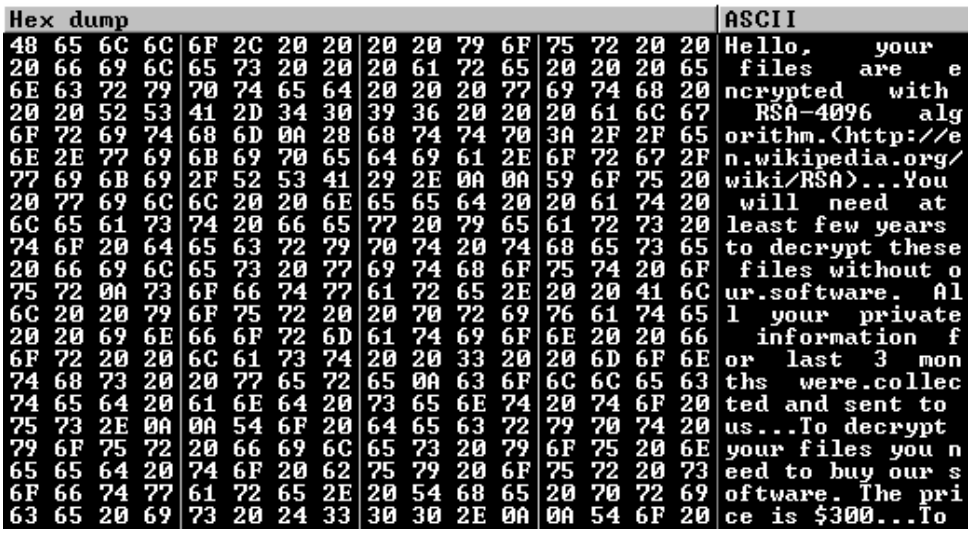
이번에 발견된 변형은 다음과 같은 확장자들을 가지는 파일을 암호화한다.



Hex dump												ASCII
2E 31 32 6D	00 00 2E 33	64 73 00 00	2E 33 64 78	.12m...3ds...3dx
00 00 2E 34	67 65 00 00	2E 34 67 6C	00 00 2E 37	...4ge...4gl...7
7A 00 00 00	2E 61 00 00	00 00 2E 61	38 36 00 00	z....a.....a86..
2E 61 62 63	00 00 2E 61	63 64 00 00	2E 61 63 65	.abc...acd...ace
00 00 2E 61	63 74 00 00	2E 61 64 61	00 00 2E 61	...act...ada...a
64 69 00 00	2E 61 65 78	00 00 2E 61	66 33 00 00	di...aex...af3..
2E 61 66 64	00 00 2E 61	67 34 00 00	2E 61 69 00	.afd...ag4...ai.
00 00 2E 61	69 66 00 00	2E 61 69 66	63 00 2E 61	...aif...aifc..a
69 66 66 00	2E 61 69 6E	00 00 2E 61	69 6F 00 00	iff..ain...aio..
2E 61 69 73	00 00 2E 61	6B 66 00 00	2E 61 6C 76	.ais...akf...alv
00 00 2E 61	6D 70 00 00	2E 61 6E 73	00 00 2E 61	...amp...ans...a
70 00 00 00	2E 61 70 61	00 00 2E 61	70 6F 00 00	p....apa...apo..
2E 61 70 70	00 00 2E 61	72 63 00 00	2E 61 72 68	.app...arc...arh
00 00 2E 61	72 6A 00 00	2E 61 72 78	00 00 2E 61	...arj...arx...a
73 63 00 00	2E 61 73 6D	00 00 2E 61	73 6B 00 00	sc...asm...ask..
2E 61 75 00	00 00 2E 62	61 6B 00 00	2E 62 61 73	.au....bak...bas
00 00 2E 62	62 00 00 00	2E 62 63 62	00 00 2E 62	...bb....bcb...b
63 70 00 00	2E 62 64 62	00 00 2E 62	68 00 00 00	cp...bdb...bh...
2E 62 69 62	00 00 2E 62	70 72 00 00	2E 62 73 61	.bib...bpr...bsa
00 00 2E 62	74 72 00 00	2E 62 75 70	00 00 2E 62	...btr...bup...b

[그림 2-2] GpCode 가 암호화 하는 파일의 확장자 일부분

암호화가 끝나면 해당 파일이 존재하는 폴더에 다음과 같은 내용의 read_me.txt 파일을 생성한다. 암호화된 것을 복호화 하기 위해서 $300을 보내야 한다고 적혀있다.



Hex dump												ASCII
48 65 6C 6C	6F 2C 20 20	20 20 79 6F	75 72 20 20	Hello, your
20 66 69 6C	65 73 20 20	20 61 72 65	20 20 20 65	files are e
6E 63 72 79	70 74 65 64	20 20 20 77	69 74 68 20	ncrypted with
20 20 52 53	41 2D 34 30	39 36 20 20	20 61 6C 67	RSA-4096 alg
6F 72 69 74	68 6D 0A 28	68 74 74 70	3A 2F 2F 65	orithm.(http://e
6E 2E 77 69	6B 69 70 65	64 69 61 2E	6F 72 67 2F	n.wikipedia.org/
77 69 6B 69	2F 52 53 41	29 2E 0A 0A	59 6F 75 20	wiki/RSA)...You
20 77 69 6C	6C 20 20 6E	65 65 64 20	20 61 74 20	will need at
6C 65 61 73	74 20 66 65	77 20 79 65	61 72 73 20	least few years
74 6F 20 64	65 63 72 79	70 74 20 74	68 65 73 65	to decrypt these
20 66 69 6C	65 73 20 77	69 74 68 6F	75 74 20 6F	files without o
75 72 0A 73	6F 66 74 77	61 72 65 2E	20 20 41 6C	ur.software. Al
6C 20 20 79	6F 75 72 20	20 70 72 69	76 61 74 65	l your private
20 20 69 6E	66 6F 72 6D	61 74 69 6F	6E 20 20 66	information f
6F 72 20 20	6C 61 73 74	20 20 33 20	20 6D 6F 6E	or last 3 mon
74 68 73 20	20 77 65 72	65 0A 63 6F	6C 6C 65 63	ths were.collec
74 65 64 20	61 6E 64 20	73 65 6E 74	20 74 6F 20	ted and sent to
75 73 2E 0A	0A 54 6F 20	64 65 63 72	79 70 74 20	us...To decrypt
79 6F 75 72	20 66 69 6C	65 73 20 79	6F 75 20 6E	your files you n
65 65 64 20	74 6F 20 62	75 79 20 6F	75 72 20 73	eed to buy our s
6F 66 74 77	61 72 65 2E	20 54 68 65	20 70 72 69	oftware. The pri
63 65 20 69	73 20 24 33	30 30 2E 0A	0A 54 6F 20	ce is $300...To

[그림 2-3] Gpcode 가 남겨놓은 메시지 일부분

작년 GPCode 가 기승을 부리고 난 이후 이와 비슷한 형태로 데이터를 암호화 하거나 시스템을 사용할 수 없도록 리소스를 점유하거나 키보드 및 마우스 동작을 방해하면서 금전을 요구하는 등 다양한 방법으로 사용자의 데이터 및 시스템을 못쓰게 하는 Ransom ware 가 유행했었다. 비록 적은 수였고 한 동안 발견 되지 않았던 이러한 Ransom ware 의 재등장은 설령 일부 국가에서 국지적으로 발생하는 현상이라 해도 안심할 수만은 없다.

또 다시 등장한 MSN 메신저 웜

Win32/Agent.worm.121344 는 MSN 메신저로 자신을 전파 시키는 웜이다. 올해 들어 MSN 메신저 웜으로 전파 되는 악성코드가 자주 보고 되고 있다. 이들의 특징은 메신저가 실행가능한 확장자를 첨부 및 전송 할 수 없도록 하자 ZIP 으로 압축한 형태로 상대방에게 전송하고 있다. 그리고 감염된 시스템에 따라 다양한 언어로 작성된 메시지를 보내어 사용자로 하여금 첨부된 파일을 다운로드 하여 실행 하도록 유도 하고 있다.

```
Text string
ASCII "Look how wasted Paris Hilton is, after she got jailed :("
ASCII "You and Me !!! .... look :p"
ASCII "Look at my photos hihi :p"
ASCII "Hey please accept my photos :o !!"
ASCII "A photo with me and my best friend :$ !!"
ASCII "This is me totaly naked :o please dont send to anyone else"
ASCII "Look what i found on the NET :o Jessica Alba NUDE !!"
ASCII "images0"
ASCII "photos0"
ASCII "album"
ASCII "photo"
ASCII "pictures0"
ASCII "picture"
ASCII "bak sana  Paris Hilton ne hale gelmis hapiste :("
ASCII "Sen ve Ben !!! .... BAK :p"
ASCII "Baksana benim fotograflara hihi :p"
ASCII "Hey benim fotolarimi kabul et :o !!"
ASCII "Iyi arkadasimla fotorafdayim :$ !!"
ASCII "benim bu ciplak fotoda :o ama baskasina yollama"
ASCII "bak ne buldum :o Jessica alba ciplak !!"
ASCII "Regarde comment Paris Hilton parait efondr?apr? qu'elle ai ??jeter en prison :("
```

[그림 2-4] 메신저로 전송되는 메시지 일부분

또한 이 악성코드는 악성 IRCBot 기능을 하도록 DLL 파일을 생성하여 특정 IRC 서버로 접속한다.

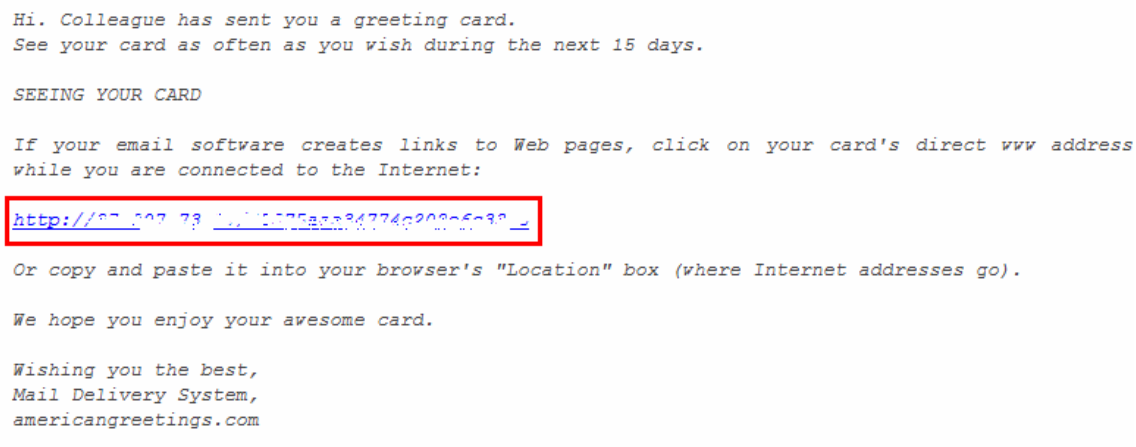
Win32/Zhelatin.worm 메일 유형

이번 달에 국내에도 다수 보고된 Win32/Zhelatin.worm 은 다음과 같은 메일 제목을 가지고 전파 되었다.

- You've received a greeting card from a Class-mate!
- You've received a greeting card from a Colleague!
- You've received a greeting card from a Neighbour!
- You've received a postcard from a Mate!
- You've received a postcard from a School friend!

- You've received a postcard from a School mate!
- You've received an ecard from a Class mate!
- You've received an ecard from a Friend!
- You've received an ecard from a School mate!
- You've received an card from a School mate!

다음의 메일 본문중 하나이다. 아래 붉은색 박스에는 특정 호스트로터 파일을 다운로드 유도하는 링크가 걸려있다.



Hi. Colleague has sent you a greeting card.
See your card as often as you wish during the next 15 days.

SEEING YOUR CARD

If your email software creates links to Web pages, click on your card's direct www address while you are connected to the Internet:

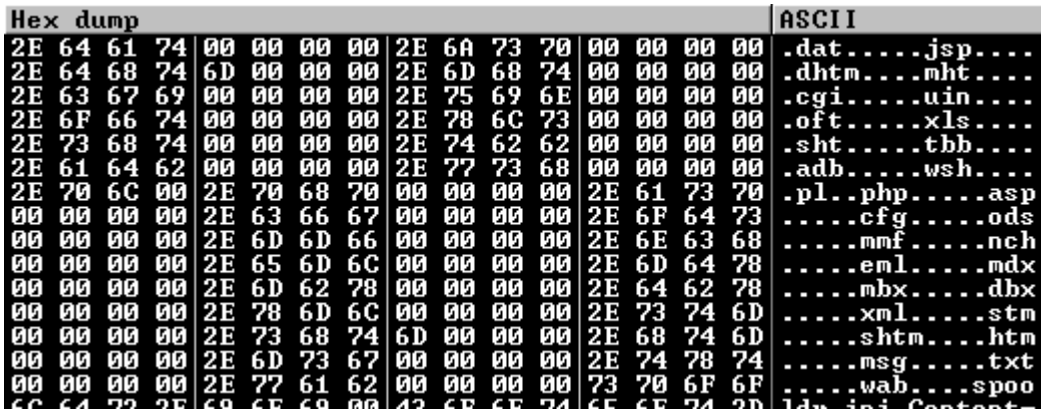
Or copy and paste it into your browser's "Location" box (where Internet addresses go).

We hope you enjoy your awesome card.

Wishing you the best,
Mail Delivery System,
americangreetings.com

[그림 2-5] Zhelatin 웜을 다운로드 유도하는 메일본문

해당 링크의 파일은 ecard.exe로 동일하며 실행하면 안티 바이러스를 비롯한 일부 보안 제품을 무력화시키고 은폐증상을 갖는 커널 드라이버 형태의 트로이목마를 생성하고 실행한다. 그리고 실행된 자신은 로컬에서 다음과 같은 확장자에 대해서 메일 주소를 수집한다. 또한 P2P 네트워크로 추정되는 특정 다수의 호스트로 접속을 시도한다.



Hex dump												ASCII
2E	64	61	74	00	00	00	00	2E	6A	73	70	.dat.....jsp....
2E	64	68	74	6D	00	00	00	2E	6D	68	74	.dhtm....mht....
2E	63	67	69	00	00	00	00	2E	75	69	6E	.cgi.....uin....
2E	6F	66	74	00	00	00	00	2E	78	6C	73	.oft.....xls....
2E	73	68	74	00	00	00	00	2E	74	62	62	.sht.....tbb....
2E	61	64	62	00	00	00	00	2E	77	73	68	.adb.....wsh....
2E	70	6C	00	2E	70	68	70	00	00	00	00	2E	61	73	70	.pl..php.....asp
00	00	00	00	2E	63	66	67	00	00	00	00	2E	6F	64	73	.....cfg.....ods
00	00	00	00	2E	6D	6D	66	00	00	00	00	2E	6E	63	68	.....mmf.....nch
00	00	00	00	2E	65	6D	6C	00	00	00	00	2E	6D	64	78	.....eml.....mdx
00	00	00	00	2E	6D	62	78	00	00	00	00	2E	64	62	78	.....mbx.....dbx
00	00	00	00	2E	78	6D	6C	00	00	00	00	2E	73	74	6D	.....xml.....stm
00	00	00	00	2E	73	68	74	6D	00	00	00	2E	68	74	6D	.....shtm....htm
00	00	00	00	2E	6D	73	67	00	00	00	00	2E	74	78	74	.....msg.....txt
00	00	00	00	2E	77	61	62	00	00	00	00	73	70	6F	6F	.....wab....spoo

[그림 2-6] Zhelatin 웜이 수집하는 메일 확장자

Zhelatin 웜의 변형은 다양한데 이와 같이 메일 확장자를 수집하여 특정 호스트로 전송하는 증상, 특정 P2P 접속 증상 그리고 감염 시스템의 정보 (국가정보 및 컴퓨터 사양 등)만을

탈취하는 증상을 갖는 변형 등 동일한 진단명으로 진단되어도 여러가지 다른 증상을 갖는 다양한 변형의 Zhelatin 웜 변형이 존재한다.

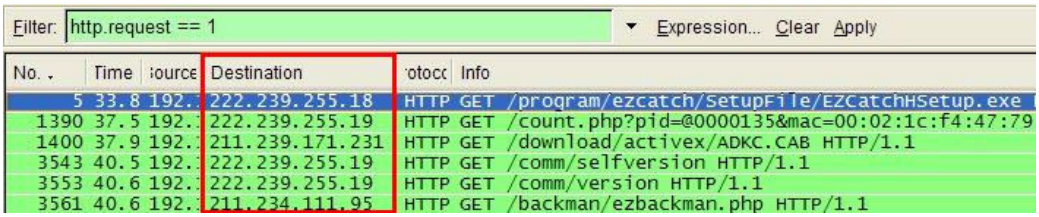
(2) 스파이웨어 - 다운로더와 번들을 이용한 배포

스파이웨어의 주된 유포 형태는 ActiveX 컨트롤 형태로 사용자의 적절한 동의없이 설치 유도하는 것이었다. 그러나 최근에는 ActiveX 컨트롤 형태로 사용자의 적절한 동의없이 설치될 경우 안티스파이웨어 제품에 의하여 진단 추가되어 스파이웨어 제작자가 원하는 수준으로 스파이웨어 유포가 진행되는 경우가 제한적이다. 이에 따라서 ActiveX 컨트롤 형태로 설치되는 스파이웨어가 감소되고 다운로더(Win-Downloader)나 특정 프로그램의 번들로 설치되는 형태가 증가하는 것으로 파악되고 있어, 스파이웨어 유포 방법이 변화되고 있는 것으로 추정된다.

정부기관을 포함한 여러 보안업체에서 ActiveX 컨트롤 설치 시 권고 사항에 관한 정보 및 가이드를 제공하였고, 이러한 영향으로 일반 사용자들은 ActiveX 컨트롤 설치 시 보안경고창이 나타날 때마다 보다 신중한 자세로 받아들이게 되자 스파이웨어 제작/배포 업체들은 다른 방법이 필요해진 것으로 추정해볼 수 있을 것이다.

IE의 ActiveX 보안경고창은 사용자의 적절한 동의를 받는 과정이라고 볼 수 없다. ActiveX 컨트롤 설치 시 나타나는 보안 경고창은 IE의 기본 기능으로 IE 보안 설정에 따라 나타나지 않을 수 있으며 ActiveX 보안경고창은 정보통신부 스파이웨어 기준, 한국정보보호 진흥원 스파이웨어 사례집(http://www.boho.or.kr/infor_data/spyware.pdf 11page)의 내용에 따라 사용자 동의를 받는 부분으로 볼 수 없다. 따라서 스파이웨어 제작업체에서 사용자에게 동의를 받는다고 하는 ActiveX 보안 경고창에 프로그램의 기능 및 이용약관이 기재되어 있는 페이지를 하이퍼링크를 이용하여 링크시키는 방식은 사용자의 동의를 받는 과정이라고 볼 수 없다. 또한 이렇게 설치되는 대부분의 스파이웨어는 설치과정에서 사용자 약관과 제품의 기능, 동작에 대한 어떠한 설명도 명시하지 않고 있어 사용자가 설치되는 프로그램을 정확한지 할 수 없고 프로그램 설치 취소를 할 수도 없다는 문제점이 있다.

아래 [그림 2-7]은 이지캐취(Win-Adware/Rogue.EZCatch)를 설치했을 때 여러 호스트에 접속하는 네트워크 데이터를 캡쳐한 화면이다.

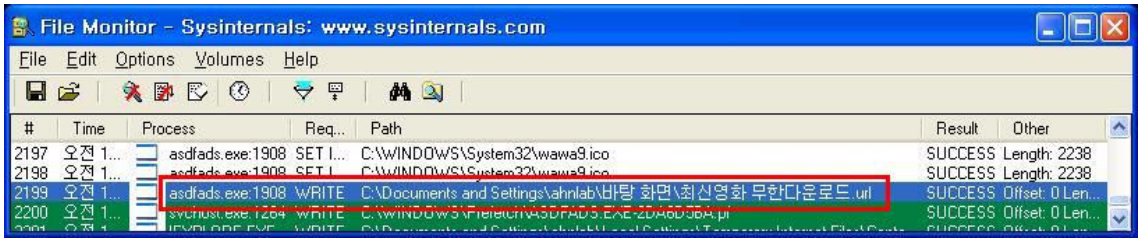


[그림 2-7] 스파이웨어 설치 시 네트워크 데이터 캡쳐한 화면

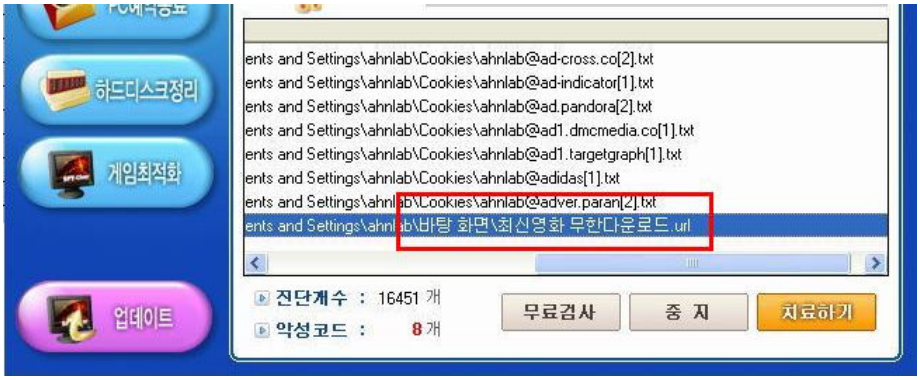
이렇게 하나의 스파이웨어가 설치되면, 동시에 여러 개의 스파이웨어를 설치하는 방법으로 하나의 회사가 다른 제품을 각각의 제어 서버에서 다운로드하여 설치하는 경우가 다수 발생

하고 있다. 특히 이지캐취의 경우에 자신이 다운로드하여 번들로 설치하는 애드웨어를 진단하기도 한다.

[그림 2-8]는 허위 안티-스파이웨어의 번들 프로그램이 바로가기를 설치하는 과정으로, [그림 2-9]에서 이렇게 생성된 바로가기를 진단하고 제거를 위해 유료 사용을 요구한다.



[그림 2-8] 이지캐취가 설치한 애드웨어에 의해 바로가기가 설치되는 화면

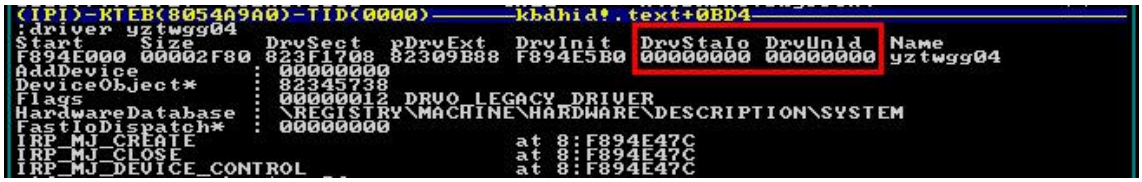


[그림 2-9] 이지캐취가 [그림 2-8]에서 설치한 바로가기를 진단하는 화면

삭제를 방해하는 진화된 시스템 드라이버

최근 중국에서 제작된 것으로 추정되는 윈도우 시스템 드라이버가 발견되었는데, 이 모듈은 일반적으로 드라이버 삭제를 위하여 필요한 드라이버언로드 (DriverUnload) 함수를 등록하지 않고 이전보다 더 제거하기 힘들게 만들어졌다

시스템 드라이버를 제거하기 위해서는 특정 IoControlCode와 인코딩된 문자열을 드라이버로 전송하여야 하고, 이러한 정보를 받은 시스템 드라이버는 파일을 삭제할 수 있는 기회를 제공한다. 이는 특정 IoControlCode와 문자열은 인가 받지 못한 프로그램이 임의로 자신을 제거 및 삭제되는 것을 방지하고자 하는 목적이 있다. 이번에 발견된 시스템 드라이버의 경우 특정 IoControlCode와 문자열뿐만 아니라 삭제를 위한 코드를 제공하지 않아 제거가 매우 어렵다.



[그림 2-10] DriverUnload 함수가 등록되지 않은 시스템 드라이버 정보 화면

결국 위와 같은 시스템 드라이버 파일을 삭제하기 위해서는 아래와 같은 순서로 서비스를 종료시켜야 하고, 해당 서비스가 종료된 후에 파일을 삭제할 수 있다.

```
DeviceIoControl (
        hDrv,
        0x839B9C28,                 ← 시스템 드라이버가 사용하는 핸들을
                                      종료시키는 IoControlCode
        "pello everyday₩0",         ← IoControlCode의 유효성을 검사하는 문자열
        0xF,
        &dwOut,
        sizeof(dwOut),
        &dwRet,
        NULL);
ControlService (hSrv, SERVICE_CONTROL_STOP, pSrvStatus);
DeleteService (hSrv);
DeleteFile ("%SystemRoot%₩₩System32₩₩Drivers₩"_FILE_NAME_".sys");
```

위의 시스템 드라이버 이외에 동일한 이름으로 %SystemRoot₩System32 폴더에 동적 라이브러리(DLL)가 생성되는데 이 파일을 제거하기 위해서는 시스템 재부팅이 필요하다. 왜냐하면 위의 시스템 드라이버는 언로드(Unload) 하는 기능이 없기 때문에 위 코드를 실행한 후에도 메모리에는 위의 시스템 드라이버가 동작하고 있기 때문이다.

시스템 드라이버의 언로드 기능이 완전히 없어졌다는 것이 이전과 달라진 점이다. 참고로 이전에는 DriverUnload 함수가 등록되어 있지 않아도 특정 IoControlCode를 전송했을 때 시스템 드라이버를 언로드하는 기능이 있었다.

(3) 시큐리티 - 티맥스 제우스 어플리케이션 서버 취약점 및 플래시 플레이어 취약점

2007년 7월 역시 영향력이 큰 어플리케이션의 패치가 발표되었다. 매달마다 정기적으로 발표되는 마이크로소프트의 정기 보안 패치 외에도 티맥스 소프사의 미들웨어인 제우스, 파이어 폭스 웹 브라우저, 플래시 플레이어에 관한 패치가 발표되었다.

마이크로소프트 보안 패치

2007년 7월에 발표된 마이크로소프트 사는 총 6개의 보안 패치를 발표하였다[표 1]. 발표된 보안 패치중 등급이 '보통'인 MS07-038을 제외한 나머지 패치는 임의의 코드 실행이 가능한 취약점에 적용되는 것으로 해당 소프트웨어를 사용하고 있는 사용자는 반드시 해당 패치를 설치하여 만약에 있을 보안 위협을 사전에 방어해야 한다.

위험등급	취약점	PoC
긴급	Microsoft Excel 취약점으로 인한 원격 코드 실행 문제점 (MS07-036)	무
긴급	Windows Active Directory의 취약점으로 인한 원격 코드 실행 문제점 (MS07-039)	무
긴급	.NET Framework 취약점으로 인한 원격 코드 실행 문제점 (MS07-040)	무
중요	Miicrosoft Office Publisher 취약점으로 인한 원격 코드 실행 문제점 (MS07-037)	유
중요	Microsoft 인터넷 정보 서비스 (IIS)의 취약점으로 인한 원격 코드 실행 문제점(MS07-041)	무
보통	Windows Vista 방화벽의 취약점으로 인한 정보 유출 문제점 (MS07-038)	무

오피스 제품군이나 인터넷 익스플로러(IE) 같은 클라이언트 어플리케이션에 집중되었던 예전 패치와는 달리 2007년 7월 패치는 클라이언트 어플리케이션의 비중이 줄고 Active Directory나 IIS와 같은 서버 어플리케이션의 비중이 늘어난 것이 특징이다. 하지만 2007년 7월 역시 엑셀과 같은 오피스 제품군에 대한 패치가 발표되었고 또 공격자가 불특정 다수의 사용자들을 공격대상으로 할 수 있다는 점에서 앞으로 클라이언트 어플리케이션의 패치 비중은 현 상태를 유지하거나 증가할 것이다.

티맥스 미들웨어 제우스의 디렉토리 및 소스코드 노출 취약점

국가 사이버 안전센터 (NCSC)는 2007년 7월 16일 티맥스 소프트의 미들웨어인 제우스(JEUS)에서 디렉토리 파일 목록 및 JSP 소스코드가 노출되는 보안 취약점을 발표하였다. 제우스 미들웨어는 국내 많은 수의 정부기관과 금융기관이 사용하고 있고 소스코드 노출로 인한 제 2의 정보노출이 가능하다는 점에서 해당 취약점의 영향은 매우 크다고 할 수 있다.

해당 취약점은 사용자가 test.jsp%00와 같이 JSP 파일 이름에 %00과 같은 URL 인코딩된 문자를 덧붙여 웹 브라우저로 요청할 경우 소스코드를 그대로 노출하게 되는 것으로 NULL-문자열 취약점과 형태와 원리가 매우 비슷하다.

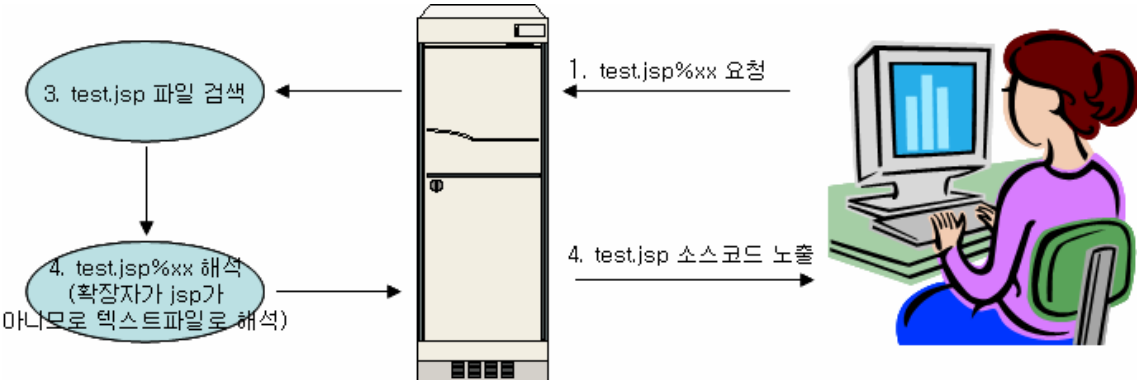
NULL-문자열 취약점은 서로 다른 프로그래밍 언어로 구현된 라이브러리가 문자열을 다른 방법으로 다루는 데서 발생한다. 예를 들어 C/C++과 같은 언어에서 %00문자는 문자열의 끝을 의미하지만 ASP, PHP와 같은 스크립트 언어에서는 문자열의 끝이 자동으로 처리되기 때문에 %00문자가 문자열의 끝을 의미하지 않는다. [그림 1]은 전형적인 널-문자열 취약점의 예이다. 패스워드를 변경하는 펄 코드로 만약 $username 변수의 값이 “root”가 아닌 경우만 패스워드 변경 작업이 가능하다. 하지만 사용자가 $username 변수의 값을 “root/0”으로 입력한 경우 펄은 /0문자를 문자열의 끝으로 처리하지 않기 때문에 결과적으로 $username 변수 값 검사를 통과하여 root 유저의 패스워드를 변경할 수 있다.

```
if($username ne "root")
{
    #패스워드 변경, passwd 명령어
}
else
{
    die("root사용자의 비밀번호는 변경할 수 없습니다.")
}
```

[그림 2-11] 전형적인 널-문자열 취약점의 예

현재 대부분의 웹 어플리케이션은 많은 수의 라이브러리로 만들어진 모듈로 구성되어 있으며 모듈 사이에 데이터 교환이 종종 일어난다. 만약 모듈 사이에 문자열을 취급하는 방법이 다르다면 [그림 2-11]의 예와 같이 심각한 문제가 발생할 수 있다. 또한 스크립트 언어와 고급언어 사이의 인터페이스뿐만 아니라, 같은 언어를 사용하여 만들어진 모듈 사이에도 문자열을 처리하는 방법이 다르다면 같은 문제가 발생할 수 있다.

티맥스의 미들웨어인 제우스 역시 많은 라이브러리를 이용한 모듈로 구성되어 있으며 이번에 발견된 취약점 역시 서로 다른 모듈들이 문자열을 다른 방법으로 취급하는 과정에서 발생한 것으로 추정된다. 만약 사용자가 JSP 파일 이름에 특정 URL 인코딩된 문자를 덧붙여 요청할 경우 URL에 해당하는 파일을 찾는 모듈은 파일 이름 끝에 붙여진 인코딩된 문자를 무시하여 해당 JSP 파일을 찾지만 인코딩된 문자를 무시하지 않는 JSP 해석 모듈에서는 파일의 확장자를 JSP가 아니기 때문에 해당 파일을 일반 텍스트 파일로 취급하여 소스코드를 노출한다.



[그림 2-12] 제우스 소스코드 노출 시나리오

따라서 웹 어플리케이션에서 이와 같은 취약점이 발생하지 않도록 하기 위해서는, 첫째 어플리케이션의 모든 모듈의 문자열 처리 방법을 통일하고, 둘째 URL 인코딩 된 문자를 올바르게 필터링 하며, 셋째 펄과 같은 스크립트 언어를 사용할 경우 유저의 입력이 시스템 명령에 사용될 수 없도록 펄의 taint 모드와 같은 설정을 하도록 하는 것이 필요하다.

FireFox firefoxrul 취약점

2007년 7월 10일 파이어폭스 웹 브라우저에서 임의의 코드가 실행될 수 있는 취약점이 발표되었다. 그 동안 인터넷 익스플로러 (IE)에 비해 상대적으로 안전하다고 알려진 파이어폭스에서도 이번 취약점이 발견되면서 더 이상 “안전”을 장담할 수 없게 되었다. [그림 3]은 파이어 폭스에서 명령어를 실행하기위한 커맨드 쉘을 실행하기 위한 코드의 예이다. 이 코드를 포함하는 URL 링크를 IE에서 클릭할 경우 커맨드 쉘이 실행된다.

[그림 2-13] 파이어폭스 취약점을 이용한 커맨드 쉘 실행 코드 예

파이어폭스를 설치하면 firefoxurl 핸들러가 등록된다. 이 핸들러의 목적은 IE처럼 HTML 파일을 읽고 해석하는 소프트웨어에서 파이어폭스를 실행하기 위한 것이다. 예를 들어 사용자가 IE에서 firefoxurl 핸들러를 명시하면 URL을 요청하면 파이어폭스가 실행된다. 이 때 firefoxurl 핸들러는 URL을 파라미터로 해석하고 이것을 명령행 인자로 사용하여 파이어폭스를 실행하는데 취약점이 존재하는 버전의 경우 파라미터에 대한 검증을 하지 않는다.

따라서 이러한 점을 악용하면 공격자는 임의의 명령행 인자로 파이어폭스를 실행할 수 있다.

특히 공격자가 –chrome 파라미터를 이용하여 파이어 폭스를 실행할 경우 chrome문맥에서 임의의 자바스크립트가 실행되므로 유저 프로파일 생성 및 XSS 공격, 임의의 코드 실행으로 인한 시스템 권한 획득이 가능하다.

해당 취약점을 이용한 공격을 방어하기 위해서는 해당 취약점에 대한 패치를 반드시 설치해야 하며 그렇지 못할 경우 firefoxurl 핸들러를 제거하여 firefox 핸들러를 이용한 파이어 폭스 실행을 차단해야 하며, 파이어폭스의 업데이트가 필요하다.

플래시 플레이어 취약점

2007년 7월 10일 플래시 플레이어가 가지고 있는 취약점이 발표되었다. 이 취약점은 플래시 플레이어가 사용하는 FLV 데이터 파일을 검증하지 못하여 발생한다. 이 취약점은 웹 브라우저에서 사용 가능한 플래시 플레이어의 특성상 불특정 다수의 사용자를 공격대상으로 할 수 있기 때문에 그 영향은 매우 크다고 할 수 있다.

일반적으로 FLV 파일은 파일헤더와 비디오, 오디오, 스크립트 데이터를 나타내는 일련의 FLV 태그로 구성된다. 다음 2개의 표는 각각 FLV 파일헤더와 태그 데이터를 나타낸 것이다. 모든 정수(integer) 데이터들은 빅엔디언(Big-Endian) 형식으로 저장되어 있다.

Offset	Size	Description
0x0000	3	Magic Code, 'FLV'
0x0003	1	Version, 항상 1
0x0004	1	Flags
0x0005	4	DataOffset/Header Size, 일반적으로 9

Offset	Size	Description
0x0000	3	태그 형식:8: 오디오 9: 비디오, 0x12:스크립트
0x0001	1	Data Size (n)
0x0004	1	Timestamp
0x0008	4	스트림아이디, 항상 0
0x000b	N	Data

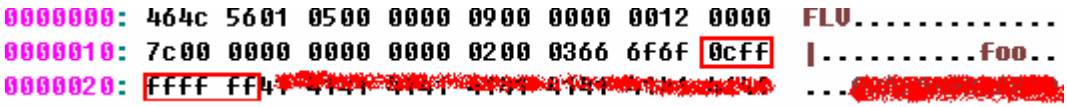
이중 스크립트 태그는 플래시 액션 스크립트를 정의하는 일련의 SCRIPTDATAOBJECT 레코드로 구성되고, SCRIPTDATAOBJECT 레코드는 다시 ObjectName 필드와 ObjectData 필드로 정의된다. ObjectName 필드의 구조는 다음 표와 같다.

Offset	Size	Description
0x0000	1	ObjectName type (항상 2)
0x0001	2	ObjectNameSize (n)
0x0003	N	ObjectNameData

ObjectData 필드의 첫 바이트는 스트링과 같은 데이터 형식을 나타내며 ObjectData 필드가 나타내는 데이터 형식은 다음과 같다.

0:Number, 1:Boolean, 2:String, 3:Object, 4:MovieClip 5:Null, 6:Undefined 7:Reference, 8:ECMA 배열, 10:Strict 배열, 11:Data, 12: Long String

이중 Long String 데이터는 문자열의 길이를 나타내는 필드와 데이터로 구성되어있다. 플래시 플레이어는 Long String 복사를 (Long String 데이터 크기 + 1)만큼의 사이즈로 메모리를 할당하는데 이때 데이터 크기를 0xffffffff로 정의하면 플래시 플레이어는 이 숫자를 부호있는 정수(-1)로 생각하여 크기가 0(-1+1=0)인 메모리를 할당하게 된다. 이 후 문자열 복사가 비정상적으로 이뤄지고 결국 오버플로우가 발생한다. 다음 그림은 오버플로우가 발생하도록 조작된 FLV 파일의 일부분으로 데이터 타입이 0xc인 Long String의 크기가 0xffffffff로 되어있기 때문에 이후 문자열 데이터가 비정상적으로 복사된다.



플래시 플레이어는 UCC 에서도 많이 사용되고 있고, 웹상에서 악성코드 배포에도 사용할 가능성이 많음으로 주의가 필요하며, 플래시 플레이어 취약점에 대한 보안 업데이트는 Adobe 사이트를 참고하면 된다.

III. ASEC 컬럼

(1) 10년전 악성코드 제작자들

지금으로부터 10년 전인 1997년 여름 악성코드 제작자들은 무엇을 하고 있었을까? 지금은 트로이목마가 악성코드의 대부분을 차지하고 있었지만, 당시에 대부분의 바이러스 제작자들은 현재에는 많이 시들해진 도스 바이러스와 매크로 바이러스를 제작하고 있었고, 조금 실력 있는 제작자들은 보다 완벽한 윈도우 바이러스 제작에 몰두하고 있었다.

다음은 1996년부터 2000년까지 발견된 윈도우 악성코드와 윈도우 바이러스에 대한 대략적인 개수이다.

년 월	윈도우 악성코드	윈도우 바이러스
1996년 1월	1	1
1997년 12월	1	1
1998년 1월	1	1
1998년 2월	12	12
1998년 3월	12	12
1998년 6월	6	6
1998년 12월	17	6
1999년 1월	45	8
1999년 6월	36	11
1999년 12월	127	20
2000년 1월	77	14
2000년 6월	104	17
2000년 12월	168	41

[표 3-1] 1997년 - 2000년까지 발견된 윈도우 악성코드 수

[표 3-1]에서와 같이 윈도우 95 바이러스가 1996년 초에 발견된 이후 일년이 지났어도 새로운 윈도우 바이러스가 등장하지 않았다. 물론 1996년 말 윈도우 95의 가상 드라이버를 이용해 기억장소에 상주하는 Win95/Punch 바이러스와 Win95/MrKlunky 바이러스가 오스트레일리아와 유럽의 바이러스 제작 그룹에서 경쟁적으로 제작되었지만 이들 바이러스는 제작시기가 한참 지난 후에 공개되었고 많은 버그가 있었다.

1997년 말부터 윈도우 바이러스가 전혀 발견되지 않다가 1998년 초부터 윈도우 바이러스가 조금씩 증가한 것을 알 수 있는데 이는 바이러스 제작자들이 이 기간 새로운 기법을 계속

연구하고 있었으며 바이러스 제작자 커뮤니티에서는 1997년 여름을 뜨겁게 달구었을 것이다.

새로운 윈도우 95, 윈도우 NT 바이러스 제작기법을 연구하는 동시에 몇몇 바이러스 제작자들은 도스 바이러스와 윈도우 바이러스를 접목시켰다. 도스 실행 파일, 윈도우 NE 실행 파일, 워드 문서를 감염시키는 이색적인 Anarchy.6093 바이러스가 발견되었지만 윈도우 3.1에서 사용하는 NewExe를 감염시키므로 현대적 의미의 윈도우 95 이상의 바이러스와는 거리가 멀다.

페루에서 자신을 Jacky Qwerty로 부르는 10대가 윈도우 95뿐 아니라 윈도우 NT 에서도 큰 문제 없이 감염되는 바이러스를 제작하고 1998년 2월 바이러스 제작 잡지를 통해 기법이 알린다. 이로써 기술적으로 증명되고 이를 이용하거나 응용한 많은 바이러스들이 등장하고 1998년부터 본격적인 윈도우 실행 파일 감염 바이러스들이 퍼지면서 사용자들을 괴롭히기 시작하였다.

1997년 11월 스페인의 바이러스 제작자는 도스, 윈도우, 매킨토시 실행 파일을 감염시키는 에스페란토 바이러스(Esperanto virus)를 제작하지만 제작자의 주장과는 다르게 매킨토시 실행 파일 감염에는 실패한다.

윈도우 95/98 상주형 바이러스도 안정적으로 변화되어 10월부터 Win95/Anxiety_Poppy 바이러스가 독일, 핀란드, 미국, 한국 등에 퍼지기 시작한다.

1997년 뜨거운 여름 전 세계 바이러스 제작자들이 보다 안정적인 윈도우 바이러스 제작을 위해 노력하고 있었다. 역사에 가정은 없다지만 그런 노력을 모두의 이익을 위한 프로그램 개선에 땀을 흘렸다면 과연 어땠을까?

(2) DLL 형태의 윈도우 바이러스 Win32/Durchina

증상 및 요약

해당 바이러스는 “thunbs.db”(71,168bytes)라는 이름을 갖는 EXE파일로 UPX로 실행압축되어 있으며, “%windows%Downloaded Program Files₩” 폴더 및 이동식 드라이브에 자신의 복사본 및 내부의 DLL모듈(muniu.dll, 58,880bytes)을 생성한다. 이동식 드라이브에는 자동실행을 위한 Autorun.inf 파일을 생성하며, DLL모듈이 실제 Virus기능 및 Trojan(Downloader, GameHack)기능을 포함한다. 감염형태는 후위형인 윈도우 바이러스이다.

특이사항

EXE파일처럼 UPX로 실행압축되어 있는 DLL파일(muniu.dll)은 실행중인 모든 프로세스에 인젝션(Injection)되어 동작하며, Kernel32.dll의 특정 API함수의 첫 5바이트를 메모리상에서 수정하여, 해당 API 사용 시 자신의 코드 중 일부로 분기(JMP)하도록 한다. 만약, 정상파일 실행 시 해당 API를 사용할 경우, 바이러스에 감염되는 증상이 나타난다. Win32/Durchina바이러스에서 수정하는 API 리스트는 다음과 같다.

FindFirstFileW, FindFirstFileA, FindFirstFileExA, FindFirstFileExW, FindNextFileA, FindNextFileW, CreateFileA, CreateFileW

이중에서 바이러스 감염루틴으로 분기하는 API함수는 CreateFileA, CreateFileW이며, 나머지 API함수는 GameHack및 Downloader기능을 수행하는 코드로 분기한다. 분기 후 존재하는 코드에는 공통적으로 자신이 수정한 원본 API 시작 5바이트를 복원하는 기능을 갖는다.

치료이슈

Win32/Durchina 바이러스에 감염 시 실행중인 모든 프로세스에 인젝션(Injection)되므로 치료 시 메모리상에서 Winlogon.exe및 Explorer.exe에 삽입된 “muniu.dll”을 Unload 해야 한다. 또한, %windows%Downloaded Program Files₩ 폴더에 생성되는 “thunbs.db”, “muniu.dll”파일의 경우, Thread 루틴에 의해 일정간격으로 삭제 및 재생성을 반복 수행함으로 실시간 감시에서 정상적으로 치료되지 않을 가능성이 있다.

바이러스 코드 삽입 시 마지막 섹션의 Size Of Raw Data값이 아닌 Virtual Size 값을 통해 자신의 코드를 삽입한다. 즉, 삽입되는 바이러스 코드가 파일의 끝이 아닐 수 있고, 일부 데이터가 바이러스 코드로 덮어 쓰여질 수 있다. 이 경우, V3에서는 덮어 쓰여진 부분을

NULL로 채우는 것으로 치료를 한다.

상세분석정보

Win32/Durchina는 %windows%, %winnt% 폴더를 제외한 모든 폴더 및 드라이브의 *.EXE, *.SCR 확장자를 갖는 PE파일을 감염대상으로 하며, “mir.exe”, “minue.exe”파일은 감염에서 제외된다. 또한, MZ, PE 문자열을 통해 PE파일 인지 여부를 체크하며, 파일크기가 0x2800 보다 크고 0xA00000보다 작은 파일만을 감염대상으로 한다.

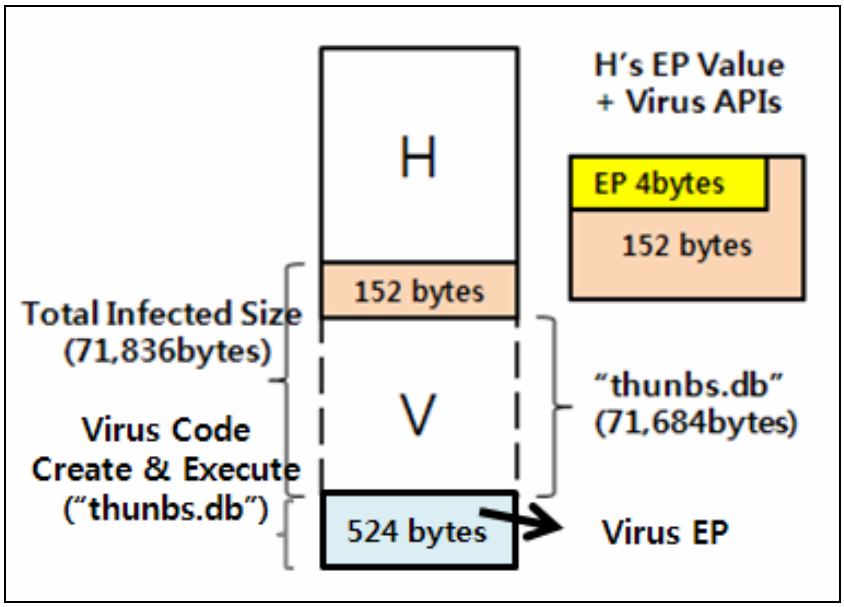
Win32/Durchina는 단순 실행 시 감염증상이 나타나지 않으며, 자신이 수정한 Kernel32.dll의 특정 API함수(CreateFileA, CreateFileW)를 사용하는 프로그램을 실행 시, 감염루틴으로 분기하여 감염이 이루어진다. 아래 [그림 3-1]은 특정 API함수를 검색하여 해당 함수의 시작코드 5바이트 수정하는 부분이다.

```
…
PUSH  EAX
CALL  muniu.00896914                ; kernel32.VirtualQuery
PUSH  muniu.008C4264
PUSH  80
PUSH  4
MOV   EAX, DWORD PTR DS:[EDI]
PUSH  EAX
CALL  muniu.0089690C                ; kernel32.VirtualProtect
PUSH  muniu.008C424C
PUSH  5
PUSH  muniu.008C41BC
MOV   EAX, DWORD PTR DS:[EDI]
PUSH  EAX
CALL  muniu.008967EC                ; kernel32.GetCurrentProcess
PUSH  EAX
CALL  muniu.00896934                ; kernel32.WriteProcessMemory
…
```

[그림 3-1] 특정 API의 시작코드 수정하는 부분

감염대상 파일을 찾으면, 감염 전에 해당 파일의 날짜정보 및 속성정보를 백업해 두었다가 감염 후 복구하는 기능을 갖는다. 아래의 [그림 3-2]는 Win32/Durchina에 감염 후 변경된 파일구조를 나타낸다. 바이러스 본체(thunbs.db)앞에 추가된 152bytes데이터는 감염 전 원본파일의 EP값 4바이트와 Virus에서 사용하는 API들을 나타낸다. 또한, [그림 3-2]에서 감염된 파일의 EP가 속한 524바이트의 코드는 “thunbs.db”(바이러스 원본)을 생성 및 실행해 주는 코드로서 152바이트에 존재하는 API들(GetProcAddress, ShellExecuteA등)을 이용한

다. 감염 시 새롭게 추가된 524바이트 코드는 감염된 바이러스마다 동일한 코드를 가지므로 진단 시 EP에서 특정 코드를 진단 값으로 활용할 수 있다.



[그림 3-2] 감염 후 파일구조

Win32/Durchina에 감염 후, 수정되는 Optional Header및 Section Header의 내용은 다음과 같다.

- Optional Header에서 수정되는 곳은 Size Of Image, Address Of Entry Point, Win32 Version Value 세 부분이다. 이 중 Size Of Image값은 감염 후 수정된 마지막 섹션의 *Virtual Size + RVA* 값으로 변경되며, Win32 Version Value는 *0x00000077*로 변경된다. 이 값은 Win32/Durchina 바이러스에서 기 감염여부 체크 시 사용하는 Signature값이다.

- Section Header 중에서 수정되는 곳은 마지막 섹션이며, Virtual Size, Characteristics, Size Of Raw Data 세 부분이다. 이 중 Virtual Size값은 원본의 *Virtual Size + 0x1189C(71,836)* 값으로 변경되며, Characteristic값은 *0xE0000E0*로 변경된다. 또한, Size Of Raw Data값은 수정된 Virtual Size 값을 File Align값에 맞춰 보정한 값이다.

치료

감염 전 원본의 OEP값은 바이러스 코드 시작 첫 4바이트 값([그림 3-2] 참고)이며, 해당 정보는 Win32/Durchina 바이러스의 EP에서 특정 옵셋만큼 떨어진 거리를 계산하여 얻어올 수 있다. 또한, 해당 옵셋부터 파일 끝까지 바이러스 코드를 잘라내고, 수정된 Optional Header및 마지막 Section Header의 내용을 감염 시 적용한 규칙에 맞춰 적절하게 복원하면

된다.

기타정보

Win32/Durchina의 실행 시 자신의 복사본 및 DLL을 생성한 "%windows%Downloaded Program Files₩"폴더를, 파일 생성 시, 사용자가 파일을 볼 수 없도록 되어 있으며, 반복적인 삭제작업으로 샘플의 수집이 어렵다. 또한, 자신을 로드 한 프로세스가 "explorer.exe"일 경우, 아래의 사이트로 접속을 시도하며, 파일다운로드 기능을 갖는다. 또한, IE에서 특정 사이트 접속 시, 사용자가 입력하는 키보드 값을 가로채는 기능도 수행한다.

http://www.md80.cn/muniu/temp.exe
http://www2.md80.cn/muniu/temp.exe
http://www3.md80.cn/muniu/temp.exe

바이러스 감염루틴이 DLL자체에서 이루어지지 않고, 특정 API 호출 시 분기하는 코드에 의해 수행됨으로 바이러스 증상이 쉽게 나타나지 않는다. 따라서 단순 디버깅만으로 감염루틴을 찾기 어려운 바이러스였다.