ASEC Report 6월

® ASEC Report

2007. 7

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) 6월 악성코드 통계

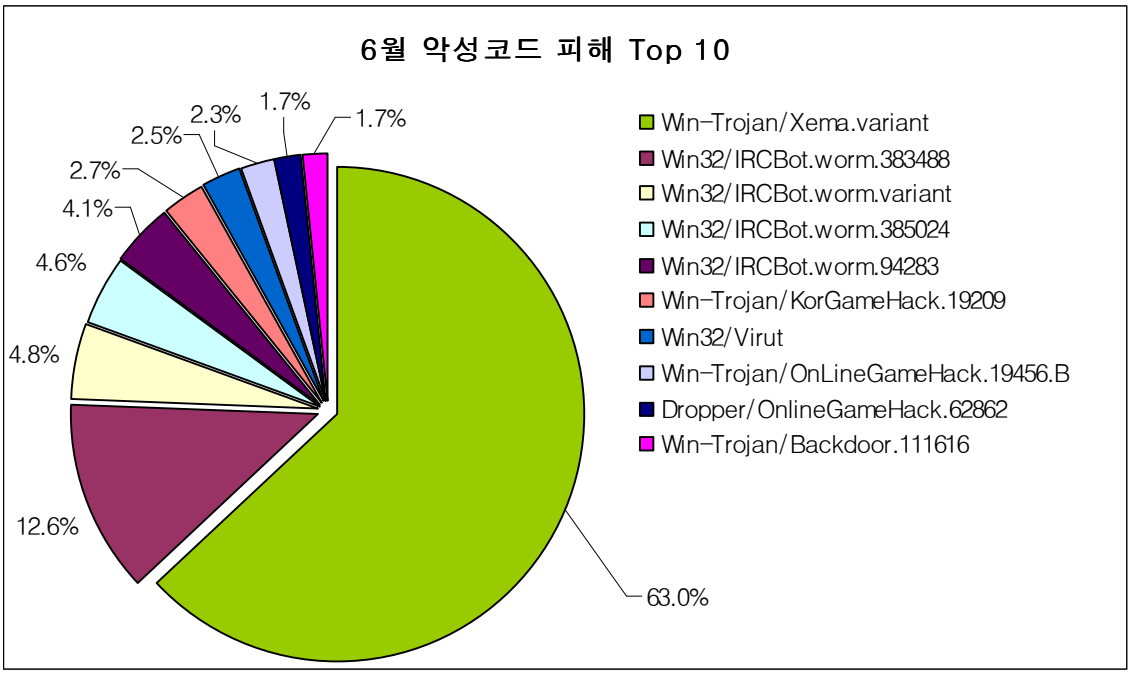
순위		악성코드명	건수	%
1	-	Win-Trojan/Xema.variant	380	63.0%
2	new	Win32/IRCBot.worm.383488	76	12.6%
3	new	Win32/IRCBot.worm.variant	29	4.8%
4	new	Win32/IRCBot.worm.385024	28	4.6%
5	new	Win32/IRCBot.worm.94283	25	4.1%
6	new	Win-Trojan/KorGameHack.19209	16	2.7%
7	↓3	Win32/Virut	15	2.5%
8	new	Win-Trojan/OnLineGameHack.19456.B	14	2.3%
9	new	Dropper/OnlineGameHack.62862	10	1.7%
9	new	Win-Trojan/Backdoor.111616	10	1.7%
합계			603	100.0%

[표 1-1] 2007년 6월 악성코드 피해 Top 10

월 악성코드 피해 동향

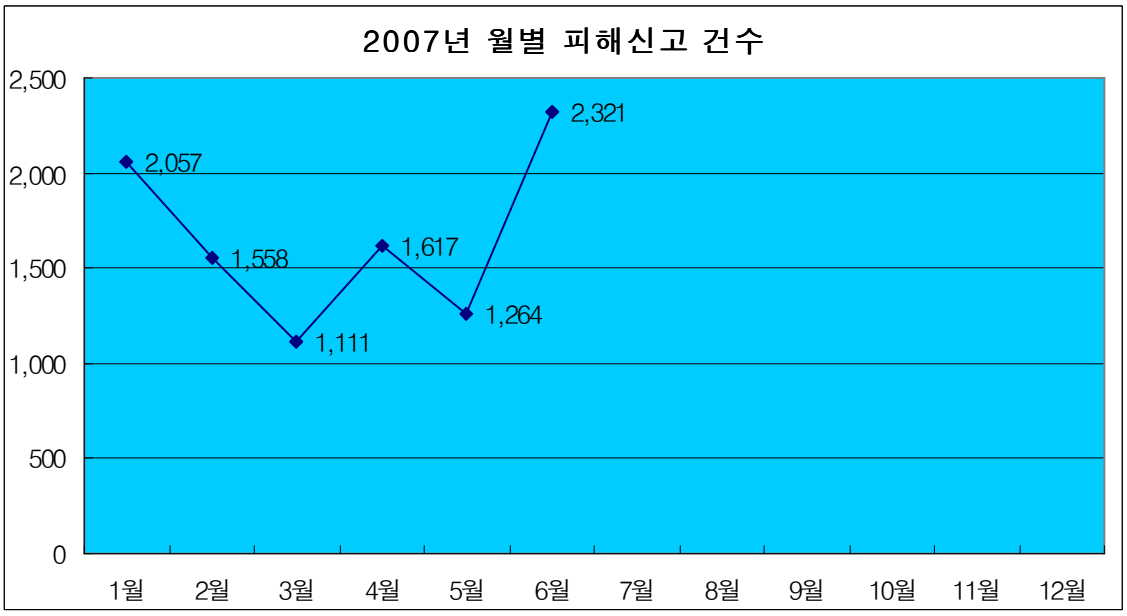
2007년 6월 악성코드Top10에는 전월 1위였던 Win-Trojan/Xema.variant 가 1위를 유지하였으며, 전월 3위였던 바이럿(Win32/Virut)은 7위로 순위가 4계단 하락하였다. Win-Trojan/Xema.variant와 바이럿(Win32/Virut)을 제외하고는 모두 새로이 Top10에 진입하였다. 이는 다양한 악성코드들이 새로이 나타나고 있음을 단적을 보여주고 있다. 하지만, 여전히 트로이 목마류는 드롭퍼까지 포함하여 5종이 포함되어 고객정보 탈취를 통한 금전적 이득을 목적으로 악성코드 개발이 진행되고 있음을 알 수 있다. 또한, 전월에 Top10에 3종이 포함되었던 아이알씨봇(IRCBOT)은 6월에는 강세를 보이며 모두 5위권 내에 4종이 포함되었다.

6월의 악성코드 피해 Top 10을 도표로 나타내면 [그림 1-1]과 같다.



[그림 1-1] 2007년 6월 악성코드 피해 Top 10

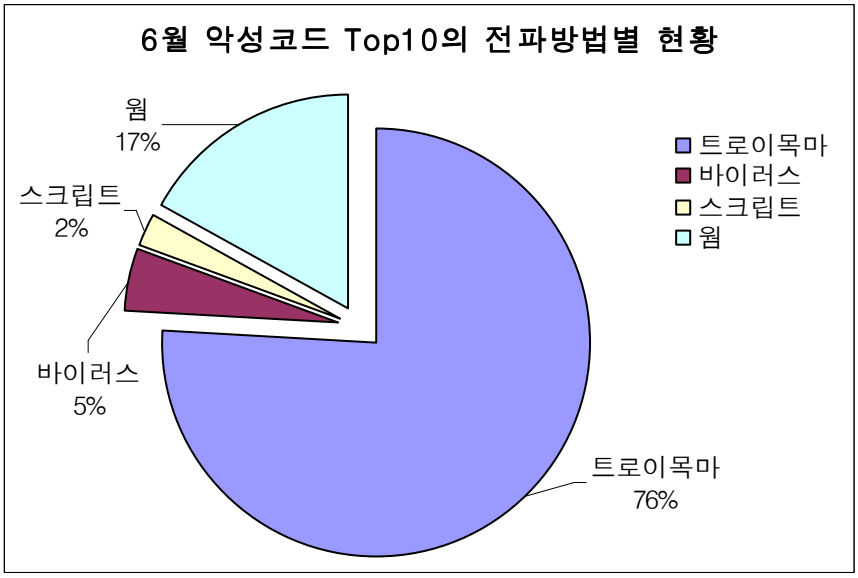
[그림 1-2]에서와 같이 1월부터 월별 피해신고 건수는 꾸준히 감소세를 보이다가 6월에는 전월보다 1000건 이상 증가하였다. 이는 확산력이 강한 아이알씨봇(IRCBOT)의 증가와 함께 새로운 악성코드로 인한 피해 신고 증가의 영향을 받은 것으로 보인다.



[그림 1-2] 2007년 월별 피해신고건수

6월 악성코드 Top 10 전파방법 별 현황

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

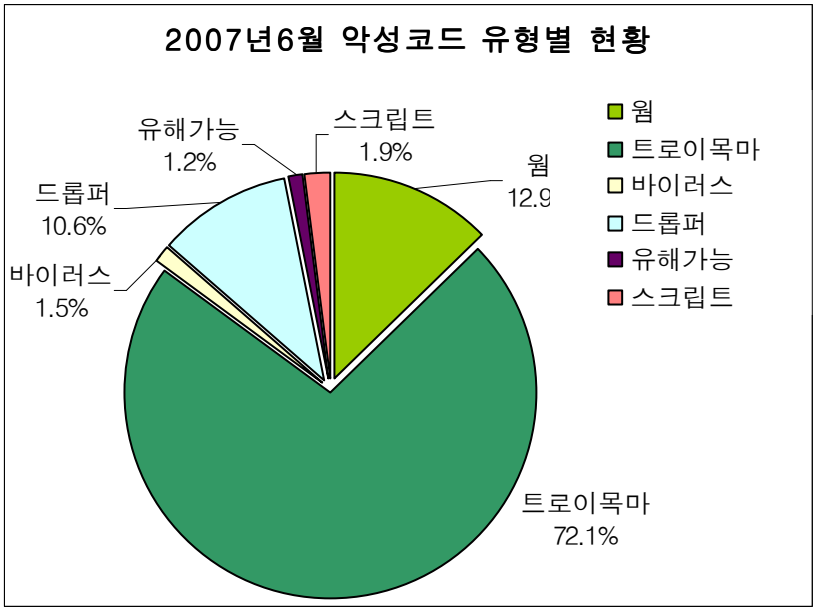


[그림 1-3] 2007년 6월 악성코드 Top 10의 전파방법별 현황

6월에도 변함없이 트로이 목마류가 가장 많은 피해를 발생시켰으며, 점유률은 76%로 전월(73%)에 비해 소폭 증가하였으며, 웜 역시 전월(16%)에 비해 소폭 증가하였다. 바이러스는 바이럿(Win32/Virut)의 순위 하락으로 전월(7%)에 비해 점유율이 하락하였다.

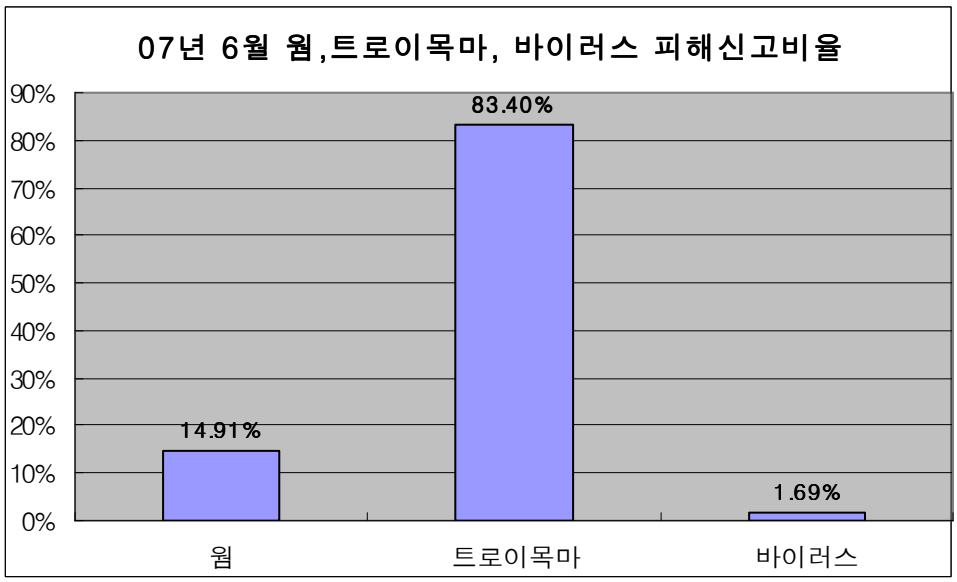
피해신고 된 악성코드 유형 현황

2006년 6월에 피해신고 된 악성코드의 유형별 현황은 [그림 1-4]와 같다.



[그림 1-4] 2007년 6월 피해 신고된 악성코드 유형별 현황

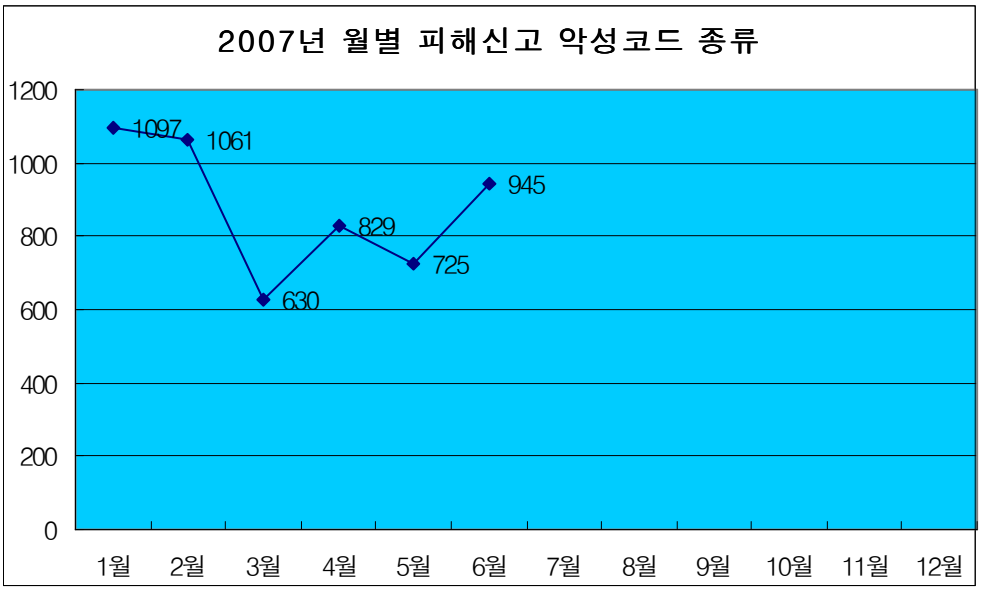
전체 피해 신고에서의 악성코드 유형을 확인해보면, Top10의 악성코드 유형과 동일한 양상을 띠고 있다. 트로이목마가 72.1%로 가장 많았으며 5월까지 2위를 차지하던 드롭퍼(10.6%)는 3위로 밀려나면서 그 자리를 웜(12.9%)이 차지하였다. 그 외 유해가능프로그램이 1.2%, 뒤를 이어 스크립트가 1.9%, 바이러스는 1.5%였다. 이중 주요 악성코드 유형인 트로이목마, 바이러스, 웜에 대한 피해신고 비율을 따져보면 [그림 1-5]와 같다.



[그림 1-5] 2007년 6월 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 있다.



[그림 1-6] 2007년 월별 피해신고 악성코드 종류 개수

국내 신종(변형) 악성코드 발견 피해 통계

6월 한달 동안 접수된 신종 (변형) 악성코드의 건수 및 유형은 [표1], [그림1]와 같다.

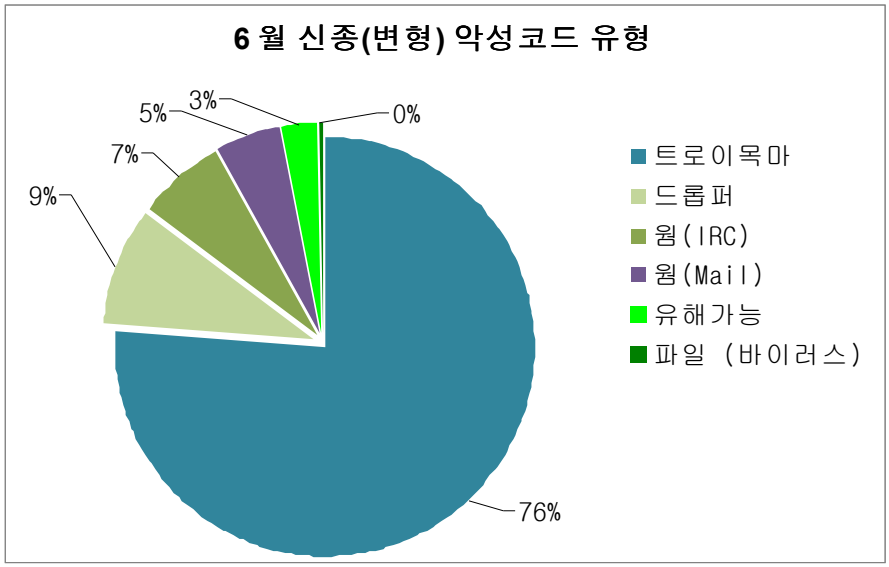
	웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
4 월	84	334	78	0	5	0	0	0	17	0	518
5 월	53	331	59	0	4	0	0	0	34	0	481
6 월	86	431	53	1	1	0	0	0	17	0	589

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

이번 달은 전월 대비 22% 정도 악성코드 수가 증가 하였다. 다음의 악성코드 유형이 증가 했지만 그 원인에 대해서는 명확하지는 않다.

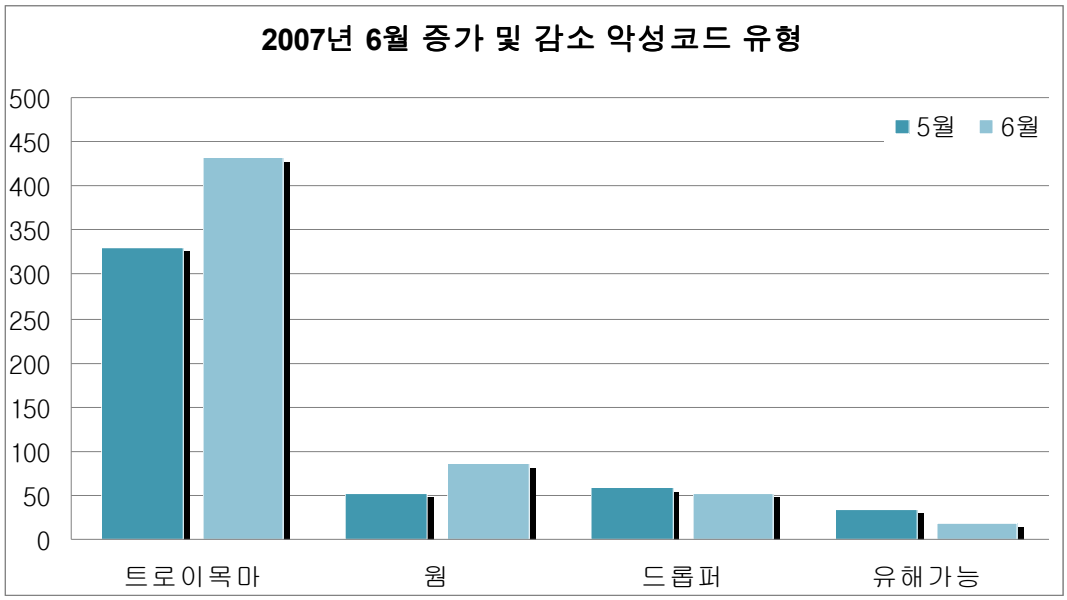
- Win32/IRCBot.worm 변형 – 지난달과 비교하여 28% 증가
- 온라인 게임의 사용자 정보 탈취 트로이목마 – 지난달과 비교하여 26% 증가
- Win-Trojan/Zlob 변형 – 지난달과 비교하여 163% 증가

악성 IRCBot 웜 경우 4월달에 알려진 DNS 관련 취약점 때문에 소폭 증가하였다가 5월에 다시 감소하였으나, 다시 6월에 대폭 증가하였다. 또한 온라인 게임의 사용자 정보를 탈취하는 트로이목마류 경우 국내 온라인 게임을 타켓으로 하는 것 보다는 중국이나 대만 등에서 제작된 게임을 타켓으로 하는 유형이 올해 급속히 증가하고 있다. Win-Trojan/Zlob (이하 지롭 트로이목마)은 다운로더 증상을 가지며 Clicker 또는 허위 안티 스파이웨어 프로그램을 설치한다. 전월 경우 워낙 적은 수가 보고 되었다가 이번 달에 무려 21개의 변형이 보고 되어 그 증가율이 높은 이유라 하겠다.



[그림 1-7] 2007년 6월 신종 및 변형 악성코드 유형

다음 [그림 1-8]은 대표적인 악성코드의 증감 내역이다. 트로이목마는 온라인 게임의 사용자 정보 탈취 트로이목마의 증가를 포함하여 전체적으로 전월대비 30% 가량 증가 하였다.

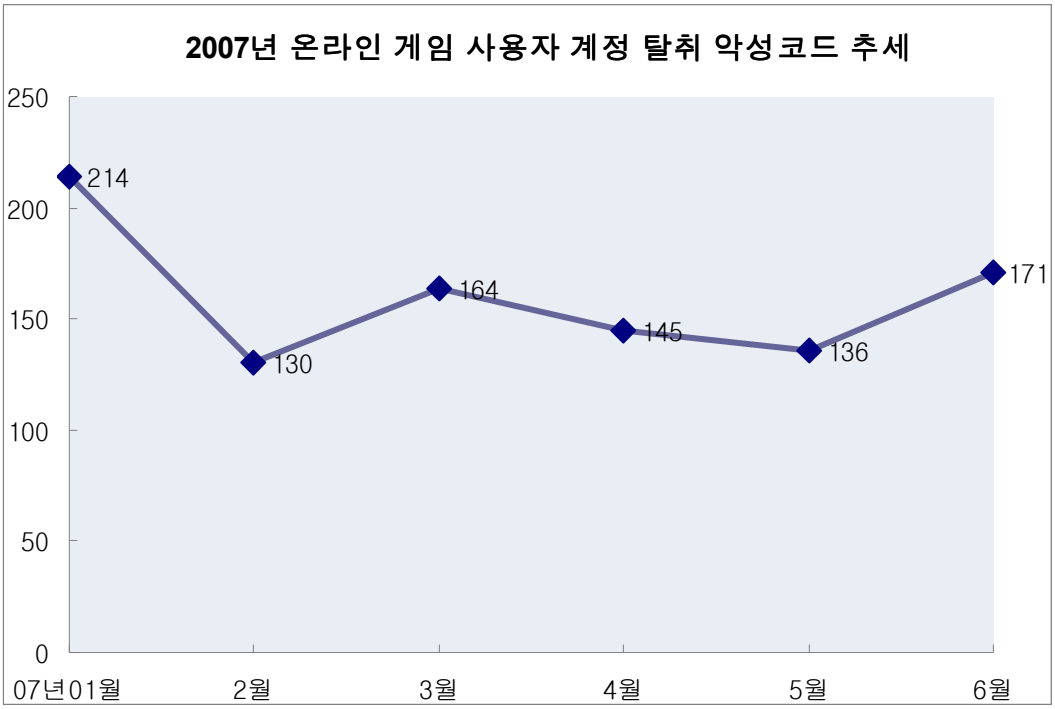


[그림 1-8] 2007년 6월 감소 및 증가 악성코드 유형

웜 유형의 경우 크게 악성 IRCBot 웜과 E-Mail 웜으로 나눌 수 있는데, 이중 악성 IRCBot 웜이 전월대비 28% 가량 증가하였고, E-Mail 웜은 큰 변동이 없으나 Starman 또는 Win32/Allaple.worm 이라고 명명된 악성코드 변형이 다수 출현 하면서 통계 수치는 소폭 증가 하였다. 이 악성코드는 자신이 실행 될 때마다 다른 코드를 가진 변형을 만들어내므로 시그니쳐 기반의 안티 바이러스에서는 이를 모두 다른 변형으로 간주로 하므로 수치가 증가 될 수 있다. 해당 악성코드에 대해서는 이미 Generic 한 진단이 엔진에 포함 되었지만 이번에 알려진 변형은 기존 진단방법에서 진단 되지 않는 형태이였다.

드롭퍼는 큰 변화가 없었고, 실행 파일을 감염시키는 바이러스의 경우 이번 달은 Win32/Viking 바이러스 변형으로 기존에 알려진 변형들과 유사한 1종만 보고 되었다. 유해가능 프로그램 유형은 지난달과 비교하여 50% 감소 하였다. 주된 감소의 원인은 지난달에 Win-AppCare/Virtumonde (이하 버추몬드) 변형이 다수 엔진에 반영됨으로써 이번 달에는 접수가 대폭 줄었다. 버추몬드의 경우 스파이제로 제품에서 대응하기 때문에 V3 통계수치와 차이가 발생 할 수 있다.

다음 [그림 1-9]는 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]

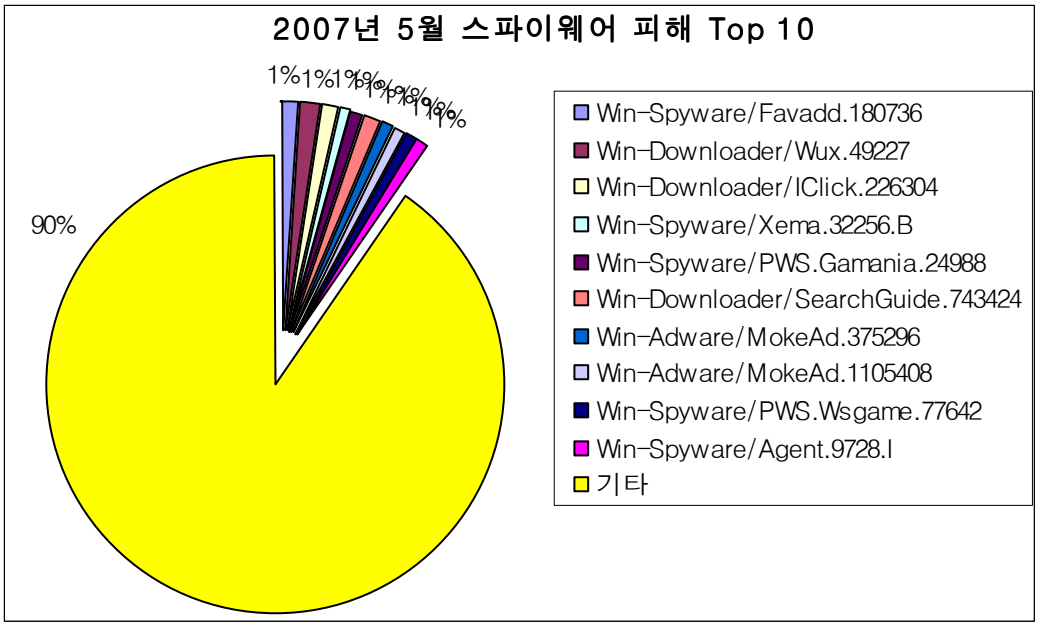
위에서 언급한대로 전월 대비 26% 가량 증가하였다. 올해 들어서는 2번째로 가장 많은 수가 발견 된 것으로 이전 보고서에서도 밝혔듯이 국내 온라인 게임을 타켓으로 하는 트로이목마 유형은 감소 추세에 있다. 그러나 국내에서는 서비스되고 있지 않는 중국이나 대만 현지의 온라인 게임의 데이터를 노리는 형태가 계속적으로 증가 하고 있는 추세라 할 수 있다. 또한 이들은 다양한 온라인 게임의 정보를 동시 다발적으로 획득하려고 하는 것 역시 추세라고 하겠다.

(2) 6월 스파이웨어 통계

6월 스파이웨어 피해 현황

순위		스파이웨어 명	건수	비율
1	New	Win-Spyware/Favadd.180736	8	1%
2	New	Win-Downloader/Wux.49227	8	1%
3	New	Win-Downloader/IClick.226304	7	1%
4	New	Win-Spyware/Xema.32256.B	6	1%
5	New	Win-Spyware/PWS.Gamania.24988	6	1%
6	New	Win-Downloader/SearchGuide.743424	6	1%
7	New	Win-Adware/MokeAd.375296	6	1%
8	New	Win-Adware/MokeAd.1105408	6	1%
9	New	Win-Spyware/PWS.Wsgame.77642	5	1%
10	New	Win-Spyware/Agent.9728.I	5	1%
		기타	592	90.0%
합계			655	100%

[표 1-3] 2007년 6월 스파이웨어 피해 Top 10



[그림 1-10] 2007년 6월 스파이웨어 피해 Top 10

2007년 6월 스파이웨어 피해 통계의 가장 많은 피해를 입힌 스파이웨어는 스파이웨어 파브애드(Win-Spyware/Favadd.180736)이다. 파브애드는 사용자 동의 없이 국내 유명 쇼핑몰로 Redirection 되는 광고 서버의 즐겨찾기를 추가하는 스파이웨어로서 국내에서 제작된 허

위 안티-스파이웨어 프로그램이나 애드웨어가 다운로드하여 설치하는 것으로 추정된다.

6월 스파이웨어 피해 통계에서도 국내에서 제작된 스파이웨어의 피해가 많은 것으로 나타나고 있으며, 애드웨어 모크애드(Win-Adware/MokeAd)와 같은 중국에서 제작된 애드웨어로 인한 피해가 눈에 띈다.

2007년 6월 유형별 스파이웨어 피해 현황은 [표 1-]와 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
4월	233	94	52	81	2	23	7	6	0	498
5월	320	109	22	122	2	10	2	9	0	596
6월	279	166	46	139	8	16	0	1	0	655

[표 1-4] 2007년 6월 유형별 스파이웨어 피해 건수

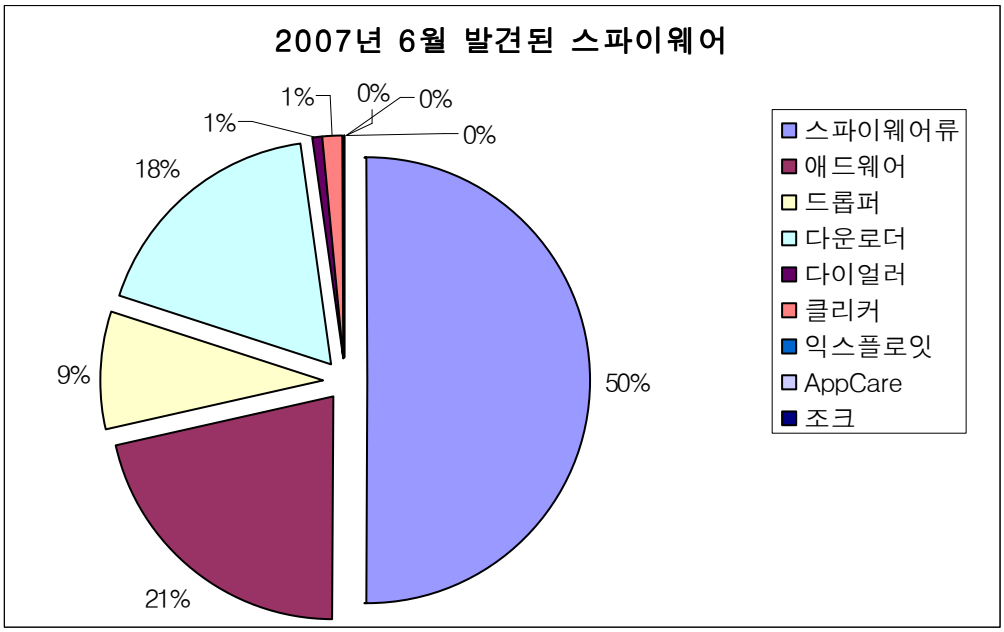
2007년 6월에는 5월보다 약 10% 증가한 655건의 피해 신고가 접수되었다. 스파이웨어의 피해 신고는 다소 감소한 반면 애드웨어의 피해는 크게 증가하였으며, 애드웨어 설치나 다운로드와 관련된 드롭퍼의 피해가 다소 증가하였으며, 위에서 언급한 국내 제작 애드웨어나 허위 안티-스파이웨어 피해 증가가 원인으로 생각된다.

6월 스파이웨어 신종/변종 발견 현황

6월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표3], [그림2]와 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
4월	105	20	13	30	1	5	3	3	0	180
5월	143	29	5	46	1	4	1	3	0	232
6월	108	46	19	38	2	3	0	0	0	216

[표 1-5] 2007년 6월 유형별 신종(변형) 스파이웨어 발견 현황

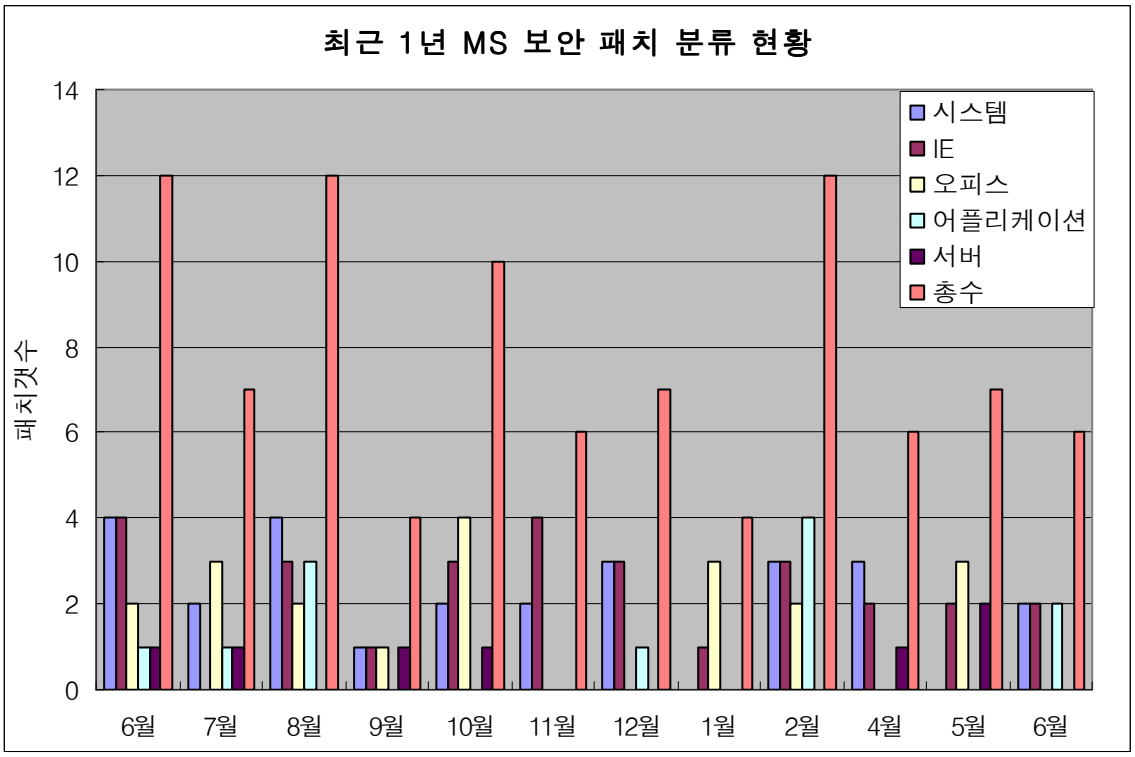


[그림 1-11] 2007년 6월 발견된 스파이웨어 비율

[표 1-5]와 [그림 1-11]은 2007년 6월에 발견된 신종 및 변형 스파이웨어 통계를 보여준다. 5월에 비하여 신종 및 변형 스파이웨어 발견 건수는 다소 감소하였으나, 신종 및 변형 애드웨어의 발견 건수가 5월의 29건에서 6월 46건으로 크게 증가하였다.

(3) 6월 시큐리티 통계

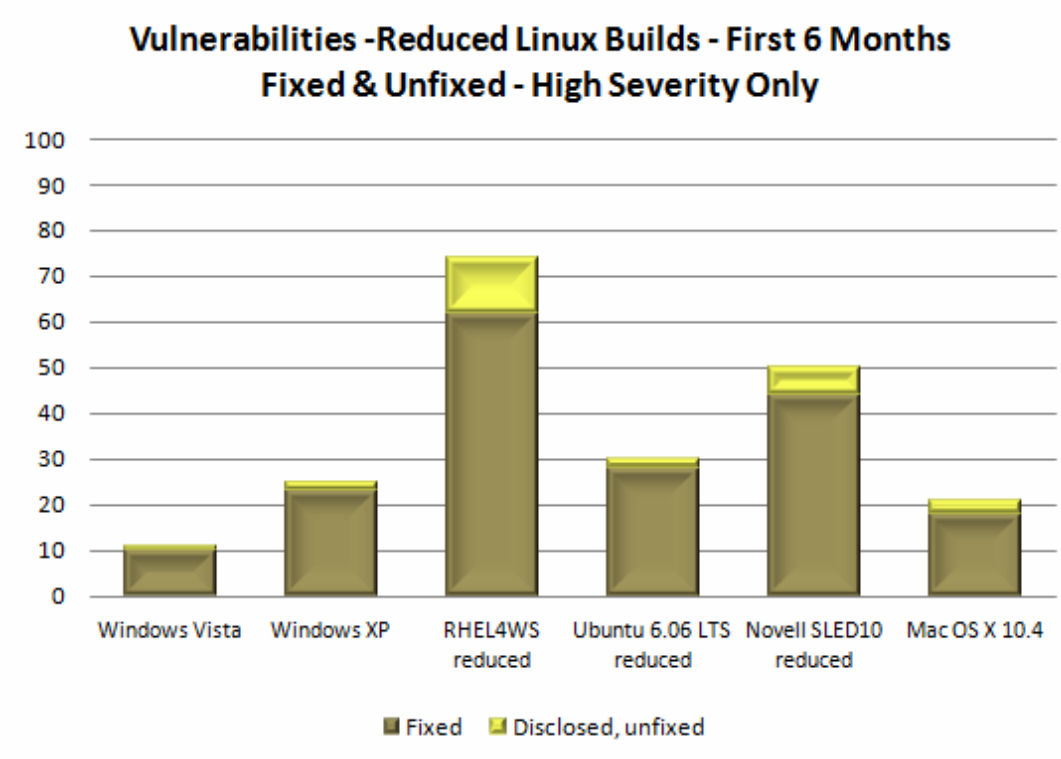
2007년 6월에는 마이크로소프트사에서 총 6개의 보안 업데이트를 발표하였으며, 긴급(Critical) 4개, 중요 1개, 보통 1개였다. 이 중에서 인터넷 익스플로러 공격에 사용될 수 있는(MS07-031, MS07-033)에 대한 패치가 포함되었으며, 윈도우 비스타의 Windows Mail에 관련 취약점 MS07-034 가 포함되어 있다.



[그림 1-12] 최근 1년 공격대상 기준 MS 보안 패치 현황

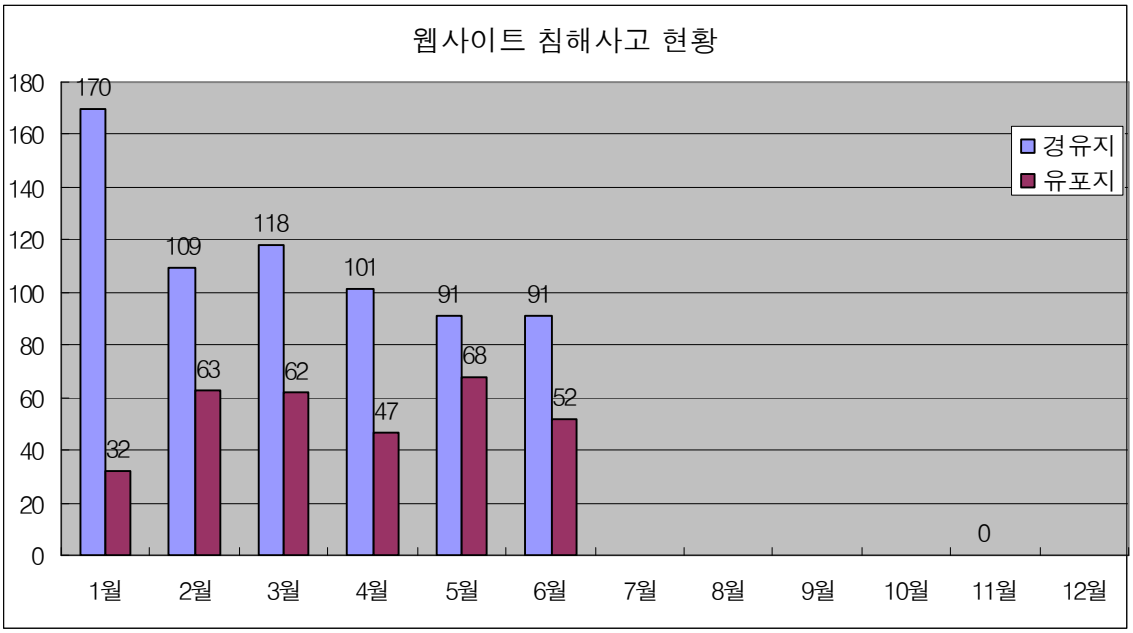
[그림 1-12]을 보면, 전반적으로 2007년에 들어와서, 오피스 및 IE 취약점이 증가 추세에 있는 것을 알 수 있다. 그러나 6월 달에는 Visio를 제외한 오피스 관련 취약점이 발표되지 않았다. Visio 관련 취약점(MS07-030) 은 중요 등급으로, 긴급에 해당하지 않으며, 엑셀, 워드, 파워포인트 등의 다른 오피스 프로그램 보다 사용률이 높지 않다.

csoonline.com에서 최근 6개월 동안 OS 들의 취약점 레포트를 조사한 것을 발표하였는데, 아래 [그림 1-13]을 보면, Windows XP SP2와 Windows Vista 의 취약점 발표 개수가 다른 OS 보다 상대적으로 많지 않음을 확인할 수 있다. 특히 Windows Vista 는 10개 미만의 숫자를 보여주고 있는데, 이는 Windows Vista 에 도입된 보안기능 들이 효과적으로 동작하는 것으로 볼 수 있다.



[그림 1-13] OS별 취약점 발견 건수[1]

2007년 6월 웹 침해사고 현황



[그림 1-14] 웹사이트 침해사고 현황

[1] 출처] http://blogs.csoonline.com/windows_vista_6_month_vulnerability_report

2007년 6월의 웹 침해사고 현황을 살펴보면 5월과 비교하여 큰 차이가 없다. 이는 MS07-017 취약점 발표 이후에 Internet Explorer과 관련하여 새롭게 발표된 위협적인 취약점이 없기 때문이다.

2007년 6월의 침해/악성 코드 유포 사이트의 수는 91/52이다. 2007년 5월과 비교하여 침해 사이트의 수는 변화가 없으며 유포사이트의 수가 16개 감소하였다. 악성코드 배포 유형을 살펴보면 MS07-017 취약점을 이용한 것이 전체의 48%로 가장 큰 비중을 차지 하고 있다. 이는 앞에서 언급한 바와 같이 MS07-017 취약점 발표 이후에 Internet Explorer과 관련하여 대중적으로 사용이 가능한 취약점이 없기 때문으로 분석되며, 새로운 취약점이 발표되기 전까지는 이러한 경향이 계속 유지 되거나 사용자 PC의 보안 패치 적용이 늘어나면서 악성 코드 유포수가 반비례하여 소폭으로 감소할 것으로 예측된다.

II. ASEC Monthly Trend & Issue

(1) 악성코드 – Win32/Alman.C 바이러스 국내 발견, 보고

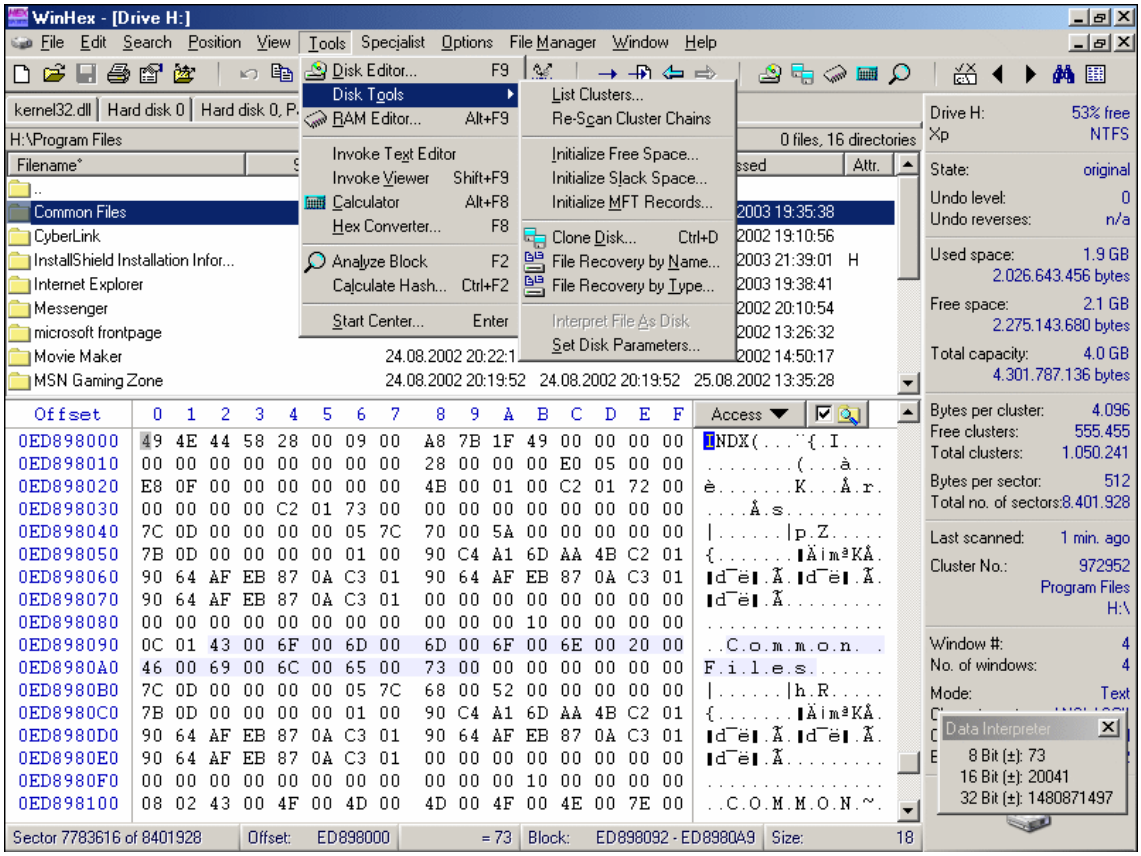
이번 달에는 공학용 계산기에서 동작하는 바이러스와 유명한 Hex 에디터의 스크립트로 만들어진 PoC (Poof of concept = 개념증명) 형태의 악성코드가 발견, 보고 되었다. 올해 들어서 자주 변형이 보고되는 MSN 메신저 웜(Win32/ShadoBot.worm)변형이 또 다시 출현 하였고, 올해 국내 발견된 바이러스 중 분석이 쉽지 않은 Win32/Alman.C 바이러스에 의한 고객 피해가 심각하게 발생하였다. 마지막으로 지난 보고서에서도 언급된 AutoRun.inf 를 생성하는 악성코드에 대해서 좀더 자세히 그리고 위험성을 정리하였다.

► TI89, WinHEX 와 관련된 개념증명 형태의 악성코드

TI89 는 공학도들에게 있어서는 없어서 안 될 아주 중요하고 유명한 계산기이다. 해당 계산기는 사용자가 프로그래밍을 하여 수식계산이나 간단한 게임 등도 제작하여 서로 공유하여 사용할 수 있도록 되어 있다. 이렇듯 Homebrew가 가능했기에 악성코드 제작도 충분히 가능한 환경으로 보인다. TI89용 악성코드는 바이러스로서 해당 계산기에 동작하는 응용 프로그램을 감염시킨다. 그리고 화면을 초기화하여 't89 GAARA' 라는 특정 메시지를 출력 한다.

[그림 2-1] TI89 계산기

WinHEX 는 유명한 Hex 에디터로 바이너리 에디팅이라는 기본 기능뿐만 아니라 포렌식에 사용 될 수 있어 분석툴로 더 잘 알려져 있다. 이 악성코드는 해당 응용 프로그램이 사용하는 스크립트로 제작 되었으며 감염활동도 해당 WinHEX 에서 사용되는 스크립트를 감염 시키도록 되어 있다.



[그림 2-2] WinHEX 실행화면 (출처 http://www.winhex.com/)

이 두 개의 PoC 악성코드는 개념증명이라는 용어에 맞게 일반 사용자가 감염 될 위험성은 낮다. 하지만 이처럼 어떤 환경이든 자유도 및 개방성이 있어 (SDK 제공 및 사용자 증가 그리고 불법적인 내부구조 해킹 등) Homebrew 활동이 증가하면 얼마든지 각종 기기에서 동작할 수 있는 악성코드도 충분히 나타날 수 있다. 대표적인 사례로 2년 전에 비디오 게임기 (PSP와 닌텐도 DS) 악성코드 사례가 있다.

► 메신저로 전파되는 – Win32/ShadoBot.worm 변형

메신저의 보안기능 강화(실행 가능한 확장자 전송불가), 안티 바이러스 제품에서의 빠른 대응 등의 복합적인 이유로 메신저 웜이 더 이상 위협적이 아니라는 것은 이제는 분명해졌다. 그러나, 이러한 상황에서도 악성코드의 전파에 메신저가 자주 사용되고 있다. Win32/ShadoBot.worm (이하 쉐도우 봇 웜) 이라고 알려진 이 악성코드의 변형은 자신을 ZIP 파일 형태로 보내며 메시지도 마치 사진파일이 들어 있는 것처럼 위장하여 메신저에 온라인 된 사용자에게 발송한다. 다음과 같다.

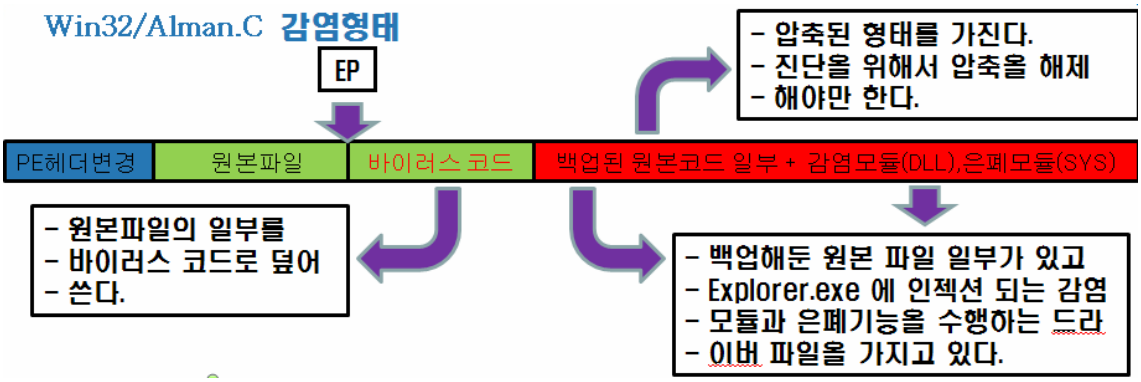
```
- Here are my very secret pictures for you.
- Here are my pictures from my vacation
- hmm is this you on the photo ?
- Check out my pics from my workplace.
- Nice new photos of me and my friends and stuff...
- ahh look this is my greatest picture made on vacation 2007, take a look
- Check out my nice photo album. :D
- hey regarde les tof de notre bande de fous. :p
- hey c'est toi dans ces tof!!???
- hey regarde les tof, c'est moi et mes copains entrain de.... :D
- j'ai fais pour toi cet album de photos tu dois le voire :p
- stp regarde cet album de photos je lai fais specialement pour toi et mes
amis...
- mes photos chaudes :D
- t'as pas encore vu ces tof???
- hey kijk eens naar mijn nieuwe foto album
- hey bekijk eens mijn nieuwe foto album
- hmm ben jij dit op de foto ?
- hey kijk ! dit is een lijst van mijn nieuwste fotos !!
- ahh kijk mijn mooiste foto album van vakantie 2007 bekijk ze eens :p
- kijk dit zijn fotos van mij werkplek! :)
- hmm ben jij dit op de foto ?
- 이하 생략
```

[표 2-1] Win32/ShadoBot.worm 이 보내는 메시지중 일부

해당 악성코드는 영어를 비롯한 여러 나라의 언어로 된 메시지를 내부에 포함하고 있고, 이러한 메시지는 사용자에게 호기심을 자극하고 첨부파일을 실행하도록 유도한다. 이 악성코드가 실행되면 DLL 파일 하나를 드롭하여 Explorer.exe에 인젝션 한 후 특정 IRC 서버로 접속을 시도한다. IRC를 이용한 원격제어의 기능이 주 목적이고 MSN 메신저를 이용한 것은 단지 자신을 전파 시키려는 하나의 수단에 불과하다.

► 분석이 난해 했던 - Win32/Alman.C 바이러스

올해 국내 발견 보고된 실행 파일을 감염시키는 바이러스 중 가장 난이도가 높은 것을 꼽으라면 Win32/Virut.C, D 형 그리고 Win32/Alman.C (이하 알만 씨형 바이러스)바이러스이다. 이들은 모두 분석을 지연시키기 위해서 복잡한 암호화 또는 시작실행시점 불명확화 기법을 사용했다. 특히 알만 씨형 바이러스는 바이러스 본체와 백업된 원본 파일을 일종의 데이터 압축 형태의 알고리즘을 이용하여 압축하여 해당 알고리즘을 분석하는데 많은 시간이 소요되었다.



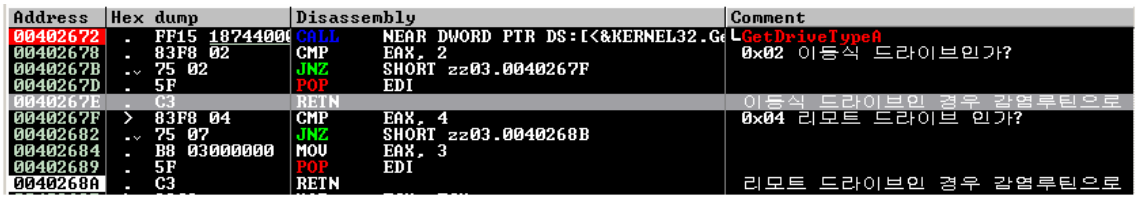
[그림 2-3] Win32/Alman.C 감염형태

또한 이 알만 변형 바이러스는 지난달 보고서에도 언급된 바와 같이 기존 안티 루트킷 프로그램을 우회하는 기법이 적용된 커널 드라이버를 가지고 있기도 하다. 그리고 국내 발견되는 악성코드에 유행처럼 사용되고 있는 AutoRun.inf 파일과 백도어를 이동식 저장 장치에 생성하는 증상 또한 포함하고 있다.

► AutoRun.inf 파일을 생성하는 악성코드의 위험성

지난 보고서에서 국내 발견되는 악성코드 중에 전파 목적으로 이동식 저장장치를 노리고 있다는 것을 언급했었다. 마치 도스시절 플로피 디스켓이 부트 바이러스의 목표가 되었던 것과 동일하다고 할 수 있다. 이번 달에는 Win32/Shlnom으로 명명된 간단한 형태의 전위형 바이러스의 코드 일부분을 분석하여 AutoRun.inf 파일이 어떤 방법으로 이동식 저장장치에 생성 및 실행 되는지 확인해 보기로 한다.

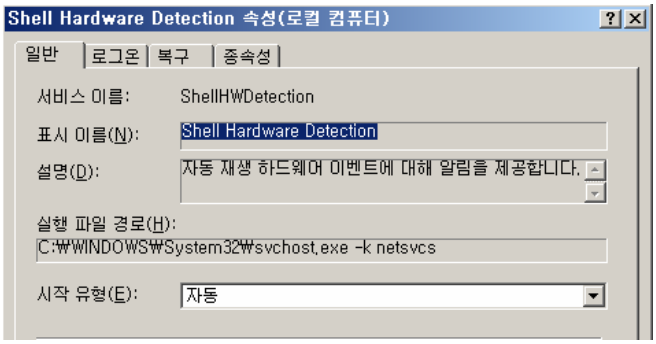
다음은 Win32/Shlnom 바이러스가 AutoRun.inf 를 생성할 대상을 선택하는 부분이다. PE 형태로 된 대부분의 악성코드가 아래와 같이 'GetDriveTypeA' API 를 호출하여 EAX 의 리턴 값을 확인하여 그 대상이 이동식 드라이브인지 그리고 리모트 드라이브인지 확인하여 AutoRun.inf 파일을 생성한다.



[그림 2-4] Win32/Shlnom 바이러스 코드 일부

AutoRun.inf가 각 드라이브 루트 폴더에 만들어지면 윈도우는 이 파일이 존재할 경우 자동으로 인식하여 AutoRun.inf에 지정된 파일을 자동실행하기 위해서 레지스트리에 기록해둔다. 즉, 다음과 같은 서비스에 의해서 이동식 저장장치의 루트 폴더에 있는 AutoRun.inf 가 읽혀

진다.



[그림 2-5] 윈도우 Shell Hardware Detection 서비스

읽혀진 내용은 OS 에 따라서 차이가 있지만 윈도우 XP 인 경우 다음 경로에 기록된다.

[HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩MountPoints2₩(일련의 클래스ID)₩shll₩AutoRun

이후 윈도우는 위 레지스트리에 기록된 정보를 참고하여 AutoRun.inf에 지정된 파일을 내 컴퓨터 -> 드라이브 진입 시 자동 실행 되도록 해둔다. 따라서 AutoRun.inf에 의한 자동실행을 차단 하기 위해서는 [그림 2-5]의 윈도우 서비스를 '중지'하면 된다. 하지만 이 방법은 해당 서비스가 자동 재생에 대한 이벤트 알림이 외에 다른 기능이 있는지 파악되지 않기 때문에 권장하지는 않는다

► ARP Spoofing 공격은 새로운 중국 발 해킹

ARP Spoofing 공격을 이용하여 악성코드를 설치하는 형태는 올해 3월 처음 알려졌다. 악성코드는 Dropper 형태로 되어 있었고 중국의 일련의 해커로부터 만들어진 자동화 공격도구와 패킷 스니핑 모듈과 드라이버 등으로 이루어진 형태로 Dropper/MulDrop이라고 명명되었다. 물론 이는 ARP Spoofing 공격 툴이 포함된 악성코드를 일반적으로 지칭하는 것은 아니며, 다수의 파일을 Drop 한 형태의 악성코드 일컫는 일반적인 진단명 이다.

작년 말부터 WinPCap 기반의 패킷 캡쳐 라이브러리를 가지고 있는 악성코드를 종종 발견되었으나, 이 파일들은 모두 정상적인 파일이므로 일반적인 패킷 캡쳐 프로그램에서도 사용 될 수 있어 악성코드로 간주하여 엔진에 추가 할 수도 없었다. 또한 이 파일을 Drop 하는 Dropper 는 접수가 되지 않아서 해당의 용도를 정확히 알지 못할 때도 있었다.

6월에 악성코드의 감염이 매우 심각한 고객으로부터 상당수의 악성 코드 샘플을 접수받아 분석하는 과정 중에 Win-Trojan/MulDrop이라는 악성코드에서 패킷 캡쳐 라이브러리와

ARP Spoofing을 하는 툴이 발견되었다. ARP Spoofing 공격이 새로운 중국 발 해킹의 형태라는 것은 인지하고 있었지만, 실제로 기업 사용자에게 심각한 피해를 입히는 형태로 발전된 것을 알게 되었다. 참고로 이번 달 테크니컬 컬럼에서 ARP Spoofing 공격에 대해서 깊게 다루기로 하겠다.

ARP Spoofing 공격은 기존의 중국 발 웹 해킹과 다르게 사용자가 해킹 당 한 사이트를 방문 하지 않아도 악성코드를 설치하게 할 수 있다. 보통은 클래스가 동일한 서브넷에 Win-Trojan/MulDrop를 실행 후 ARP Spoofng 공격툴의 약간의 세팅 만으로 악성코드를 감염시킬 수 있다. 기업들이 대부분 웹 기반의 그룹웨어를 사용하므로 해당 클라이언트에서 해당 그룹웨어 서버로 연결 시 ARP Spoofing 툴을 이용하여 80/TCP HTTP 패킷에 iframe 태그를 삽입 해둔다. 해당 iframe에 명시된 호스트는 인터넷 익스플로러 취약점이 존재하는 외부 HTTP 호스트 URL 이다. 따라서 자신은 정상적으로 웹 서버 메인 페이지 접속했지만 실제 패킷을 덤프 해보면 메인 페이지 이외에 iframe 태그가 삽입 되어 있음을 알 수가 있다. 이러한 공격 방법은 굳이 웹 서버를 해킹하지 않아도 더 많은 사용자들을 위험에 노출 시킬 수 있어 주의가 필요하다. 따라서 다시금 인터넷 익스플로러뿐만 아니라 윈도우에 대한 보안 패치 적용이 중요성을 더 한다고 하겠다.

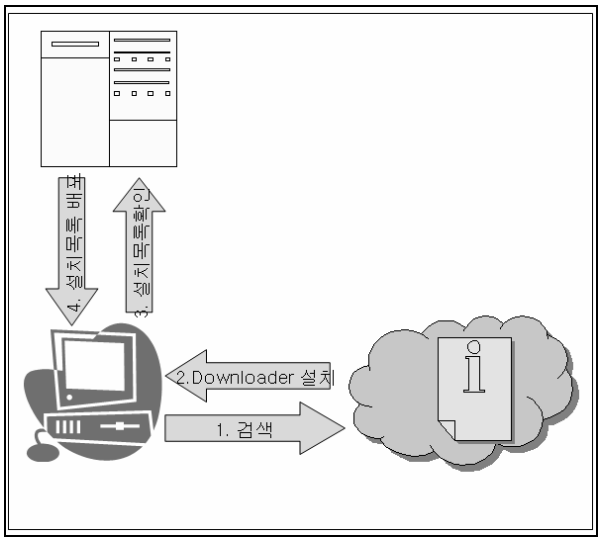
(2) 스파이웨어 - 스파이웨어의 새로운 시도

배포 방식의 변화

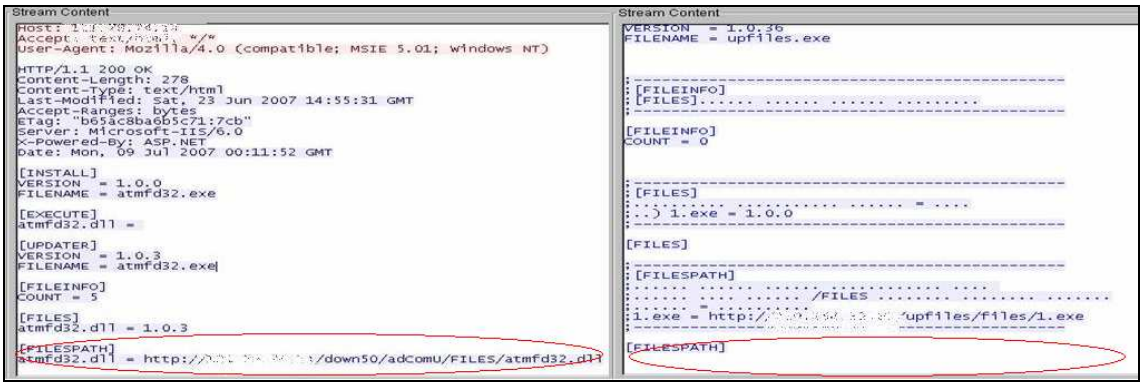
금전적 이득을 노리는 스파이웨어와 보안 업체간의 숨바꼭질은 끝이 없는 것으로 보인다. 스파이웨어 제작자는 자신이 배포하는 파일이 보안업체의 분석이 완료되어 진단이 시작되기 전에 최대한으로 전파되어 최고의 수익을 얻고자 한다. 이들은 효과적인 스파이웨어 배포를 위해 대형 포털 사이트의 검색 순위에 상위 랭크된 단어나 사회적인 이슈를 일으키는 검색어를 이용해 끊임없는 낚시 글을 등록하고, 이를 보고 클릭한 사용자들을 대상으로 원하는 컨텐츠를 보기 위하여 특정 ActiveX를 설치하여야 한다는 방법으로 스파이웨어 설치를 유도하는 방법으로 배포하고 있다.

최근에 발견된 다운로더 까만(Win-Downloader/Ggamans.21552)은 기존의 배포방식과는 달리 서버에서 필요한 목록을 다운로드하고 사용자 PC에 다운로드된 목록에 포함된 스파이웨어를 능동적으로 다운로드하여 설치하는 형태로 스파이웨어를 유포하는 것이 발견되었다.기존에 접수된 다운로더류의 경우 설치하는 파일에 대한 정보가 파일 내에 하드코딩 되어 항상 동일한 스파이웨어와 그 변형만을 설치하는 업데이터의 성격이 강했다. 그러나, 2007년 초부터 꾸준히 보고가 되고 있는 다운로더 까만과 같은 새로운 형태의 다운로더는 웹에서 설치 목록과 다운로드 경로 모두를 전달받아 사용자의 시스템에 다수의 스파이웨어를 설치한다.

새로운 형태로 스파이웨어를 유포하는 다운로더 까만의 경우 다운로더 까만 자체는 기존 스파이웨어의 배포방법과 동일하게 낚시 글을 이용하거나, P2P프로그램의 번들 형식으로 사용자 동의 없이 설치 된다. 일반적인 다운로더의 경우 시스템에 설치가 되면 즉시 툴바나 허위 안티-스파이웨어와 같은 스파이웨어의 설치를 유도하는 등의 동작을 시작한다. 이를 통하여 사용자는, 설치된 스파이웨어를 제거하는 것이 쉽지 않을 수도 있으나, 설치 사실을 즉시 인지할 수 있기 때문에 동일한 방법을 통해 재배포 하는 것은 쉽지 않다. 그러나, 다운로더 까만의 경우 설치후 다운로드 목록을 바로 서버에서 받아와서 목록에 등록된 스파이웨어 설치를 시작하지 않는다면 증상이 전혀 없기 때문에 사용자가 스파이웨어 설치 사실을 인지하기 어렵다. 따라서 스파이웨어 배포자는 충분한 기간 동안 다운로더 까만과 같은 류의 스파이웨어를 배포하며, 스파이웨어 설치를 유도하기 위한 낚시 글 배포와 같은 더 이상의 노력없이 효과적이고 신속하게 다수의 스파이웨어/애드웨어를 배포함으로써 수익의 극대화를 추구할 수 있다. 단순하게 다운로더 까만류에 의하여 설치된 스파이웨어/애드웨어를 제거한다고 하더라도 본체가 제거되지 않기 때문에, 서버에 새로운 다운로드 목록이 등록되면 새로운 스파이웨어/애드웨어가 사용자 동의 없이 설치될 수 있다.



[그림 2-6] 새로운 스파이웨어 배포 방법



[그림 2-7] 좌)다운로드 목록이 존재하는 경우 우)다운로드 목록이 없는 경우

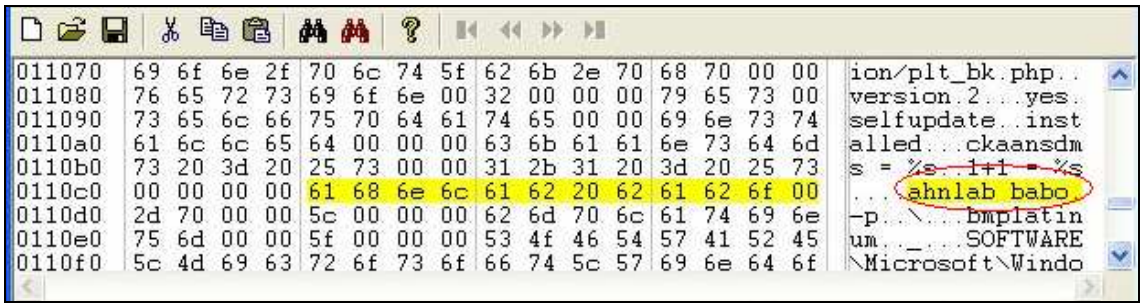
다운로더 까만와 같은 형식의 다운로더는 2006년 최초 확인된 이후 계속해서 발견되어오고 있으며 2007년 6월에는 11건의 변형이 보고되었다. 이 모든 다운로더들은 웹에서 설치목록에 대한 정보를 메모리상에서 읽는 방법을 선택하고 있으며 이 것은 웹에서 흔히 구할 수 있는 오픈소스를 이용한 것이다.

[그림 2-7]에서 좌측 그림은 다운로드 목록이 있는 경우로 주소표시줄 검색 결과를 변경하는 스파이웨어를 설치하게 되며, 우측과 같이 [FILEPATH]에 값이 없는 경우는 아무런 동작을 하지 않는다.

스파이웨어 제작 Vs 스파이웨어 분석

스파이웨어임을 알면서 프로그램을 제작한 경우라도 애써 제작한 프로그램이 스파이웨어로 분류되는 경우 개발자들은 기분이 좋지 않을 것이다. 최근 배포되는 스파이웨어 배포 업체

중 1곳은 ‘Ahnlab. Babo’라는 문구를 프로그램에 삽입하여 자신들이 제작한 프로그램을 분석하는 이들에게 불편한 심기를 그대로 드러내고 있다. 외국에서 제작한 악성코드의 경우 내부에 특정 AV업체를 비방하는 문구를 삽입해 자신의 메시지를 전달하는 사례가 종종 있으나, 국내의 경우는 흔치 않다. 이렇게 내부에 특정 백신 업체를 비방하는 문구를 프로그램 내에 삽입하는 것은 자신을 진단하는 것에 대한 의사 표현일 수 있으나, 스스로가 제작한 프로그램이 스파이웨어라고 인정하는 것으로 해석할 수도 있다.



[그림 2-8] 스파이웨어 내부 Text 정보

(3) 시큐리티 - 공격자를 위한 종합 선물 세트 MPACK

2007년 6월에 발표된 마이크로소프트사 보안 업데이트는 총 6건으로 각각 긴급 4건, 중요 1건, 보통 1건의 보안수준을 갖는다. 과거, 해당 취약점에 대한 공격시도가 보안 업데이트 발표 시점을 시작으로 활발히 증가하였던 것과는 다르게, 최근에는 별 다른 이슈 없이 지나가고 있다. 그러나, 과거의 취약점을 종합적으로 활용하는 공격 툴이 등장하는 것을 보면, 시스템 보안 패치를 간과하는 사용자들은 언제든지 피해를 입을 수 있다는 것을 인지하여야 한다.
다음은 2007년 6월에 발표된 취약점 중에서 악의적인 공격에 이용될 수 있는 주요 취약점들에 대한 목록이다.

위험등급	취약점	PoC
긴급	Windows Schannel 보안 패키지의 취약점으로 인한 원격 코드 실행 문제점(MS07-031)	무
긴급	Microsoft Speech API 4.0 ActiveX Controls 버퍼 오버플로우 (MS07-033)	유
긴급	Outlook Express 및 Windows Mail 누적 보안 업데이트(MS07-034)	유
긴급	Microsoft Win32 API 취약점으로 인한 원격 코드 실행 문제점 (MS07-035)	유

기존의 다수를 차지하던 Office 관련 취약점과 Internet Explorer 취약점뿐만 아니라 6월에는 다양한 서비스와 애플리케이션을 대상으로 하는 취약점이 포함되어 있다. 그러나, 공격에 이용되는 취약점은 특정 운영체제나 서비스에서 벗어나 가장 대중적이고 쉽게 취약점을 찾아 공격할 수 있는 Internet Explorer 및 오피스에 집중되고 있다.

6월의 동향으로 Internet Explorer를 통해 공격 가능한 일부 취약점들(MS Speech API 4.0 ActiveX Controls 버퍼오버플로우(MS07-033) 문제점, MS Win32 API 취약점(MS07-035)과 최근 이슈가 되고 있는 MPack툴에 대해서 살펴보도록 하자.

변함없이 등장하는 다수의 IE 도용 취약점들

이 달에 발표된 MS Speech API 4.0 ActiveX 컨트롤 취약점은 IE가 MS Speech 관련 ActiveX 개체를 처리하는 과정에서 발생하는 스택 기반의 버퍼 오버플로우 취약점이다. MS Speech는 음성으로 시스템을 운영할 수 있도록 MS에서 제공하는 기능으로, Windows 2000 시스템에는 디폴트로 설치되어 있다. 이를 악용하는 Exploit은 기존과 동일한 방식으로 해당 ActiveX 컨트롤을 로드하여 취약한 Method를 호출하고, 자바스크립트를 통해 적절한 쉘 코드를 배치하는 방식으로 구성되어 있다.

ActiveX Load	<object id=xlisten classid="clsid:4E3D9D1F-0C63-11D1-8BFB-0060081841DE"></object>
	...
Shellcode	nop1 = unescape("%01%6E%40%6E%40%6E%40%6E%40%6E%40%6E%40%6E%40%6E%40")
	c1 = unescape("%6E") : REM add byte ptr esi, ch (as nop)
	...
Function Call	xlisten.find(strLong);

취약한 ActiveX 컨트롤은 아래 두 가지이며, 본 문서에서는 Xlisten.dll 에 초점을 맞춘다.

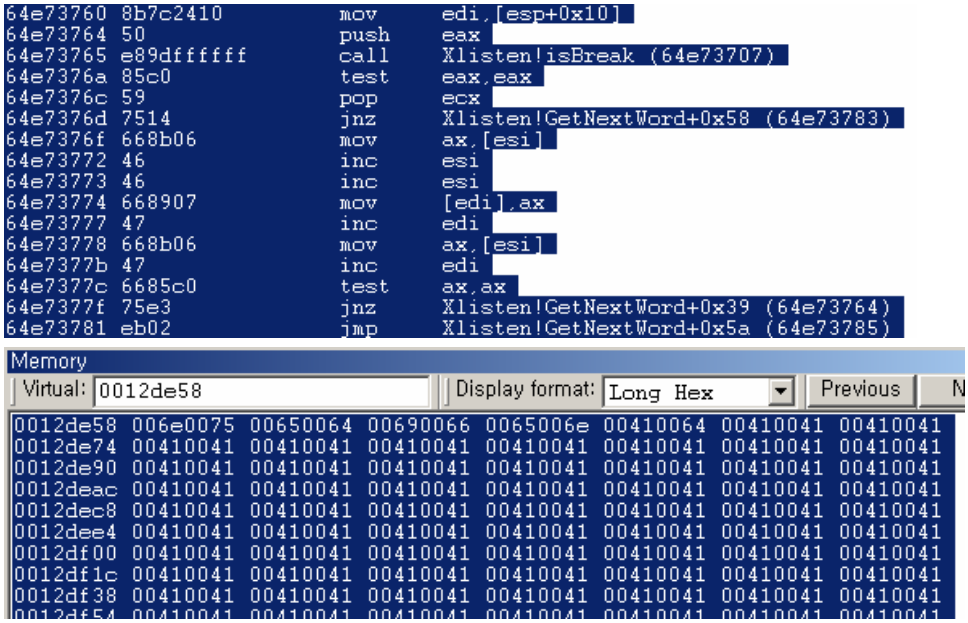
ProgID	DirectSR.DirectSR	DirectSS.DirectSS
CLSID	4E3D9D1F-0C63-11D1-8BFB-0060081841DE	EEE78591-FE22-11D0-8BEF-0060081841DE
DLL	Xlisten.dll	Xvoice.dll

Xlisten.dll, Xvoice.dll을 통해 오브젝트가 처리되는 과정을 살펴보면, FindEngine(), Find() 메쏘드에 넘겨지는 파라미터에 대한 적절한 유효성 체크 코드가 존재하지 않는다. Find() 메쏘드는 로컬 데이터를 위해 0x278 크기의 스택 공간을 확보한 후 실제 문제의 데이터를 복사하는 GetNextWord() 함수를 호출한다.

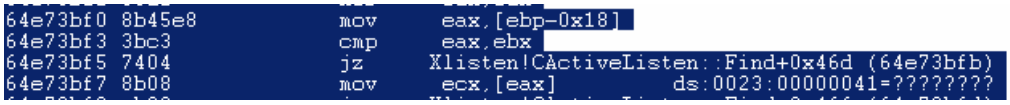
```
Xlisten!CActiveListen::Find:
64e7378e 55              push    ebp
64e7378f 8bec            mov     ebp,esp
64e73791 81ec78020000    sub     esp,0x278
64e73797 53              push    ebx
64e73798 56              push    esi
64e73799 8d8588fdffff    lea     eax,[ebp-0x278]

64e737df 895db0          mov     [ebp-0x50],ebx
64e737e2 895da4          mov     [ebp-0x5c],ebx
64e737e5 bfe8030000      mov     edi,0x3e8
64e737ea e83cffffff      call    Xlisten!GetNextWord (64e
```

GetNextWord() 함수는 입력된 파라미터의 문자열을 2바이트씩 스택의 [ebp-0x278] 지점으로부터 복사한다. 이 과정에서 입력에 대한 어떠한 검증 코드도 수행하지 않기 때문에 입력으로 넘겨진 긴 문자열은 정해진 스택의 크기를 넘어서 다른 메모리 공간을 침범(Overwrite)하게 된다.



이렇게 Overwrite된 지점이 후에 다른 코드에 의해 참조되는 과정에서 오류를 발생하게 된다. 이 때, 입력되는 문자열의 크기를 조절하여 Call 코드의 참조 지점에 매핑시키고, 쉘코드로 점프하도록 처리함으로써 단순 크래쉬(Crash)뿐만 아니라 공격자가 원하는 코드를 실행할 수 있다.



또 다른 취약점 MS Win32 API 취약점은 IE가 Resource scheme (res://)를 사용하여 로컬 시스템에 존재하는 DLL 파일을 참조하는 과정에서 발생하는 Integer Overflow 메모리 참조 오류이다. 보통 Resource scheme의 사용은 다음과 같은 형태로 이루어진다.

```
res://sFile[1][/sType]/sID[2]  (EX) res://kernel32.dll/#xxx
```

그러나, 이를 처리하는 FindResourceW() 함수가 적절한 파라미터 검사를 수행하지 않기 때문에, 65535 (0xFFFF) 이상의 sType, sID 값이 입력되는 경우, 잘못된 메모리 참조로 인하여 오류가 발생한다. 해당 취약점 또한 적절히 입력을 조정하고 쉘코드 삽입하여 임의의 코드를 실행할 수 있다.

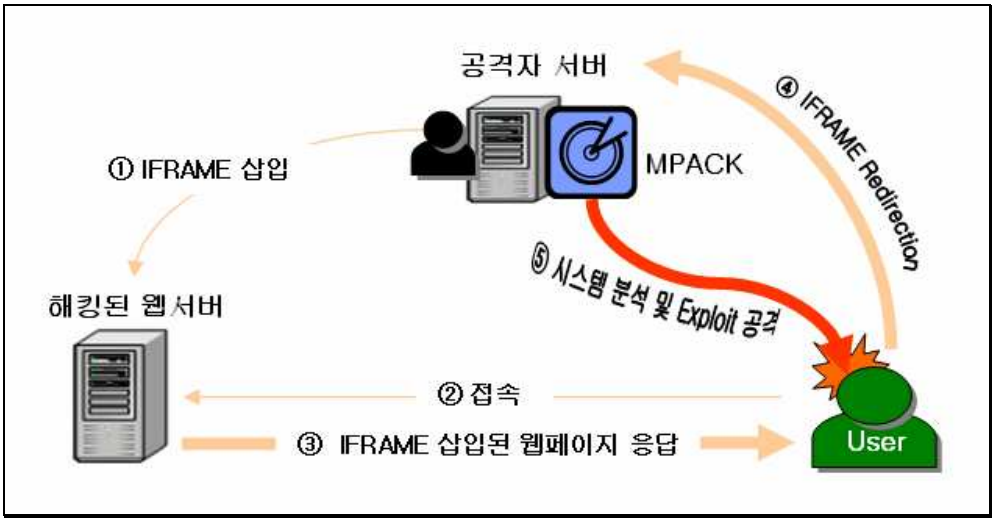
Internet Explorer는 가장 대중적인 애플리케이션이며, 이같이 수많은 취약점들을 내포하고 있기 때문에 언제든지 공격의 매체로써 손쉽게 악용될 수 있다. 따라서, 꾸준한 패치 업데이트만이 사용자의 시스템을 위협으로부터 방어하는 최선의 방법이다.

[1] resource를 내장하고 있는 모듈의 경로 및 이름
[2] resource 구분자 또는 구분 문자열

공격자를 위한 종합 선물 세트 MPACK

지난 6월 중순. 많은 보안 전문가들의 관심이 이탈리아에 쏠리기 시작했다. 10,000대 이상의 이탈리아 웹 서버가 해킹되었고, 그 위협이 점점 전 유럽으로 퍼져나가고 있다는 소식이 전해졌기 때문이다. 일명, 'Italian Job' 이라고 불리는 이 공격 뒤에는 다양한 공격 Exploit을 내포하고 있어 전문가들 사이에서 '종합선물세트', '맥가이버칼' 이라 평을 받는 MPACK툴이 있었다.

MPACK은 다음과 같은 공격 시나리오를 통해 사용자를 공격한다.



[그림 2-9] Mpack을 이용한 공격 시나리오

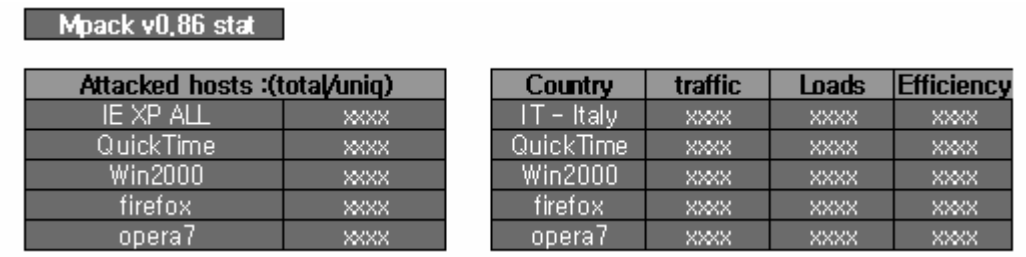
1. 웹 서버를 해킹한 후 공격자의 웹 서버 주소가 포함된 <iframe> 태그를 삽입한다.
2. 사용자가 해킹된 웹 서버에 접속한다.
3. <iframe> 태그가 삽입된 웹 페이지가 사용자의 브라우저를 통해 로딩된다.
4. 공격자 서버(MPACK이 설치된)로 redirection 된다.
5. 공격자 서버에 설치된 MPACK이 사용자 시스템을 분석한다.
6. 분석된 시스템 정보를 기반으로 알맞은 Exploit 공격을 찾아 사용자 시스템을 공격한다.

MPACK은 PHP로 구성되어 있으며, MySQL 서버가 설치된 웹 서버에서 운영된다. Redirection에 의해 사용자가 처음으로 접속하게 되는 MPACK의 메인 페이지 'index.php'는 다음과 같은 절차를 통해 사용자 시스템을 공격한다. 우선 'index.php' 파일에 존재하는 detect_browser(), GetCountryInfo() 등의 함수가 접속한 사용자의 시스템 정보들을 분석한다.

분석 정보	분석 대상	내용

	(HTTP_HEADER)	
웹 브라우저	User-Agent	opera, conqueror, lynx, msie, links, netscape 구별
OS	User-Agent	Linux, Windows, Macintosh, FreeBSD 구별
국가	IP	GeoIP.dat 데이터 활용

분석된 정보는 MySQL 서버에 저장되고, 이 데이터를 기반으로 국가별, 브라우저별, 운영체제별 형태로 조회도 가능하다.



다양한 Exploit은 각각의 PHP 파일로 되어 있고, 분석된 웹 브라우저와 OS 정보를 기반으로 해당하는 Exploit PHP 파일들을 "index.php" 파일에 include 한다.

* **mdac4.php** : MS06-014 Microsoft Windows MDAC 취약점
* **ms06-044_w2k.php** :
  - MS06-014 Microsoft Windows MDAC 취약점
  - MS06-044 Microsoft 관리 콘솔 취약점
* **ani2.php, anifile.php** : MS07-017 - Windows 애니메이션 커서 취약점
* **ff.php,o7.php** : MS06-006 타사 인터넷 브라우저용 Windows Media Player 플러그인 취약점
* **qt.php** : QuickTime 힙 기반(Heap-based) 오버플로우 취약점
* **xml.php** : MS06-071 Microsoft XML Core Services 취약점
* **megapack1.php** :
  - **startWVF**() : MS06-057 Windows Explorer WebViewFolderIcon ActiveX 취약점
  - **startWinZip**() : WinZip CreateNewFolderFromName ActiveX 오버플로우 취약점

MPACK은 자체 Encrypt 모듈인 cryptor.php, crypt.php 파일을 사용하여 index.php 파일을 통해 로딩되는 취약점 Exploit 코드를 복잡한 문자열로 인코딩한다.

<Encoding된 index.php 파일 소스>

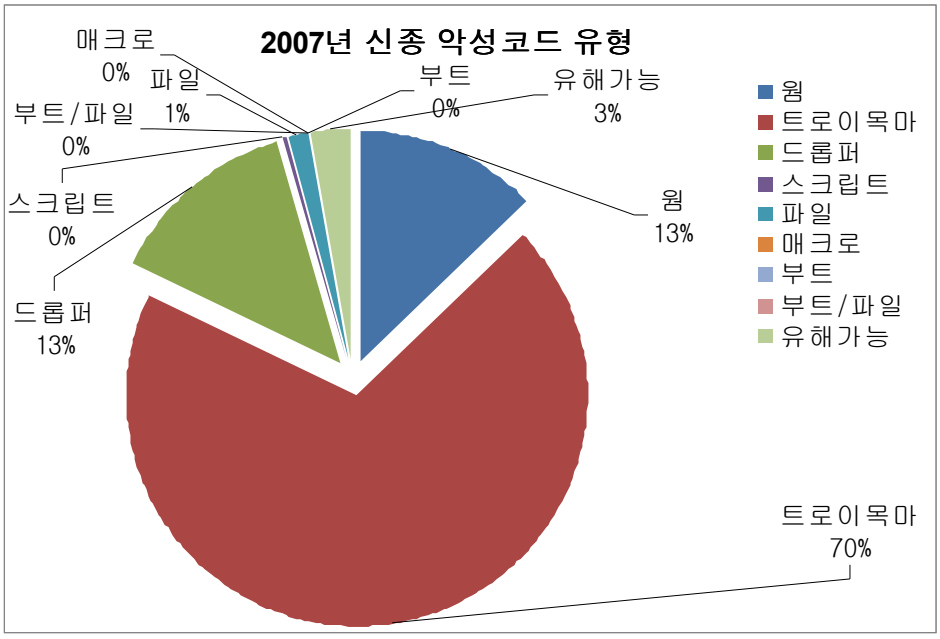
위의 분석은 MPACK v0.86 버전을 기준으로 이루어졌기 때문에, 그 이후 최신버전에는 보다 많은 Exploit 파일이 존재할 수 있다. MPACK을 분석하는 과정에서 필자는 내장된 Exploit PHP 파일이 공개된 Exploit 코드와 거의 동일하다는 점과 마치 플러그인 방식처럼 필요한 취약점 코드를 자유롭게 PHP 파일 형태로만 끼워 넣어 사용할 수 있다는 점에 주목하였다. 이는 일반적인 스크립트 키드 수준의 사용자들도 얼마든지 새로운 공개 Exploit 코드를 사용하여 또 다른 버전의 MPACK을 제작할 수 있는 가능성을 암시하기 때문이다.

MPACK이 사용하는 Exploit 코드들은 대부분 이미 패치가 릴리즈된 취약점들이였다. 항상 강조해도 지나치지 않는 보안 업데이트만 충실히 수행하였다면 'Italian Job'과 같은 대형 사고는 발생하지 않았을 것이다.

III. 2007년 상반기 동향

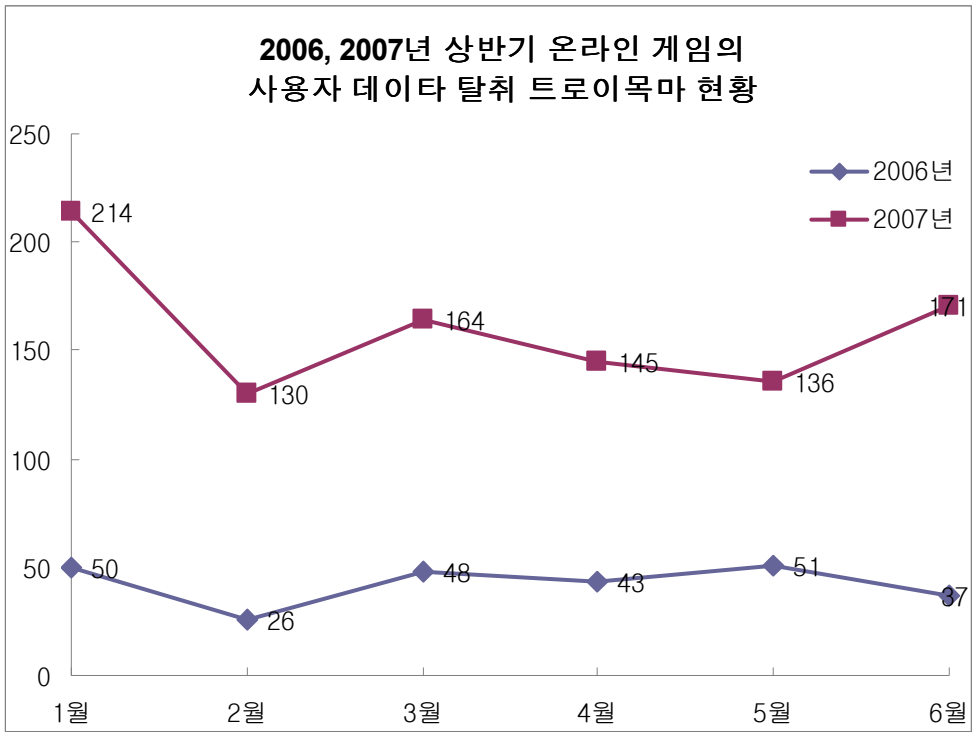
(1) 2007년 상반기 악성코드 동향

올 상반기는 악성코드의 국지적인 발생과 피해 그리고 그 비율이 뚜렷했다. 물론 이러한 현상은 오래 전부터 시작 되었고 우리나라를 비롯한 아시아 지역(주로 중국, 대만, 일본)은 올해 들어 다른 나라와 더욱 뚜렷하게 구분 되고 있다. 악성코드가 노리는 대상 역시 클라이언트 시스템이며 우리나라를 비롯한 아시아 지역에서 발생하는 악성코드가 노리는 것은 개인정보이다. 여기서 말하는 구체적인 개인정보는 여러 가지로서 서버 시스템을 공격한 경우라면 어떠한 DB 형태로 저장된 개인정보 일 것 이며 클라이언트를 공격 했다면 익히 알고 있는 온라인 게임의 사용자 정보(데이터)를 훔쳐내는 형태 일 것 이다.



[그림 3-1] 2007년 국내발견 신종 및 변형 악성코드 유형

[그림 3-1]에서와 같이 올 상반기 악성코드 유형 중 트로이목마는 전체의 70%를 차지 할 정도로 비율이 높다.



[그림 3-2] 2006, 2007 상반기 온라인 게임 트로이목마 현황

[그림 3-2]에서와 같이 2007년 상반기는 전년도 동기대비 무려 276%나 증가 하였다. 아울러 올해 들어 다른 특징이라면 작년은 국내 온라인 게임을 타켓으로 정보를 훔쳐냈다면 올해 들어 중국 및 대만의 온라인 게임이 직접 타켓이 되고 있다는 것이다.

국내 유명 온라인 게임 업체들은 보안에 매우 신경을 쓰고 있고, 이에 따라서 다양한 보안 로그인 방법 및 보안을 강화하고 있어 특정 온라인 게임을 대상으로 하는 악성코드의 수가 차츰 줄고 있는 것으로 보인다. 그리고 중국 그리고 대만 등 자국내 온라인 게임의 자체 개발 및 상용화가 되므로 제작자들은 보안 솔루션이 갖춰진 국내 온라인 게임에서 조금씩 멀어 진 것으로 보인다.

이 역시 국내 온라인 게임을 노리는 악성코드가 한 순간 없어졌다라는 것은 아니고 작년 후반기 상황과 비교하면 약간씩 감소추세에 놓여 있다고 하겠다. 분명히 할 것은 이것은 특정 국내 온라인 게임만을 대상으로 하는 악성코드에 대하여 이러한 현상이 나타나고 있다는 것으로 국내 온라인 게임의 전부를 대상으로 하는 것은 아니다. 그러나 국내에서 타국의 온라인 게임을 훔쳐내는 악성코드의 수가 증가하는지 원인에 대해서 명확하지 않다. 아마도 이것은 국내 취약한 시스템을 악성코드 유포의 중간 숙주로 사용하고 있는 것으로 추정될 뿐이다.

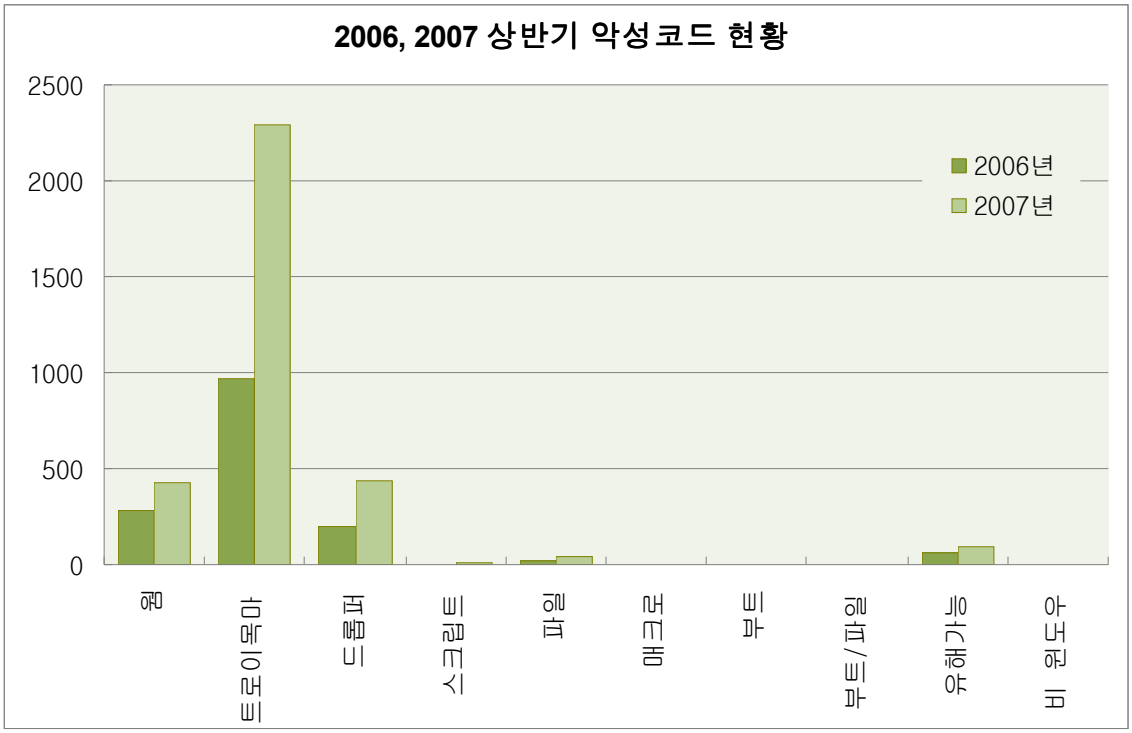
반면 Win32/Zhelatin.worm 그리고 Win32/Stration.worm 과 같은 악성코드들은 주로 위에

서 언급되지 않는 지역에서 주로 발생하여 피해를 입혔다. 물론 이 악성코드의 피해가 우리나라를 비롯한 아시아 지역에 전혀 없다는 것은 아니지만, 해당 악성코드들은 수 많은 변종이 올 상반기에 보고되었다. 이들 악성코드는 사용자들의 호기심을 자극할 만 한 국제적인 이슈 등을 제목 또는 내용으로 사용하여 메일로 전파 되었다. 국내를 비롯한 아시아 지역은 단지 그 수가 상대적으로 적다고 추정 하고 있다.

해당 악성코드들 역시 주 감염 대상은 클라이언트 시스템이다. 이들의 주요 증상은 주로 자신의 복사본 또는 다운로더 형태를 이 메일에 첨부하여 확산하거나, 스팸 메일 발송에 사용된다. 특히 Win32/Zhelatin.worm은 사용자들 및 일부 보안 프로그램을 우회 하도록 설계되어 감염되어도 이를 인지하거나 발견할 수 없다. 또한 변형을 진단하지 못하도록 프로세스 및 파일을 은폐하는 스텔스 기법과 일부 안티 바이러스의 에뮬레이터를 우회 하도록 설계되어 안티 바이러스의 진단 기법을 회피하기도 한다. 이들은 복잡한 다형성 코드와 커스텀 형태의 실행 압축을 사용한 유형이 많았으며, 악성코드 내에 불필요한 쓰레기 코드를 삽입한 형태가 많이 발견 되고 있는데, 이를 Win-Trojan/Obfuscated이라고 명명하고 있다. 즉, 이들 지역에서 발견 된 악성코드는 감염 시스템을 스팸 프록시나 백도어 등으로 사용하면서 상당히 지능적으로 안티 바이러스 및 보안 프로그램을 우회하는 자기 방어적 기능에 초점이 맞춰져 있다.

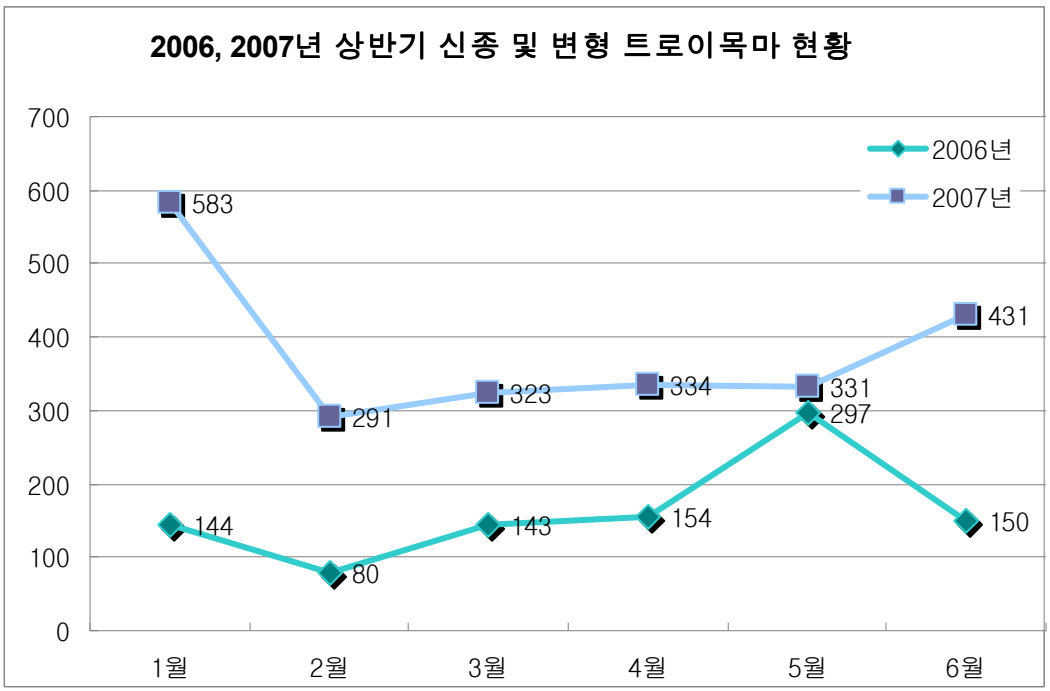
국내에서 발견 되는 악성의 특징을 본다면 위에서 언급 했듯이 개인 사용자 정보를 훔쳐내는 악성코드의 양상이 뚜렷하다. 그러나 올해 나타난 현상으로 개인 정보를 훔쳐낼 대상의 온라인 게임의 종류가 많아졌고, 또한 국내 보다는 이러한 악성코드를 만들어 내고 있는 중국 내 온라인 게임을 대상으로 데이터를 훔쳐내는 형태가 많아졌다는 것이다.

다음은 작년 동기와 비교한 상반기 신종 및 변형 악성코드 현황이다.



[그림 3-3] 2006, 2007 상반기 악성코드 현황

작년 동기 대비 악성코드는 116% 증가 하였다. 가장 많이 증가한 악성코드는 단연 트로이목마로 작년 동기 대비 137% 증가 하였다.



[그림 3-4] 2006, 2007 상반기 신종 및 변형 트로이목마 현황

최근 4개월간 트로이목마 유형은 별다른 증가 추세를 보이고 있지 않다가 6월에 전월 대비 30% 가량 증가하고 있다.

올해는 중국 발 해킹과 악성코드 전파의 패러다임에 있어 앞의 6월 악성코드 트렌드 및 이슈에서 언급한 바와 같이 ARP Spoofing을 이용하여 악성코드를 전파할 수 있는 방법이 사용되기 시작하였다.

또 하나 상반기 악성코드의 주요 패러다임의 변화는 이동식 저장장치를 노리는 악성코드이다. ASEC 리포트 보고서를 통해서도 작년에 Win32/Viking과 Win32/DellBoy 등의 실행 파일 감염 바이러스로 인한 로컬 네트워크 침투 사례를 언급한 바 있다. 즉, 바이러스의 부활과 기승으로 인하여 로컬 네트워크의 자원을 손쉽게 감염시킬 수 있다는 것이다. 이제는 작은 USB 메모리 스틱이나 윈도우가 인식하는 모든 이동식 저장장치가 악성코드 감염 대상이 되었고, 이들이 감염되지 않은 다른 시스템을 감염 시킬 수 있게 되었다. 마치 도스시절에 플로피 디스켓에 부트 바이러스가 감염되었던 사례와 비슷하다고 하겠다.

굳이 웜이 아니더라도 요즘 중국산 악성코드 대부분은 자신의 복사본을 이동식 저장 디스크 또는 네트워크 드라이브에 만든다. 그리고 이것이 사용자 개입없이 자동으로 실행되도록 하기 위해서 AutoRun.inf 파일을 만든다. 이 파일은 윈도우에서 자동으로 인식되어 사용자가 특정 드라이브를 클릭하는 순간 AutoRun.inf 파일에 지정된 실행파일이 자동 실행되는 것이다. 이것은 작년 상반기에는 없었던 유형이며 단순해 보이는 이 방법은 효과적으로 자신을 이동식 저장 매체에 증식하며 사용자를 괴롭히고 있다.

다음으로 올해 발견 된 PoC (Poof of concept = 개념증명)형태의 악성코드로 크게 3가지 유형이 있었다. 하나는 잘 알려진 MP3 플레이어를 대상으로 한 악성코드 감염 시도였다. 이것은 윈도우 이외의 OS에서만 실행 될 수 있었고 사용자가 개입 되어야만 했다. 다음에 알려진 것은 유명한 공학용 계산기에서 동작 되는 악성코드로 이 계산기는 유저가 만든 게임이나 응용 프로그램을 구동 시킬 수 있었고 따라서 악의적인 코드도 제작이 가능 했을 것으로 추정된다. 끝으로는 분석가나 응용 프로그램 개발자들이 잘 이용하는 HEX 편집기에 대한 악성코드이다. 이 악성코드는 해당 편집기가 사용하는 스크립트로 만들어졌으며, 이 편집기는 스크립트를 이용하여 자동화된 처리를 할 수 있도록 되어 있는데 이것을 악용한 사례라 할 수 있다.

다음은 위 내용에 나오는 올해 이슈가 된 악성코드에 대하여 간단히 정리 해보았다.

바이러스의 위험한 도전

작년에 Win32/Viking 바이러스가 국내외적으로 심각한 피해를 입혔습니다. 단기간에 폭발적

인 변형이 보고된 바이러스로 선정할 수 있을 정도였습니다. 올초에는 이와 비슷하게 Win32/DellBoy 바이러스 변형이 빠르게 증가하였습니다. 그러나 이 바이러스 제작자가 중국당국에 붙잡힌 이후로 심각하게 피해를 주는 변형은 더 이상 보고되고 있지 않습니다.
Win32/DellBoy 바이러스 이외에 Win32/Virut 변형과 Win32/Alman.C 바이러스가 사용자에게 심각한 위협을 끼쳤습니다. 먼저 이들은 분석 및 백신 제작을 지연 시킬 목적으로 은폐/암호화되어 이전 변형과 비교하여 한 단계 업그레이드 된 형태 입니다.

국내 첫 파밍 공격의 시도

Win-Trojan/Banki로 명명된 악성코드는 국내 최초로 호스트 파일을 변조하여 위장된 금융권 웹 사이트로 사용자를 유도하는 파밍 공격을 시도하였습니다. 이 악성코드로 인하여 일부 금융권 사용자가 개인 정보는 물론 공인 인증서까지 탈취당하는 피해를 입었습니다.

ANI 취약점을 이용하는 제로데이 공격 발생

ANI 취약점은 매우 심각한 제로데이 공격에 사용된 취약점으로 윈도우 비스타와 인터넷 익스플로러 7 에서도 동작하였습니다. 윈도우 애니메이션 커서와 아이콘 파일에 존재하는 취약점으로 이 취약점 공격코드가 알려지자마자 기존 중국 발 웹 해킹으로 공격 당한 국내 웹 사이트에서 악성코드를 전파하는데 이용하는 방법으로 이 취약점을 이용하는 사례가 급증하였습니다.

ARP Spoofing 공격으로 인한 악성코드 유포

2007년 상반기에 ARP Spoofing 공격을 이용한 악성코드 유포라는 새로운 형태의 공격이 나타났습니다. 웹서버 보안에 대한 인식이 증대되고 보안성이 강화되면서, 인지도가 높은 웹 서버 자체를 공격하여 악성코드 경유지로 활용하던 과거의 공격패턴과는 달리, 악성코드 감염 대상인 특정 네트워크 서브넷 내에 침투하여 ARP Spoofing을 통해 해당 서브넷 내의 PC들을 감염시켰다는 점에서 주목할 만한 사건이라 할 수 있습니다. 임의의 시스템에 ARP Spoofing 기능을 가지고 있는 일부 Win-Trojan/MulDrop과 같은 악성코드가 설치되고 약간의 세팅만으로 동일 클래스내의 다른 시스템에 쉽게 악성코드가 설치될 수 있습니다. 물론 보안 패치가 적용되지 않은 인터넷 익스플로러를 대상으로 하지만, 이전과 달리 사용자가 이상한(해킹된) 웹사이트를 방문하지 않더라도 악성코드가 설치될 수 있습니다.

AutoRun.inf 를 이용한 자동실행 급증

AutoRun.inf 파일은 그 자체로는 악의적이지 않지만, 이 파일에 명시된 파일들이 자동 실행되기 때문에 그 위험성을 인지해야 합니다. AutoRun.inf와 여기에 자동 실행되도록 명시 된

파일(악성코드)을 DOS 시절 플로피 디스켓에 부트 바이러스가 감염되는 것처럼 컴퓨터에 연결되는 모든 이동식 저장장치에 생성하는 악성코드의 수가 급격히 증가하고 있습니다. 이는 AutoRun.inf를 이용하여 사용자 개입 없이 이동식 저장장치 연결 후 단지 해당 이동식 드라이브를 클릭 하는 것 만으로 자동 실행 되기 때문에 악성코드 제작자들이 악성코드를 전파 및 실행 시키는데 악용하고 있습니다.

이메일 웜…. 끝나지 않는 전쟁

올 상반기 기억될 최악의 악성코드 중 하나로 Win32/Zhelatin.worm. Win32/Stration.worm 을 들 수 있습니다. 비록 국내에 큰 피해를 주지 않았지만 국외에서는 보도자료를 통해서 자주 소개 되었습니다. 전용진단 함수를 추가하기 전까지 V3에 반영된 변형이 16천여개가 반영될 정도로 많은 변형이 발견되었습니다. 특히 메일로 전파되기 때문에 호기심을 자극할 국제적인 이슈를 가진 메일 제목과 내용을 사용하여 사용자로 하여금 첨부 파일을 실행하도록 유도하였습니다.
두 웜은 분명히 다른 형태이지만, 목적은 감염 숙주를 더 많이 확보하여 스팸 메일 발송과 같이 악의적인 목적을 가지고 있으며 서로 경쟁적으로 만들어지고 있는 것으로 보입니다.

LSP (Layered Service Providers) 후킹을 이용한 정보 탈취

국내 온라인 게임의 사용자 계정을 탈취하는 악성코드들에서 LSP 를 이용하여 TCP/IP 핸들러를 삽입하고, winsock2의 연결을 변경하여 자신을 실행하고 정보를 훔쳐내는 형태가 단기간 증가 하였습니다. LSP를 이용한 정보 탈취 및 악성코드 실행은 마치 유행처럼 번졌다가 삽시간 사라졌습니다. 그러나 지금도 간혹 이 방법을 이용한 악성코드가 보고 되고 있습니다.

오피스 문서 취약점을 노린 검은 속셈

오피스 문서의 취약점은 어제, 오늘의 일은 아니다. 취약점을 악용하여 오피스 문서를 오픈할 때 내부에 포함된 트로이목마 (주로 백도어)를 실행 하는 형태이다. 이 취약점은 제로데이 성격 보다는 작년에 보고 된 오피스 취약점을 이용한 형태가 부쩍 많았다.

메신저 웜 다시 기승

Win32/ShadoBot.worm 이라고 명명된 MSN 으로 전파 되는 악성코드가 올 상반기 보고 되었다. 이것은 마치 사진이 들어 있는 압축파일로 자신을 위장하여 사용자로 하여금 압축을 풀고 첨부된 파일을 실행 하도록 유도한다. 이 악성코드는 특정 IRC 서버에 접속하여 시스템의 제어권을 탈취 하도록 설계 되었다.

(2) 2007년 상반기 스파이웨어 동향

2007년 상반기 신종 및 변형 스파이웨어 발견 현황

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
1월	62	38	29	42	4	6	2	0	1	184
2월	72	17	12	41	1	10	2	0	1	156
3월	48	17	10	20	0	5	2	0	0	102
4월	105	20	13	30	1	5	3	3	0	180
5월	143	29	5	46	1	4	1	3	0	232
6월	108	46	19	38	2	3	0	0	0	216

[표 3-1] 2007년 상반기 신종 및 변형 스파이웨어 발견 현황

온라인 게임 계정 유출 스파이웨어의 피해

2006년 하반기부터 증가하기 시작한 온라인 게임계정 유출 스파이웨어의 피해는 최근까지 이어지고 있으며, 2007년 1월에 최고조에 달했다. 주로 중국발 해킹에 의한 웹사이트 변조로 시작되는 스파이웨어 감염은 취약점 패치를 설치하지 않은 IE 브라우저 사용자가 공격코드가 삽입된 웹 사이트에 방문하는 것 만으로도 쉽게 감염되기 때문에 국내 여러 사용자에게 피해를 입혔다.

온라인게임 계정 유출 스파이웨어 설치에는 MS07-017 취약점이 가장 많이 사용되었으며 스파이웨어 마토리(Win-Spyware/Matory)의 일부 변형은 웜의 기능이 추가되어 네트워크 상의 취약한 시스템을 공격하고 스스로 전파되기도 하였다. 스파이웨어는 주로 국내 주요 온라인 게임의 계정을 공격자에게 이메일로 전송하는 목적으로 만들어졌다. 이들 공격의 대부분이 중국으로부터 시작된다는 사실은 2007년 초부터 만연하고 있는 DDoS 공격에 이은 웹 사이트 인질극이나 보이스피싱과 맥락을 같이 한다.

UCC를 이용한 스파이웨어 감염

UCC 열풍과 함께 UCC를 이용한 스파이웨어 배포가 증가하였다. 이미 2005년에 동영상파일 또는 플래쉬(Flash) 파일에 스파이웨어 설치를 유도하는 스크립트가 삽입된 형태의 UCC가 발견된 바 있으나, UCC라는 단어가 대중화 되기 시작한 올해부터는 더욱 다양한 형태의 UCC를 이용한 스파이웨어 배포가 시도되고 있다. 가짜 코덱으로 알려진 비디오코덱(Video ActiveX Codec, 진단명 Win-Adware/Rogue.Codec.gen)의 경우 성인 동영상을 미끼로 동영상을 보려면 코덱 설치가 필요하다는 메시지를 보여주고 설치를 유도한다. 그러나 실제로는 동영상 코덱과 관련된 어떠한 구성요소도 설치하지 않으며, 스파이웨어 훼이크얼럿(Win-

Spyware/FakeAlert), 애드웨어 툴바 프로텍션바 (Win-Adware/ToolBar.ProtectionBar) 등의 스파이웨어를 설치한다.

국내에서도 동영상을 미끼로 허위 안티-스파이웨어 및 애드웨어의 ActiveX 컨트롤 설치를 유도하는 웹 사이트가 여럿 발견되었다. 이들 웹 사이트의 대부분은 실제로는 동영상을 제공하지 않으며, 스파이웨어 배포를 목적으로 제작된 것으로 예상된다. 유명 포탈사이트의 상위에 랭크된 검색어를 이용하여 카페나 블로그의 이른바 '낚시 게시물'을 작성하고 방문을 유도하는 방법을 사용하기도 한다.

국내 애드웨어, 허위 안티-스파이웨어 프로그램의 피해 증가

국외에서 제작된 스파이웨어의 피해가 상대적으로 감소한 반면 국내 제작 애드웨어 및 허위 안티-스파이웨어 프로그램으로 인하여 많은 사용자에게 피해가 발생하였다. 제휴 마케팅 사이트를 중심으로 애드웨어 제작사와 이를 배포하는 배포자(파트너)가 증가하면서 국내 애드웨어 및 허위 안티-스파이웨어 프로그램의 제작 배포가 늘었으며 이들의 활동은 모두 금전적인 이익을 목적으로 한다.

광고와 유료사용자 확보를 목적으로 하는 제작사와 배포당 배당금이 지급되는 배포자(파트너) 모두 많은 사용자에게 배포할수록 이익이 발생할 확률이 높아지므로 위에서 언급한 UCC 동영상을 이용하거나 유용한 프로그램으로 속여 배포한다. 최근에는 백그라운드로 동작하는 다운로더를 사용자 몰래 설치하고 이를 이용하여 배포당 배당금을 지급하는 애드웨어를 설치하는 사례도 늘고 있어 사용자의 각별한 주의가 필요하다.

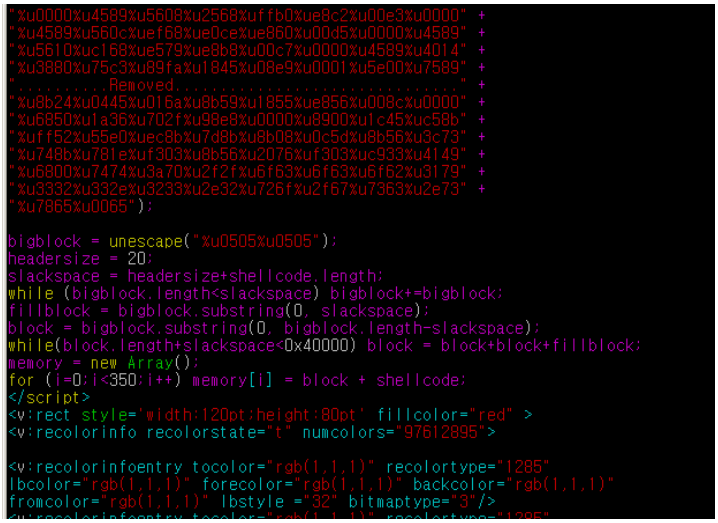
허위 안티-스파이웨어 프로그램인 로그 씨씨(Win-Adware/Rogue.CC)의 경우 루트킷을 설치하여 구성요소를 은폐하고 실행 중인 사실을 숨기는 등 프로그램 동작 측면에서도 악성코드화 되어 가고 있으며, 예상하지 못한 오류로 시스템 가용성을 크게 위협한다. 특히 애드웨어 네마리(Win-Adware/Nemari) 등의 몇몇 스파이웨어의 경우 바이럿(Win32/Virut) 바이러스에 감염된 채로 배포되어 뜻하지 않게 컴퓨터 바이러스 감염의 매개체가 되기도 하였다. 또한 애드웨어 어도드(Win-Adware/Adod)의 경우 프로그램 자체의 버그로 인하여 IE를 실행시키자 마자 IE가 종료되는 문제를 유발하였다.

(3) 2007년 상반기 시큐리티 동향

2007년 상반기 주요 시큐리티 이슈는 아래와 같다.

MS06-004 VML 취약점

VML 취약점은 1월9일 MS07-004 취약점 패치가 발표 되었고 얼마 지나지 않아 1월16일, 17일에 각각 공격코드가 공개되었다. 해당 취약점은 마이크로소프트사가 지원하는 VML(Vector Markup Language)컴포넌트 상에서 발생하는 Integer Overflow 취약점이다



[그림 3-5] MS07-004 취약점을 웹 사이트에 악용한 사례

Sun Solaris 텔넷 인증 우회 취약점

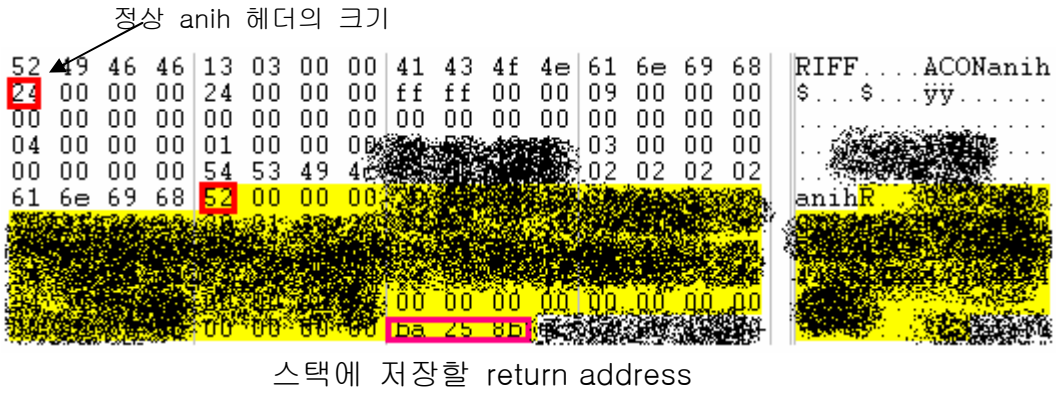
지난 2월 12일 Sun 마이크로시스템사의 새로운 취약점 발표 소식을 듣고 많은 사용자들은 허탈함을 금치 못했을 것이다. 그 이유는 해당 취약점이 별다른 공격기술이나 공격도구 없이 단지 특정 옵션을 사용하는 것만으로 매우 치명적인 결과를 초래할 수 있는 단순한 취약점 이었기 때문이다. 이 취약점은 1990년대 중반에 발표된 rsh 취약점과 매우 유사하다

```
SECURE# telnet -l "-froot" <telnet server ip>
Trying <client_ip>...
Connected to <client_ip>.
Escape character is '^]':
#
```

MS07-017 Animated Cursor Handling(ANI 파일) 취약점

2007년 3월 user32.dll 파일의 취약점을 이용한 제로데이 공격이 출현하였다. 이 취약점은 2005년에 발견된 취약점(MS05-002)과 동일한 곳에서 발견되어 결과적으로 과거 MS사의 패치가 잘못되었다는 것을 보여주었다.

MS05-002는 힙 오버플로우인 반면에, MS07-017은 사용자가 조작된 Animated Cursor 파일을 특정 어플리케이션에 로드할 경우 취약점이 존재하는 곳에서 버퍼 오버 플로우가 발생하며 그결과로 공격자는 임의의 코드를 사용자의 시스템에서 실행할 수 있다. 취약점이 존재하는 곳은 User32.dll의 LoadAniIcon 함수로 이 함수의 역할은 Animated Cursor 파일의 헤더를 파싱하고 해당 데이터를 처리하는 것이며 이 함수는 Animated File 을 로드할 때 실행된다.



[그림 3-6] 조작된 animated cursor 파일 덤프

MS07-029 MS DNS SRV 취약점의 악성코드화

MS07-029 취약점은 원격에서 코드를 실행할 수 있는 취약점이 존재하는 것으로, 관리자 권한으로 로그인 되어 있는 경우 공격자는 시스템을 제어할 수 있는 모든 권한을 얻을 수 있게 된다.

이 취약점은 DNS 서버 서비스에 바인딩 되어 있는 RPC 에 조작된 공격 패킷을 보내 임의의 코드를 실행할 수 있다. RPC 의 UUID "50abc2a4-574d-40b3-9d66-ee4fd5fba076" 의 DnssrvQuery 값(0x01 DnssrvQuery)을 설정하여 악용하는 것이다. 공개된 개념증명코드(Proof of Concept)에서는 포트바인딩 쉘코드(PortBind Shellcode)를 사용하여 MS DNS RPC서비스 취약점을 이용한 시스템 권한 획득이 가능함을 보여주었다. 또한, Windows 2000 서버의 DNS 서비스를 공격하는 악성코드가 발견되기도 하여 그 위협의 심각성을 짐작케 하였다. (V3진단명: Win32/IRCBot.worm.199680.I)

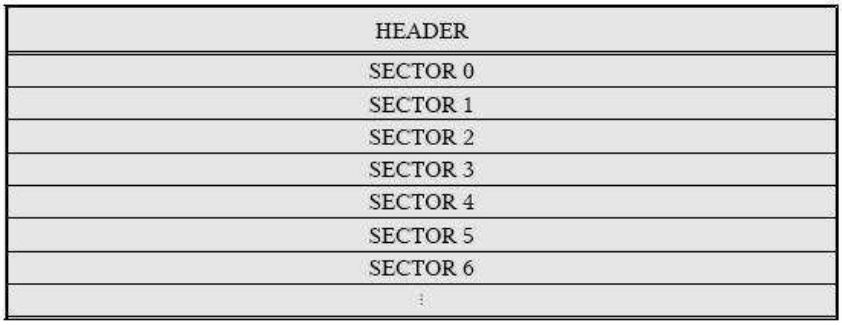
마이크로소프트 오피스 취약점의 꾸준한 증가

오피스 프로그램은 대다수 사용자가 이용하는 응용 프로그램으로 스프레드 시트 프로그램인 엑셀(Excel), 문서 작성/편집 프로그램인 워드(Word), 프리젠테이션 관련 프로그램인 파워포인트(PowerPoint), 데이터 베이스 관련 프로그램인(Access), 이메일 프로그램인 아웃룩(OutLook)등으로 구성되어져 있다.

MS 오피스 취약점은 이러한 오피스 프로그램 및 오피스 라이브러리에 버그(Bug)가 존재하는 것을 말한다. 사용자가 악의적으로 조작된 오피스 파일(File)을 읽는 과정에서, 사용자가 관리자 권한으로 로그인 되어 있는 경우 취약점을 악용한 공격자는 프로그램의 설치, 보기, 변경, 데이터 삭제등과 같은 권한을 얻게 되어 시스템을 완전히 제어할 수 있게 된다. 하지만, 취약점을 이용한 공격에 성공하기 위해서는 사용자의 개입이 필요하다.

MS 오피스 프로그램이 기업의 많은 컴퓨터에 설치되어 있기 때문에, 위험의 심각도가 있다고 볼 수 있다. MS Office는 다수의 애플리케이션으로부터 생성된 데이터를 하나의 파일에 포함시킬 수 있는 Compound Document File Format 을 갖는다. Compound Document file 은 실제 파일 시스템과 유사한데, 데이터를 다수의 Stream(파일 개념)으로 분할하여 Storage(디렉토리 개념) 속에 나누어 저장한다. 다시 Stream은 작은 데이터 블록 단위인 Sector로 구분되는 데 반드시 연속되는 Sector들이 하나의 Stream을 이루는 것은 아니며 Stream의 구성은 Sector들의 연결 Chain(SID chain)으로 표현된다.

Compound Document File Format [1]은 일반적으로 다음과 같이 메타 데이터를 저장하고 있는 Header 와 고정된 사이즈의 Sector들로 구성되어 있다.



일반적으로 MS 오피스의 취약점은 특정 오브젝트의 특정 필드에서 Overflow 버그가 발생하거나, 오피스 공통 라이브러리에서 취약점이 발견되는 경우도 존재한다. 2007년 상반기에 발표된 MS 오피스 취약점은 아래와 같다.

---

[1] Microsoft Compound Document File Format
(http://sc.openoffice.org/compdocfileformat.pdf)

MS07-002 Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점(927198)
MS07-003 Microsoft Outlook의 취약점으로 인한 원격 코드 실행 문제점(925938)
MS07-014 Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점(929434)
MS07-015 Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점(932554)
MS07-023 Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점 (934233)
MS07-024 Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점 (934232)
MS07-025 Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점 (934873)
MS07-030 Microsoft Visio의 취약점으로 인한 원격 코드 실행 문제점(927051)

MS 오피스 취약점은 2006년 상반기부터 본격적으로 나타나기 시작하였다. MS 사의 보안 패치 중에 2006년과 2007년 6월까지 MS 오피스 공격에 이용될 수 있는 취약점은 총 22건이다. 이것은 같은 기간 동안의 전체 보안 패치중에 약 19.4% 정도를 차지하고 있다.

취약점을 이용한 공격에는 조작된 파일을 특정/불특정 사용자에게 메일 또는 웹으로 전달하여 사용자가 해당 오피스 파일(File) 읽는 경우 임의의 코드 또는 악성코드를 실행할 수 있게 된다.

악성코드는 V3 진단명으로 PP97M/Exploit-PPDropper, X97M/Exploit.Excel, X97M/Exploit.ControlExcel, W97M/Exploit-OleData등이 존재하고, 오피스 문서 내부 코드에 트루잔(Trojan) 및 다운로더(Downloader)등이 포함되어져 있기도 하며, 최근에는 특정 오피스 취약점을 공격하는 자동 제작기가 중국에서 발견되기도 하였다.

외국뿐만 아니라 국내에서도 MS 오피스 취약점을 이용한 공격이 발생하고 있는데, 이러한 공격은 주로 특정 목적을 가지고 수행되는 것으로 보이며, 개인 및 기업등의 민감한 정보를 노리는 것으로 파악된다. MS 오피스 취약점은 제로데이(Zero-Day) 공격에도 자주 사용이 되고 있기 때문에, 주의가 필요하다.

오피스 사용자가 주의해야 할 점은 아래와 같다

1. 오피스 프로그램의 보안 패치를 주기적으로 해야 한다.
2. 오피스 파일을 메일 또는 웹으로 받은 경우에는 신뢰되지 않은 사용자이거나 신뢰되지 않은 웹 사이트인 경우에 주의가 필요하다.
3. Anti-Virus 제품 및 개인 방화벽을 사용한다.
4. 네트워크 관리자는 네트워크 보안 제품의 사용을 고려한다.
5. 네트워크 관리자는 메일 서버에서 오피스 파일이 첨부된 이메일(E-Mail)을 필터링(Filtering)하는 것을 고려할 수도 있다.

사회공학 기법인 전화사기(보이스 피싱) 극성

인간의 행동은 예측 가능하지 않기 때문에 사회의 절차나 제도, 사람의 심리등을 악용하여, 필요한 정보를 구하는 기법이 사회공학이다. 이러한 사회공학 기법을 이용한 보이스 피싱/전화사기가 극성을 보이고 있다. 보이스 피싱/전화사기는 2006년 부터 꾸준하게 일어나고 있으나, 2007년에 들어서는 보다 교묘한 방법으로, 정부기관 및 기타 단체, 개인등을 사칭하여, 금품을 노리고 있다.

보이스 피싱/전화시기를 예방하기 위해서는 2007년 상반기에 금융감독원에서 발표한 “전화금융사기 피해를 막을 수 있는 8가지 수칙”을 참고하도록 하자.

- 전화로 개인정보 요구시 응하지 말 것
- "현금지급기로 세금 환급"도 사기
- 속아서 계좌이체 했다면 은행에 지급정지 신청
- 개인정보 알려줬다면 은행에 신고
- "나, 동창생인데.." 입금요구시 사실관계 확인
- 발신자 전화번호 확인해야
- ARS 사기전화 주의
- SMS 서비스 적극 이용

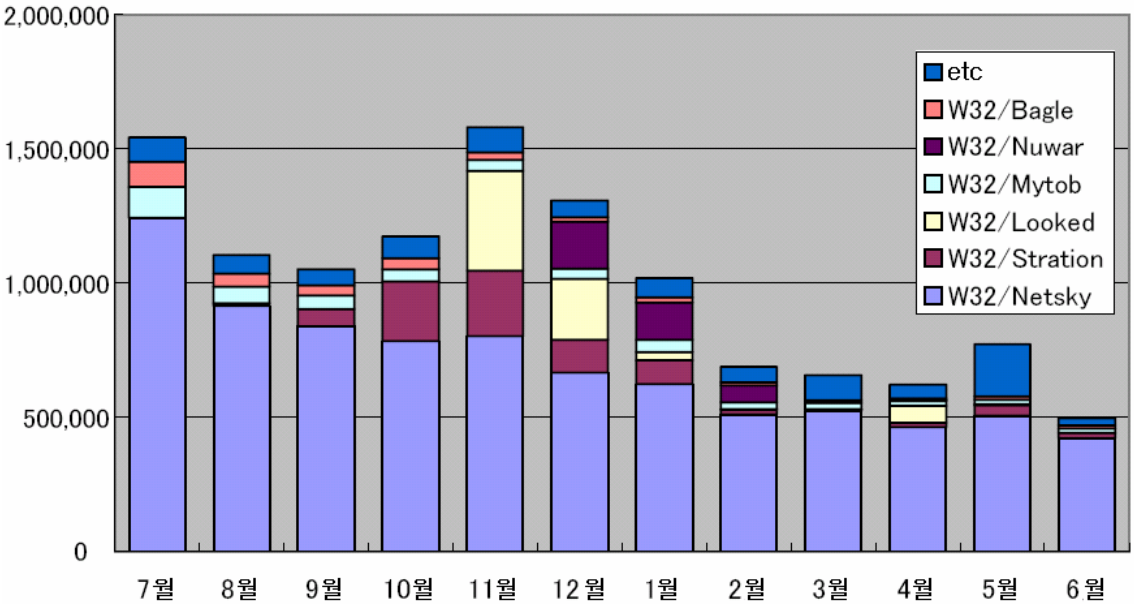
(4) 2007년 상반기 일본 악성코드 동향

2007년 상반기 일본의 악성코드 동향과 관련하여 특이할 만한 사항은 새롭게 발견된 이메일 웜들이 많은 감염 피해를 발생시킨 것과 실행 파일을 변조하고 악성코드를 다운로드하여 설치하는 악성코드인 바이럿 바이러스의 감염이 증가한 점을 들 수 있다.

최근의 악성코드와 관련한 주요 변화로는 금전적인 이익을 취하기 위한 트로이목마가 전체 악성코드에서 차지하는 비율이 높아지고 몇 년 전부터 기승을 부리던 이메일 웜의 감염 피해가 낮아지고 있는 점이다. 그러나 일본의 경우 2007년 상반기에도 이메일 웜에 의한 피해가 여전히 높게 나타나고 있고 타 지역에서 감염 피해가 높지 않은 악성코드에 의한 피해 또한 높게 보고되고 있다. 또한 실행 파일을 감염시키는 바이러스인 바이럿의 급격한 피해 증가 또한 눈에 띈다. 바이럿의 경우 감염 후 다른 악성코드를 다운로드하여 설치함으로써 추가 감염의 위험성이 매우 높은 상태이고 제작 목적이 사용자 정보를 취득하기 위한 것이므로 PC 사용자의 주의가 필요하다.

악성코드 피해 동향

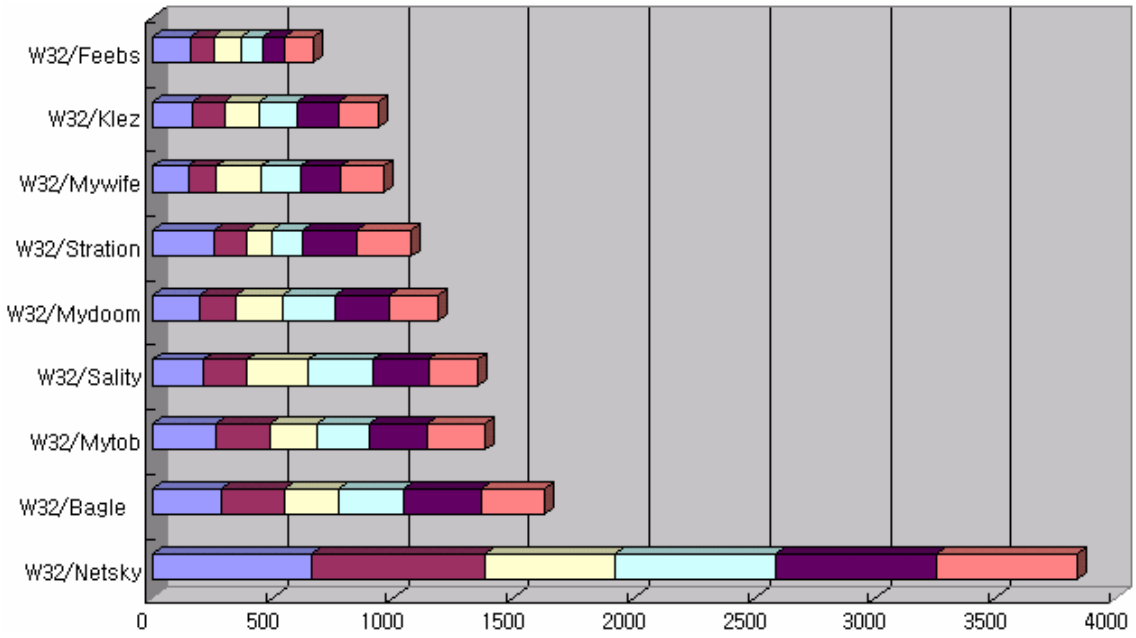
2007년 상반기에 일본에서 가장 많은 감염 피해가 발생한 악성코드는 넷스카이 웜(Win32/Netsky.worm)이다. 넷스카이 웜 이외에도 베이글 웜(Win32/Bagle.worm)과 마이탑 웜 (Win32/Mytob.worm)등의 메스메일러의 피해가 여전히 많이 발생하고 있으며 이러한 상황은 전년과 비교해서 크게 달라지지 않았다.



[그림 3-7] 2007년 상반기 악성코드 탐지 통계(일본)[1]

[1] 자료출처: 일본 IPA

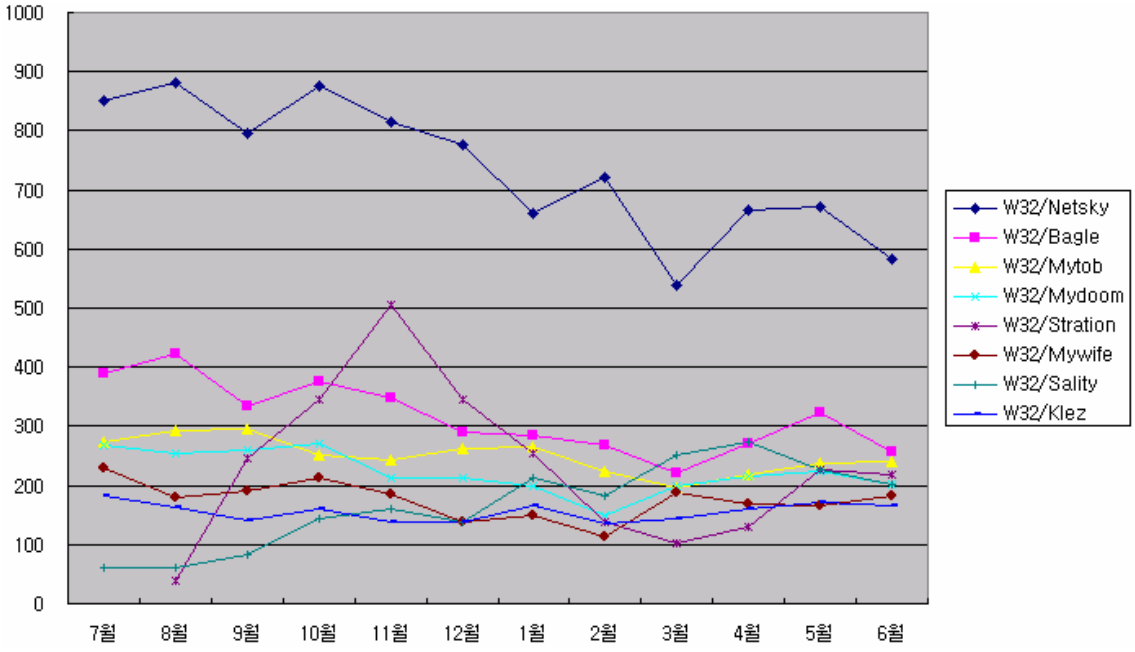
[그림 3-7]은 일본의 IPA에서 발표한 월별 악성코드 검출 개수에 대한 통계를 그래프로 나타낸 것이다. 넷스카이 웜의 탐지 개수가 다른 악성코드들에 비해서 월등하게 많은 것을 볼 수 있다. 이러한 현상은 전년에 비해서 크게 다르지 않으나 전체적인 검출양은 올 해에 들어와서 점진적으로 감소하고 있는 것을 볼 수 있다. 넷스카이 웜 뿐 아니라 다른 악성코드들의 경우에도 미세하지만 점차 탐지 양이 감소하는 것을 볼 수 있다. 위의 통계에서 특이한 점은 2007년 5월에 전체 검출 양이 전월에 비해 갑자기 증가한 것인데 이는 해당월에 소버 웜(Win32/Sober.worm)의 탐지 수가 갑자기 늘어난 것이 원인이다.



[그림 3-8] 2007년 상반기 악성코드 감염 신고 통계[1]

[그림 3-8]은 2007년 상반기 일본에서 사용자들에게서 감염 피해가 발생한 신고 통계를 그래프화한 것이다. 위의 그래프에서 핍스 웜(Win32/Feebs.worm)와 살리티 웜(Win32/Sality.worm)의 감염 피해가 매우 많은 것에 주목할 필요가 있다. 두 악성코드들의 경우 다른 지역에서는 그다지 많은 피해 보고가 되고 있지 않으나 일본에서는 상대적으로 많은 양의 피해가 발생하고 있다.

[1] 자료출처: 일본 IPA



[그림 3-9] 월별 악성코드 피해 통계[1]

[그림 3-9]는 일본에서 많은 감염피해가 발생하고 있는 주요 악성코드들의 월별 피해 통계를 그래프로 나타낸 것이다. 살리티 웜의 경우 2007년 1월에 갑자기 피해 양이 증가한 후 현재까지도 많은 피해를 입히고 있는 것을 확인할 수 있고, 핍스 웜 또한 비슷한 시기에 감염 피해가 증가한 것을 알 수 있다. 전반적으로 다른 이메일 웜들의 감염 피해가 감소하고 있는 현 추세에서 이러한 현상은 지속적인 관심을 가질 필요가 있을 것으로 보인다.

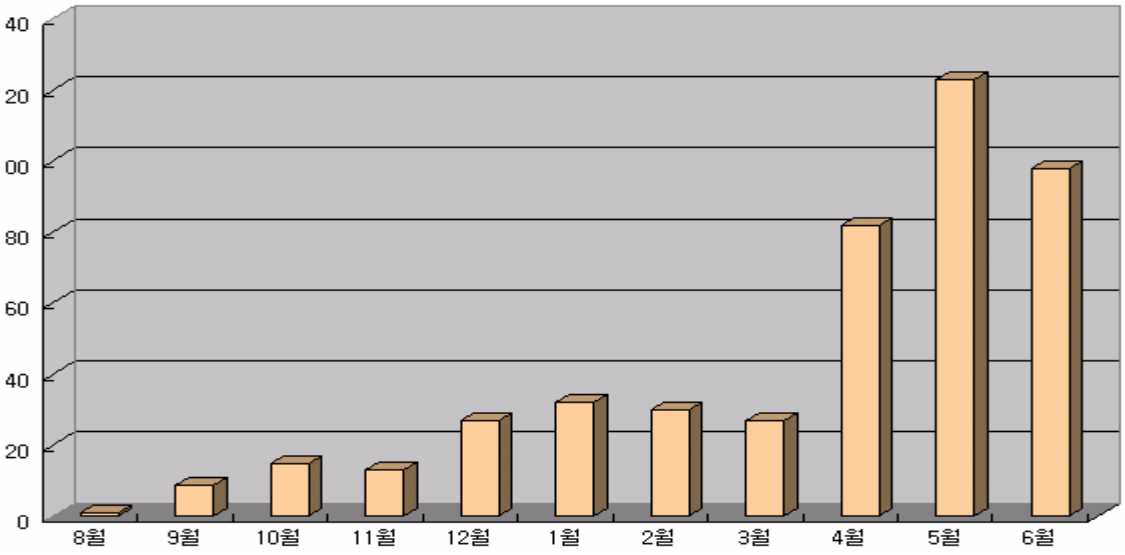
트로이목마 유포를 목적으로 하는 바이러스 감염 증가

바이럿(Win32/Virut) 바이러스는 윈도우 실행파일을 감염시키고 감염된 파일이 실행될 때 특정 URL에서 악성코드 샘플을 다운로드하여 설치하는 악성코드로써 2006년 5월경 최초로 발견된 이후 현재까지도 많은 사용자들에게 피해를 입히고 있다. 바이럿 바이러스가 다운로드하는 파일의 대부분은 악성의 동작을 하는 파일을 다운로드하여 설치하는 다운로더나 드로퍼이고 이러한 악성코드들이 궁극적으로 설치하고자 하는 것은 온라인게임의 계정 정보를 탈취하기 위한 트로이목마이다.

한국의 경우 처음 바이럿 바이러스가 유포되었을 때 많은 사용자들의 피해가 발생했으나 일본에서는 작년까지 바이럿 바이러스로 인한 피해가 보고된 사례가 많지 않았던 것으로 보인다. IPA의 자료에 의하면 일본에서 최초로 바이럿이 발견된 시기는 2006년 7월로 추측되고 이는 2006년 5월에 최초 악성코드가 발견된 후 급속하게 감염 피해가 발생했던 한국의 상

[1] 자료출처: 일본 IPA

황과 비교된다. 그러나 올 해에 들어오면서 바이럿으로 인한 감염 피해가 급격하게 증가하고 있다.



[그림 3-11] 바이럿 바이러스 감염 피해 현황-일본

[그림 3-11]은 월별로 발생한 바이럿 바이러스 감염 피해 신고 현황을 그래프로 나타낸 것이다. 2006년 8월 최초로 발견된 이후 올 해 3월까지 점진적인 증가 추세를 보이던 감염 피해 건수가 4월 이후 급격하게 늘어난 것을 알 수 있다.

바이럿의 경우 감염으로 인해 시스템에 미치는 직접적인 피해도 문제가 되고 있지만 그보다는 사용자 정보를 빼가기 위한 악성코드를 설치하는 용도로 사용되는 점이 사용자에게는 더 위협이다. 게다가 파일 바이러스의 특성상 사용자가 감염 초기에 감염 사실을 쉽게 인지하지 못하는 경우가 대부분이므로 백신 프로그램을 이용하여 주기적인 검사를 실시해 주는 것이 감염으로 인한 피해 예방을 위해 중요하다.

(5) 2007년 상반기 중국 악성코드 동향

중국산 트로이목마의 강세가 전반적인 대세를 이루고 있는 한국의 상황과 유사하게 중국 악성코드 동향도 2007년 상반기에 트로이목마가 큰 축을 이루고 있다. 이러한 트로이목마의 대세는 근본적으로 온라인 머니에서 현실의 리얼 머니까지 금전적인 탈취가 가장 큰 목적을 이루고 있다. 이러한 목적으로 인해 악성코드 제작자는 예전과 달리 아마추어가 아니라 전문적인 프로그래밍 실력을 가지고 있는 집단으로 변화하고 있는 것으로 보인다. 그리고 이러한 악성코드 제작자들은 안티 바이러스 소프트웨어에 대해 다양한 테스트를 통해서 탐지 회피와 함께 직접적인 공격을 가할 수 있는 새로운 방법들을 지속적으로 개발하고 있는 실정이다.
이러한 사항들을 바탕으로 중국의 악성코드 동향을 중국 보안 업체인 라이징(Rising)과 지앙민(JiangMin)의 자료를 통해서 살펴보도록 하자.

악성코드 TOP 10

순위 변화	순위	Rising
New	1	Trojan.PSW.OnlineGames
New	2	Trojan.Mnless
New	3	Trojan.DL.MnLess
↓ 3	4	Trojan.DL.Agent
New	5	Hack.SuspiciousAni
-	6	Worm.Viking
New	7	RootKit.Agent
New	8	Trojan.DL.JS.Agent
New	9	Trojan.PSW.QQPass
New	10	Trojan.PSW.RocOnline

[표 3-2] 2007년 2/4 분기 중국 라이징(Rising) 악성코드 TOP 10
'-' - 순위변동 없음, 'New' – 순위에 새로 진입, '↑'- 순위 상승, '↓' - 순위 하락

먼저 라이징의 악성코드 TOP 10인 [표 3-2]부터 살펴보면, 2분기에도 지난 1분기와 마찬가지로 트로이목마가 대세인 것을 확인할 수 있다. 그리고 트로이목마의 대세 속에서도 가장 큰 변화는 온라인 게임의 사용자 정보를 외부로 유출하는 형태의 트로이목마가 대거 순위에 진입한 것이다. 이러한 변화는 대부분의 공격 대상이 되는 온라인 게임들이 한국에서 개발된 것들이었으나, 이제는 대만 또는 중국 내에서 제작된 온라인 게임들로 공격 대상이 변화되고 있기 때문이다. 이는 중국어권 내의 온라인 게임이 다양하게 출시되어 공격의 타켓이 다양화된 측면도 있지만, 한국 내의 온라인 게임 개발업체들이 중국산 악성코드의 공격으로부터 고

객을 보호하기 위해 다양한 보안 제품과 정책들을 적용한 것도 한 몫하고 있는 것으로 분석된다.

지난 1분기에도 순위에 포함되었던 악성코드로는 유일하게 바이킹(Win32/Viking) 변형이 차지하고 있다. 한국에서는 바이킹 바이러스 보다는 델보이(Win32/Dellboy) 바이러스 변형이 많이 발견된 것과는 차이를 보이고 있다.

2007년 상반기의 중국내 악성코드의 큰 축을 이루고 있는 다양한 형태의 트로이목마들이 어떻게 전파되는지를 잘 보여주는 취약점이 순위에 포함되어 있는데, 바로 MS07-017 ANI 취약점을 이용하는 Hack.SuspiciousAni(Win-Trojan/Exploit-ANI)이다. 해당 취약점이 5위에 포함되었다는 것은 이 취약점이 다양한 트로이목마의 감염 수단으로 이용하고 있다는 것을 명확히 확인시켜주는 것이라고 할 수 있다.

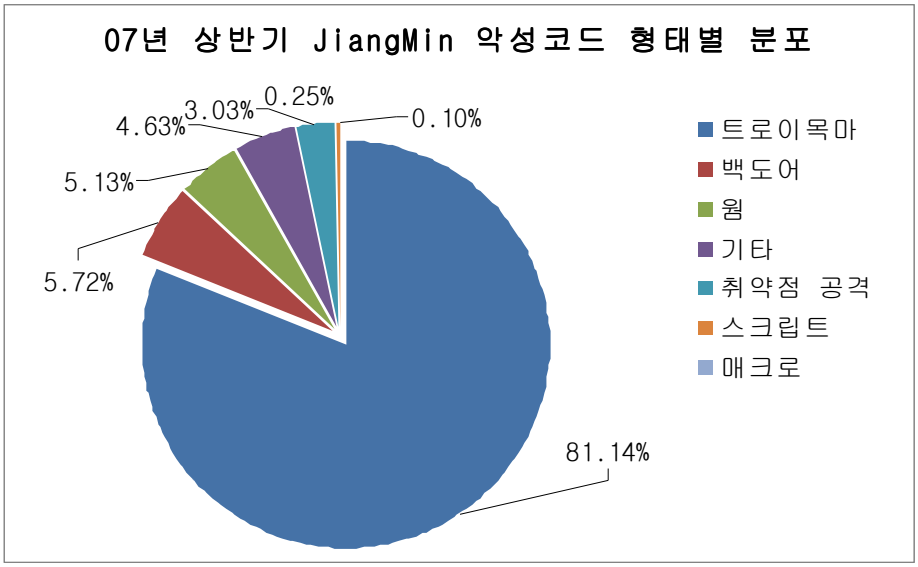
순위 변화	순위	JiangMin
New	1	Checker/Autorun
New	2	Exploit.ANIfile.b
New	3	Trojan/PSW.GamePass.hwd
New	4	TrojanDownloader.Adload.lp
New	5	Trojan/PSW.GamePass.ify
New	6	Trojan/PSW.GamePass.kwr
New	7	Trojan/PSW.GamePass.gdt
New	8	Backdoor/Agent.mkp
New	9	Worm/Viking.ahj
New	10	Trojan/PSW.GamePass.lpb

[표 3-3] 2007년 2/4 분기 중국 지앙민(JiangMin) 악성코드 TOP 10

'-' - 순위변동 없음, 'New' – 순위에 새로 진입, '↑'- 순위 상승, '↓' - 순위 하락

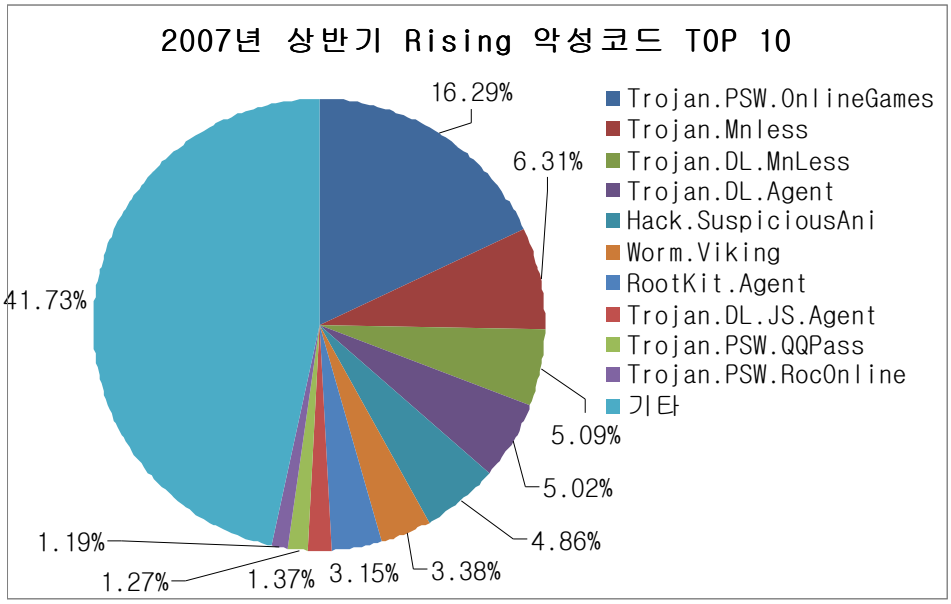
[표 3-3]은 지앙민의 악성코드 TOP 10 순위를 나타낸 것으로, 라이징과 유사하게 온라인 게임 관련 트로이목마가 순위에 대거 포함된 점과 바이킹 바이러스 역시 순위에 포함되어 있다. 그러나, 특이할 만한 점은 1위를 차지하고 있는 Checker/Autorun으로 최근 중국산 악성코드에서는 새로운 감염 기법으로 Autorun.inf 파일을 사용하고 있다. Autorun.inf을 이용하여 USB와 같은 외장형 저장 장치를 통해서 다른 시스템으로 감염을 시도하고 있는데, 이 Autorun.inf 파일을 지앙민에서는 Checker/Autorun 라는 진단명으로 진단하고 있다. 이 진단명이 1위를 차지하고 있다는 점을 통해서 중국 내에서는 이미 Autorun.inf 파일을 이용한 악성코드가 상당수를 차지하고 있다는 것을 알 수 있다.

[그림 3-12]는 지앙민에서 2사분기 동안 발견된 악성코드 형태별로 분류한 분포도 이다. 해당 분포도를 참고하면 한국과 유사하게 트로이목마와 백도어가 81.14%와 5.72%을 차지하며 전체의 절대 다수를 차지하고 있다는 것을 잘 알 수 있다.



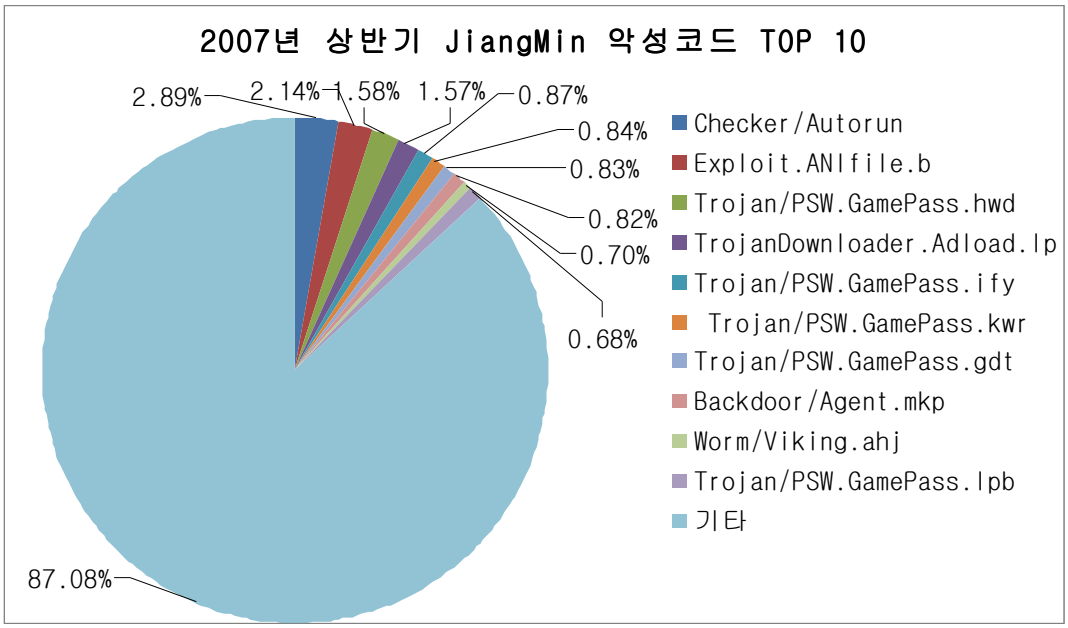
[그림 3-12] 2007년 상반기 중국 지앙민(JiangMin) 악성코드 형태별 분포

악성코드 TOP 10 분포



[그림 3-13] 2007년 상반기 중국 라이징(Rising) 악성코드 TOP 10과 분포

[그림 3-13]은 라이징의 악성코드 TOP 10에 따른 전체 악성코드 분포도이다. 악성코드 TOP 10의 순위에 포함된 악성코드는 전체의 과반수를 겨우 넘길 정도인 것으로 미루어 다양한 형태의 악성코드가 중국 현지에서 발견되고 있는 것으로 분석된다.



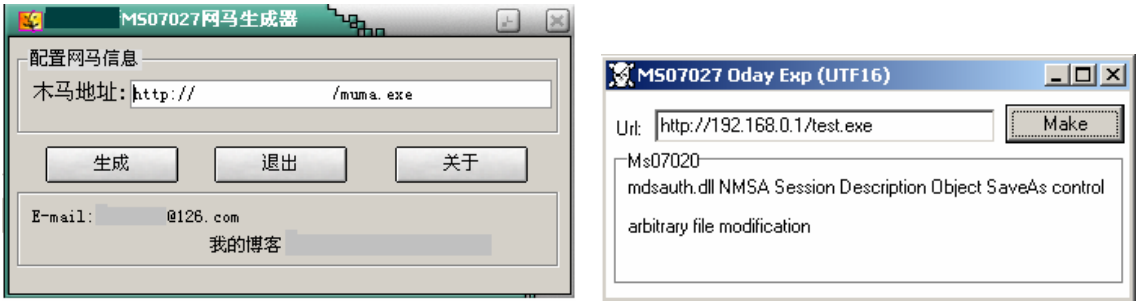
[그림 3-14] 2007년 상반기 중국 지앙민(JiangMin) 악성코드 TOP 10과 분포

지앙민의 악성코드 TOP 10의 분포를 나타낸 [그림 3-14] 역시 라이징과 유사하게 TOP 10의 악성코드가 전체의 과반수를 차지하지 못하고 있으며 기타에 포함된 다양한 악성코드가 87.08%로 절대 다수를 차지하고 있는 것을 잘 알 수 있다.

라이징과 지앙민의 악성코드 피해 분포도를 분석한 결과 피해 순위를 집계하는 것이 무의미할 정도로 악의적인 목적에 따라서 제작되는 악성코드가 점점 다양해지고 있는 것으로 보여지고 이러한 변화는 악성코드에 의해 발생할 수 있는 보안 사고도 점점 다양해 질 수 있다는 것을 염두에 두어야 할 것이다. 그리고 이에 따른 대비책도 복합적인 공격 형태에 초점을 맞춘 보안 정책과 대응책이 마련되어야 할 것으로 보여진다.

자동화된 악성코드 생성

과거부터 악성코드 제작자들은 악성코드의 변형을 조금 더 쉬운 방식으로 제작하기 위해 다양한 악성코드 제작툴(Constructor)들을 제작하였으며, 이를 이용하여 안티 바이러스 소프트웨어에 탐지되지 않는 변형들을 단시간 내에 많이 양산하고 있다. 최근에는 실행 압축을 이용하여 악성코드에 대한 변종 생성이 더욱 간편해지면서 이러한 제작툴 들이 점차 줄어드는 듯한 추세를 보였다. 그러나 2007년 들어 중국 언더그라운드에서는 단순히 변형된 트로이목마 생성보다는 취약점을 공격하는 익스플로잇(Exploit)이 포함된 스크립트를 생성해주는 제작툴 들이 자주 발견되고 있다.



[그림 3-15] MS07-027 취약점을 공격 트로이목마 생성 도구

앞서 라이징과 지앙민의 악성코드 TOP 10을 살펴보면서 악성코드 확산에 악용되고 있는 MS07-017 ANI 취약점에 대해서 언급하였는데 악성코드 제작자들은 이러한 보안 취약점을 공격하는 스크립트를 쉽게 제작하기 위해 [그림 3-15]와 같이 MS07-027 취약점을 공격하는 스크립트 제작 툴들을 제작하여 공유하고 있다.

취약점을 공격하는 스크립트 생성툴들은 [그림 3-15]와 같이 트로이목마를 다운로드 할 주소만 변경해주고 생성 버튼만 클릭해주면 새로운 스크립트를 생성 할 수가 있게 된다. 그리고 경우에 따라서는 안티 바이러스 분석가들의 분석을 지연시키기 위해 인코딩(Encoding) 또는 암호화를 적절하게 가미시킬 수 도 있다.

[그림 3-16] 다양한 취약점을 공격하는 트로이목마 생성 도구

[그림 3-15]와 같이 특정 취약점만 포함된 스크립트를 생성할 수 있는 제작 툴이 있는 반면 [그림 3-16]와 같이 MS07-017 ANI 취약점을 비롯하여 MS06-014와 MS07-027 취약점 모두를 공격할 수 있는 스크립트도 생성 할 수 있는 제작 툴도 발견되었다.

과거 특정 취약점이 발견될 경우에는 일부 언더그라운드 그룹에서만 해당 취약점을 공격하는 익스플로잇 코드를 제작하고 사용해왔으나, 최근에는 이러한 제작 툴을 인터넷을 통하여 쉽게 공유함으로써 익스플로잇 코드는 순식간에 많은 사람들에 의해 악용될 수 있다. 이러한 점들을 생각한다면 운영체제에 대한 보안 패치 적용이 얼마나 중요한지 새삼 강조하지 않을 수 없다.

(6) 2007년 상반기 세계 악성코드 동향

2007년에도 악성코드의 지역화, 단기 공격화가 지속되고 있으며 바이러스나 웜보다 트로이 목마가 많이 발견되고 있다. 이에 여러 보안업체에서는 현실과 다소 거리가 먼 악성코드 피해 집계 방식을 변경하고 있다. 그 동안 집계 방식은 고객 신고와 메일에 첨부된 악성코드 수에 대한 집계 방식이었는데 이는 일반 사용자들의 체감과 달랐다.

소포스의 2007년 2/4분기 웹 사이트 기반의 악성코드 피해 통계는 Mal/Iframe이 64.0%로 1위를 차지했다. 우리나라의 경우 2005년부터 웹사이트 해킹 후 취약점을 이용한 코드를 심어두고 패치가 안된 시스템이 접속하면 악성코드가 자동으로 설치되는 형태의 공격이 유행하고 있다. 유럽 등에서는 이러한 형태의 공격이 최근에 본격적으로 문제가 부각되고 있는 것으로 보인다. 특히 2007년 6월 초 이탈리아에서 수 천 개의 웹 사이트에 악성코드를 다운로드를 코드가 숨겨진 사건이 발생했으며 여기에는 $500~ $1,000 정도로 판매되는 MPack이라는 툴이 사용되었다.

몇 년 전만 해도 악성코드 주 발생 지역은 미국, 러시아, 유럽이었지만 최근 몇 년 동안 중국이 악성코드 대국으로 급격히 부상하고 있다. 중국에서만 한 달에 대략 2만개 정도의 신종 악성코드가 제작되는 것으로 추정되고 있으며, 이들 중 상당수는 악성코드로 돈을 벌려는 사람들이 적극 가담하고 있는 것으로 보인다. 1990년대 초반까지 주요 바이러스 제작국은 구 소련과 동유럽이었는데, 당시에는 프로그래밍 기술은 높지만, 높은 실업률로 취업이 힘들어 바이러스를 제작/유포하는 경우가 있었다. 그러나, 현재 중국와 러시아의 상황은 금전적인 이득을 위하여 악성코드와 스팸을 제작하고 배포하고 있다.

이런 악성코드 제작자들의 공격에는 국가적 자존심도 반영되는 경우도 있다. 5월에는 러시아 쪽에서 에스토니아(Estonia) 서버에 대한 공격이 있었다. 이는 구 소련에서 독립한 에스토니아가 과거 구 소련의 잔재를 없애기 위해 구 소련 시절 조각들을 해체하면서 촉발했다. 에스토니아 사이트에 대한 대규모 해킹이 발생했고 에스토니아 사이트를 전문적으로 공격하는 DDoS 툴이 배포되었다. 이에 에스토니아 사람들은 러시아 사이트를 해킹해 자신들의 정치적 메시지를 담기도 했다. 흡사 과거 발생한 미국-중국간, 중국-일본간 사이버 분쟁과 흡사한 일이었다. 실제 테러에 비교할 수는 없겠지만 종종 악성코드 제작자나 해커들은 정치적 사건에도 자신들의 기술을 이용하기도 한다.

IV. ASEC 컬럼

(1) ARP spoofing의 습격

최근 ARP Spoofing을 이용한 공격 기능이 탑재된 악성코드가 발견되고 있다. 공격자는 이 ARP Spoofing 공격기능을 이용하여 기업 내부 네트워크를 마비시키거나, HTTP 사용자인증 정보, VoIP 음성 데이터 등의 중요 정보를 가로챌 수 있으며, 최근에는 웹 서버와 클라이언트 간의 웹 트래픽 정보를 변조하여 악성코드를 감염시키는 데 활용되기도 하였다. 이미 오래전부터 ARP Spoofing 공격에 대해서는 많은 연구들이 진행되어 왔지만 정상적인 ARP 응답/요청 메시지와 크게 구별되지 못하는 등의 문제로 인해 아직까지 이러할 만한 대응 체계가 마련되지 못하고 있는 실정이다.

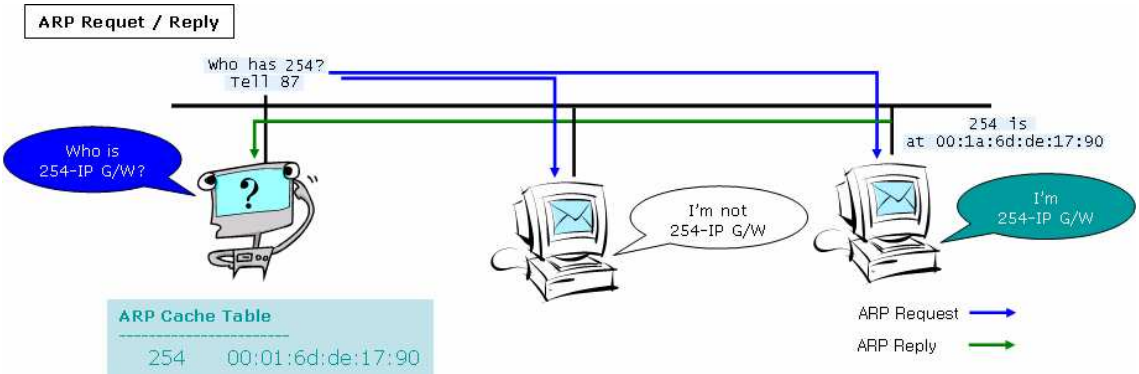
본 칼럼을 통해 ARP Spoofing과 이를 이용한 공격 등을 살펴봄으로써, 기업 내 보안 위협으로 다시금 부가되고 있는 ARP Spoofing을 방어하는 최선의 전략에 대해 공유하도록 한다.

1. ARP Spoofing과 MITM 공격의 이해

먼저, ARP(Address Resolution Protocol)이 살펴보고, ARP의 취약점이 무엇이고, 이를 이용한 ARP Spoofing과 MITM (Man-In-The-Middle) 공격이 무엇인지에 대해 알아보기로 한다.

(1) ARP(Address Resolution Protocol)

동일한 LAN 환경에서, 특정 시스템과 통신하기 위해서는 해당시스템의 논리적인 IP 주소와 매칭되는 물리적인 MAC주소를 알아내야 한다. 이 때 사용되는 프로토콜이 ARP/RARP이다. ARP는 IP-to-MAC주소를 얻기 위한 프로토콜이고, RARP는 그와는 반대로 MAC-to-IP주소를 얻기 위한 프로토콜이다. 시스템 A가 동일 LAN 상의 시스템 B와 통신하기 위해서는 다음과 같은 절차를 거치게 된다.



[그림 4-1] 동일 LAN 상에서 ARP 통신

① 시스템 A는 통신하고자 시스템 B의 실제 MAC주소를 얻어 내기 위해 시스템 B의 IP 주소를 포함한 ARP 요청 메시지를 동일 LAN상에 Broadcast한다.

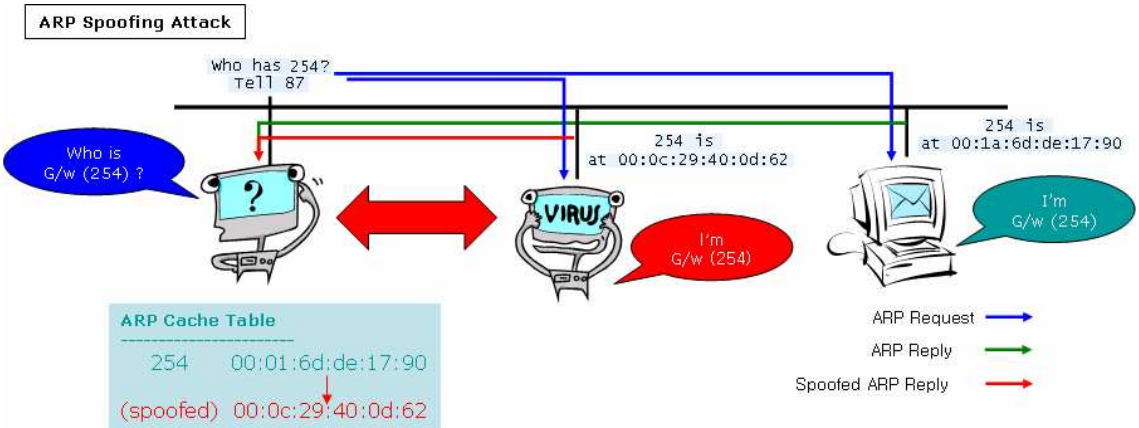
② 시스템 A의 ARP 요청메시지는 동일 LAN상의 모든 시스템 (시스템 B 포함)에게 전달되고, ARP 요청 메시지에 포함된 IP주소를 보고 자신의 IP주소와 일치하는 경우 요청자에게 ARP 응답메시지를 보낸다. 자신의 IP주소가 아닐 경우 ARP 요청메시지를 무시하게 된다. 시스템 A의 요청메시지에는 시스템 B가 응답시에 사용할 수 있도록 자신의 IP/MAC pair 정보가 담겨있다.

③ 시스템 B의 응답메시지를 수신한 시스템 A는 자신의 ARP Cache 테이블에 시스템 B의 IP/MAC pair 정보를 일정시간 동안 저장한 후 재사용하게 된다. ARP Cache Expired Time 이 지나면, 해당 엔트리는 자동적으로 삭제된다 (ARP Cache 만료시간은 OS마다 캐쉬 정보 사용 여부에 따라 다를 수 있다)

(2) ARP Spoofing 공격

ARP 프로토콜의 취약점은 ARP 요청/응답 메시지에 대한 확실한 인증 메커니즘이 없다는 데 발생하게 된다. 공격자(attacker)는 실제 존재하지 않는 MAC주소나 자신의 MAC주소를 이용하여 ARP 응답메시지를 조작하여 공격대상인 피해시스템(victim)에게 전송하게 된다. APR 응답메시지를 수신한 시스템은 ARP 응답메시지 만으로 실제 시스템에서 온 것인지 공격자가 조작하여 보낸 것인지 판단할 수가 없다. 따라서, 자신에게 도착한 모든 ARP 응답메시지 대해 어떠한 확인과정을 거치지 못한 체 무조건 받아들이게 되어 ARP Cache Poison 현상이 발생하게 된다.

ARP Spoofing 공격 절차는 다음과 같다.



[그림 4-2] ARP spoofing 과정.

① 공격자 C는 시스템 A에게 유입되는 모든 데이터 정보를 알고 싶어한다.

② 공격자 C는 시스템 A에 대한 ARP 응답요청이 있는 경우 요청자에게 시스템 A를 대신하여 시스템 A의 주소와 공격자 C의 MAC주소를 이용하여 동일 LAN 상의 모든 시

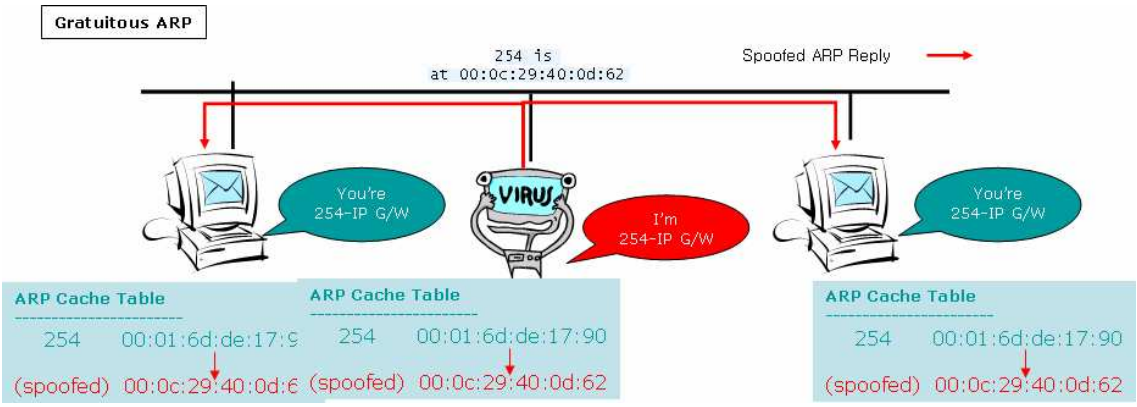
스템에게 ARP Reply 응답한다. (공격자는 시스템 A가 원활하게 ARP 응답을 하지 못하도록 DoS 공격을 수행하기도 한다)

③ 동일 LAN상의 모든 다른 시스템의 ARP Cache 테이블에는 시스템 A에 대해 공격자 C의 MAC주소가 매핑되어 향후 시스템 A로 유입되는 모든 데이터 정보는 공격자 C에게 전달된다.

④ 공격자 C는 주기적으로 자신의 조작된 ARP 응답메시지를 보내어 시스템들의 변조된 ARP Cache 테이블이 계속적으로 유지될 수 있도록 한다.

Gratuitous ARP

ARP에는 Gratuitous ARP라는 기능이 있다. ARP 요청메시지 없이도 ARP 응답메시지 형태를 보낼 수 있고, 일반적인 ARP 응답 메시지와는 다르게 ARP 응답메시지를 Broadcast하게 된다. 이 Gratuitous ARP 메시지를 수신한 동일 LAN 상의 모든 다른 시스템은 자신의 ARP 테이블에 해당 IP/MAC pair 정보를 저장하게 된다. 이러한 기능은 본래 자신의 IP/MAC정보를 동일 LAN 상의 시스템에 알리기 위한 용도로도 사용되고 있으나, 동일 LAN 상의 모든 시스템에 거짓된 APR Cache Poison을 위해서 활용되기도 한다.



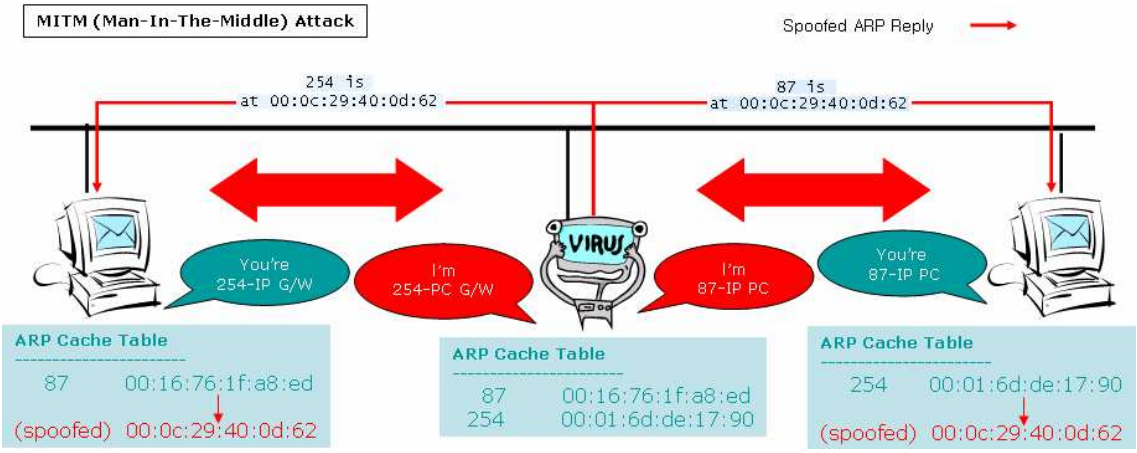
[그림 4-3] Gratuituos ARP 공격 과정

이러한 ARP Spoofing 공격 패킷의 특징은 주기적으로 반복된다는 데에 있다. Ethereal 등을 이용한 네트워크 패킷 모니터링시, ARP 요청 없이 반복되는 ARP 응답 메시지에 대해서는 한번쯤은 의심할 필요가 있다.

(3) Man-In-The-Middle 공격

ARP Spoofing 기법은 일반적으로 MITM(Man-In-The-Middle) 공격을 수반하여 동일 LAN 상에서 공격대상 시스템에 오고 가는 통신 내용을 스니핑하기 위한 목적으로 악용되는 것이 가장 일반적이다. MITM공격을 이용해서 스니핑 뿐만 아니라 데이터 변조 과정이 충분히 가

능하고, 암호화 통신 사이에서 위치하여 평문화된 내용의 정보를 가로챌 수도 있다.



[그림 4-4] 공격자 C가 MITM 공격을 수행하는 과정

ARP Spoofing을 이용한 MITM 공격 절차는 다음과 같다.

① 공격자 C는 시스템 A와 시스템 B의 IP/MAC pair를 확보한다. 공격자는 시스템 A와 B사이에서 정상적인 통신을 수행하게 된다.

② ARP Spoofing을 이용한 MITM 공격을 수행한다. (시스템A ← 공격자C → 시스템B)
- 시스템 A에게는 시스템 B의 IP주소와 공격자 자신의 MAC주소로 위조하여 전달
- 시스템 B에게는 시스템 A의 IP주소와 공격자 자신의 MAC주소로 위조하여 전달

③ 시스템 A, B의 ARP Cache 테이블에는 시스템 A, B의 IP주소와 함께 공격자의 MAC 정보가 저장된다.

④ 공격자 C는 2의 과정을 일정시간마다 반복적으로 수행하여 시스템 A, B의 변조된 ARP 정보를 유지한다.

⑤ 공격자 C는 시스템 A와 B의 사이에 위치하여 해당 시스템 간의 모든 네트워크 트래픽을 스니핑 및 변조를 통해 2차 공격을 감행한다.
- VoIP 도청: 데이터 스니핑 후 음성트래픽 재생
- 파밍(Pharming)공격: DNS 요청/응답 변조
- 개인정보 탈취: 데이터 스니핑 후 로그 분석
- 악성코드 유포: http redirection 혹은 iframe injection 수행

최근에는 이러한 MITM 공격 기법이 악의적인 목적이 아닌 NAC(Network Access Control) 솔루션 구현이나 호텔 룸에서의 인터넷 환경 제공시 사용되기도 한다.

2. ARP Spoofing을 이용한 공격 사례

본 장에서는 앞서 설명한 ARP Spoofing과 MITM 공격이 실제 필드에서 어떻게 활용되고

있는 지 사례를 통해 살펴보도록 한다.

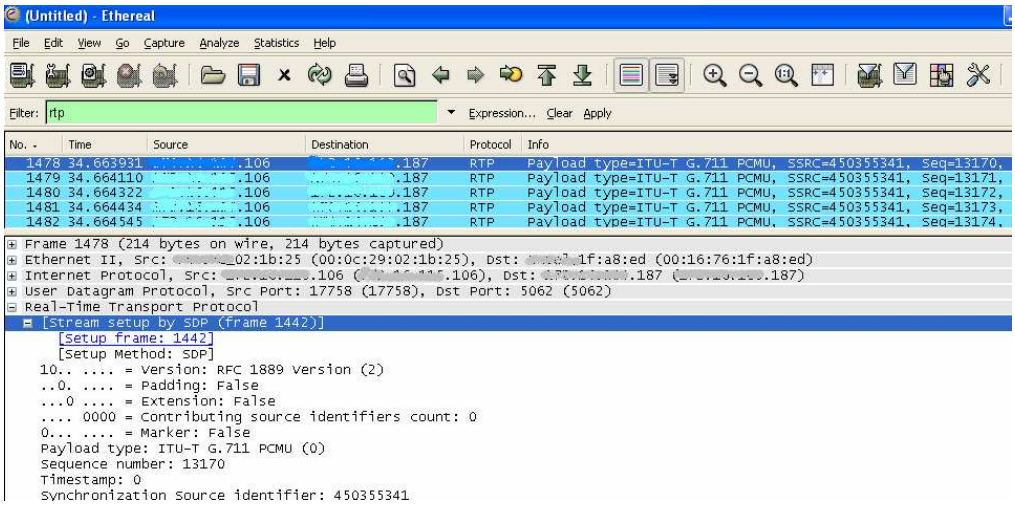
(1) ARP Spoofing을 이용한 VoIP 도청 가능성

VoIP 서비스가 아직 국내 시장에서는 크게 활성화되고 있지는 못하지만, 내년 번호이동제도의 도입 등으로 인해 활성화가 기대되고 있다. 기존 PSTN에서는 공격자가 전화 내용을 도청하기 위해서는 교환기 등에 물리적으로 접근하여야 하는 제약 사항이 있어 쉽지 않았던 것이 사실이다. 하지만 IP기반의 VoIP 인터넷전화 시대에는 이미 존재하는 IP 환경에서의 데이터 스니핑 도구를 통해 전화 내용에 보다 쉽게 접근할 수 있기 때문에 과거에 비해 그 위험성이 높다고 할 수 있다.

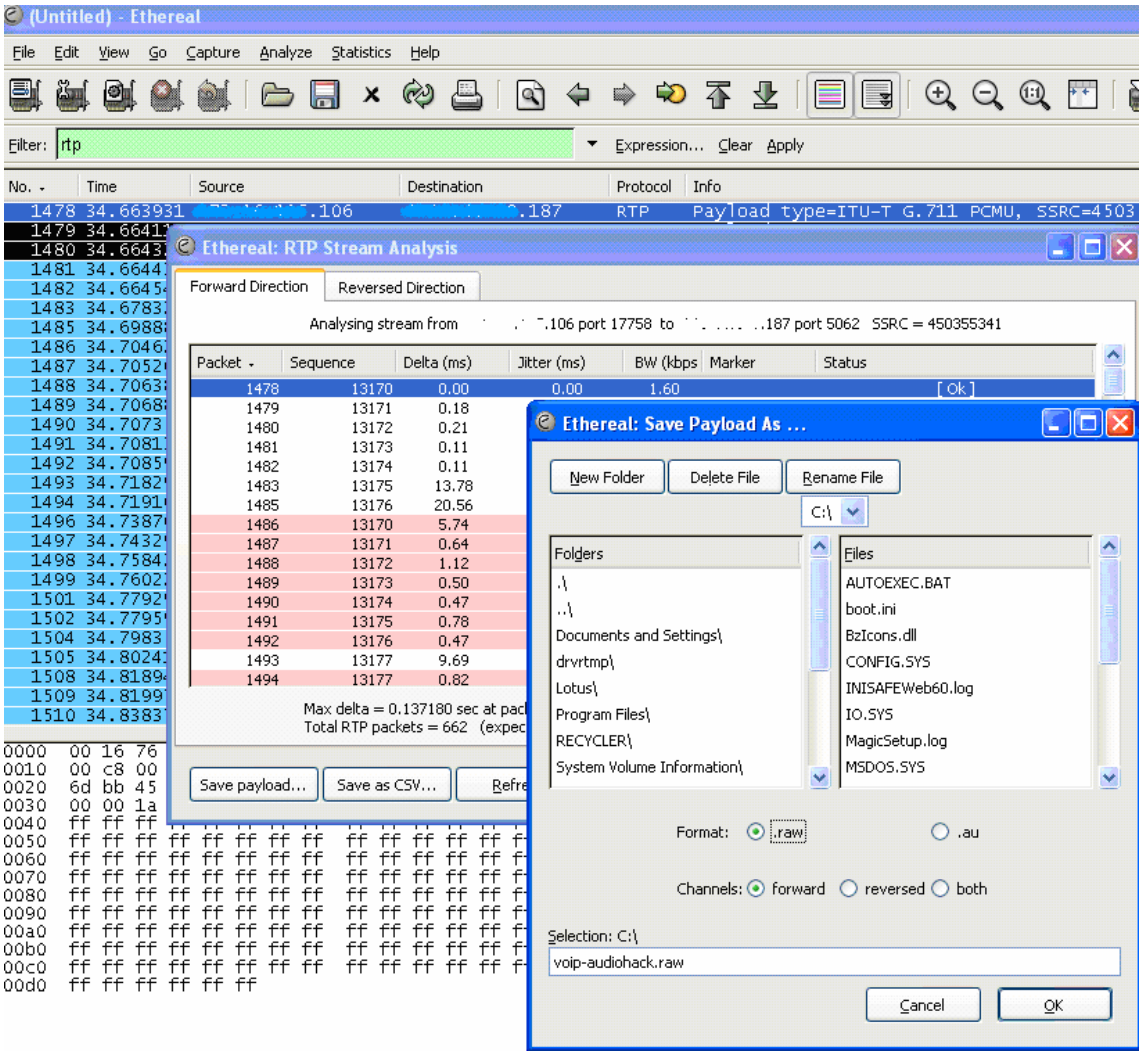
VoIP 데이터를 가로채기 위한 방법으로는 동일 네트워크 서브넷 상에서 VoIP 데이터를 스니핑하는 방법과 VoIP 소프트폰이 동작하고 있는 시스템을 해킹하여 데이터를 가로채는 방법 등이 가능하다. 본 문서에서는 ARP Spoofing을 이용한 VoIP 데이터 스니핑 공격에 대해서 언급하고자 한다. VoIP 도청을 위해서 반드시 VoIP 전용 공격도구가 필요한 것이 아니고, Ethereal 등의 IP 기반의 데이터 스니핑 도구들을 이용해서도 충분히 가능하다. (하지만 VoIP 도청을 위해서는 스니핑하고자 하는 대상의 동일 네트워크 서브넷에 침투하는 것이 필요하지만, 서브넷 침투가 그리 쉬운 일은 아니다)

Ethereal을 이용한 VoIP 도청

Ethereal은 Network Protocol Analyzer로서 Packet Sniffing/Analyzer 기능을 가진 공개 소프트웨어다. 이 Ethereal를 이용하여 RTP Packet을 Sniffing하고 Packet을 분석할 수 있다. 또한 분석한 정보의 Payload를 저장하여 실제 통화내용을 도청할 수 있다.



[그림 4-5] RTP Packet을 Sniffing한 결과



[그림 4-6] RTP Packet을 분석하여 VoIP 미디어 내용을 저장하는 과정

[그림 4-6]에서와 같이 저장된 미디어 데이터는 미디어 플레이어로 재생하여 들을 수 있다.

Cain & Abel을 이용한 VoIP 도청

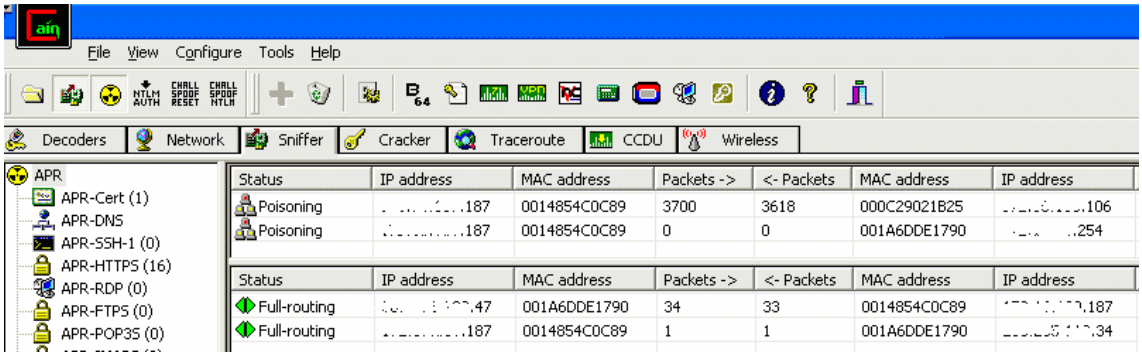
Ethereal와 달리, Cain & Abel은 ARP Poison Attack 을 통하여 Mac 주소를 Spoofing 하여, 스위치 환경의 네트워크 망에서도 네트워크 패킷 스니핑을 가능하게 해주어 MITM(Man-In-The-Middle) 공격을 통해 다양한 정보 수집에 악용될 수 있다. Cain & Albel 도구에는 손쉽게 VoIP 음성대화를 레코딩 해주는 기능이 있다. VoIP 서비스를 이용한 중요한 음성 대화시, 사용자의 사적 내용이나 주요 기업정보들이 노출될 가능성도 존재한다.

Cain & Albel 의 주요 기능은 아래와 같다.

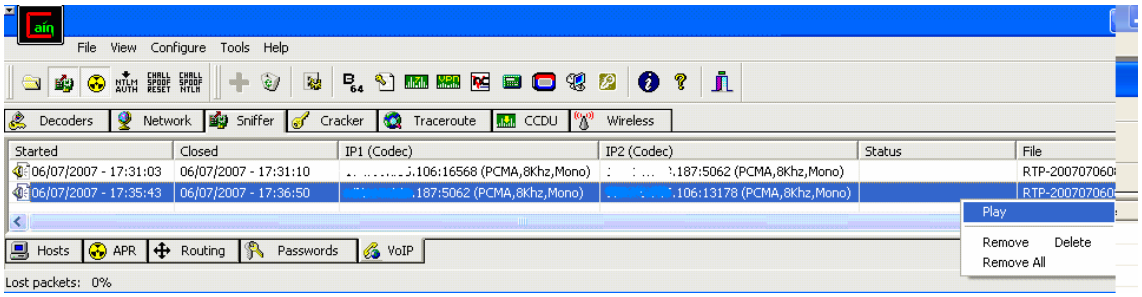
- 아웃룩, IE, MSN, Dialup, Cisco VPN Client/VNC Client 패스워드 디코더
- LSA Secrets 덤프

- APR(ARP Poison Routing)
- SID Scanner
- Network 정보수집
- 스니퍼 – 패스워드, hash 값 캡처, VoIP SIP/RTP 프로토콜 음성대화 캡처
- 라우팅 프로토콜 모니터
- Mac Address 스캐너
- 무선(Wiresless) 스캐너, WEP 크래커
- 패스워드 크래커 – 사전대입방식
- TCP/UDP 테이블 뷰어

우리가 주목해야 할 ARP Spoofing과 스니핑 기능(SIP/RTP 프로토콜 음성대화 캡처)을 살펴보도록 하자.



[그림 4-7] Cain & Abel을 통해 두 시스템 사이에서 MITM 공격



[그림 4-8] Cain & Abel은 VoIP 데이터를 레코딩

이러한 VoIP 데이터 등의 중요 정보가 유출되는 것을 방지하기 위해서는 VoIP 상에서 암호화 통신을 이용하는 방법 등이 필요하다.

(2) ARP Spoofing의 악성코드화 (공격도구 zxarps)

2007년 상반기에 보고된 공격도구 zxarps에는 다양한 기능이 포함되어 있다. 최근 발생되고 있는 주요 보안 공격 등을 한자리에 모아 놓았다고 할 수 있을 만큼, 원하는 공격 도구를 제

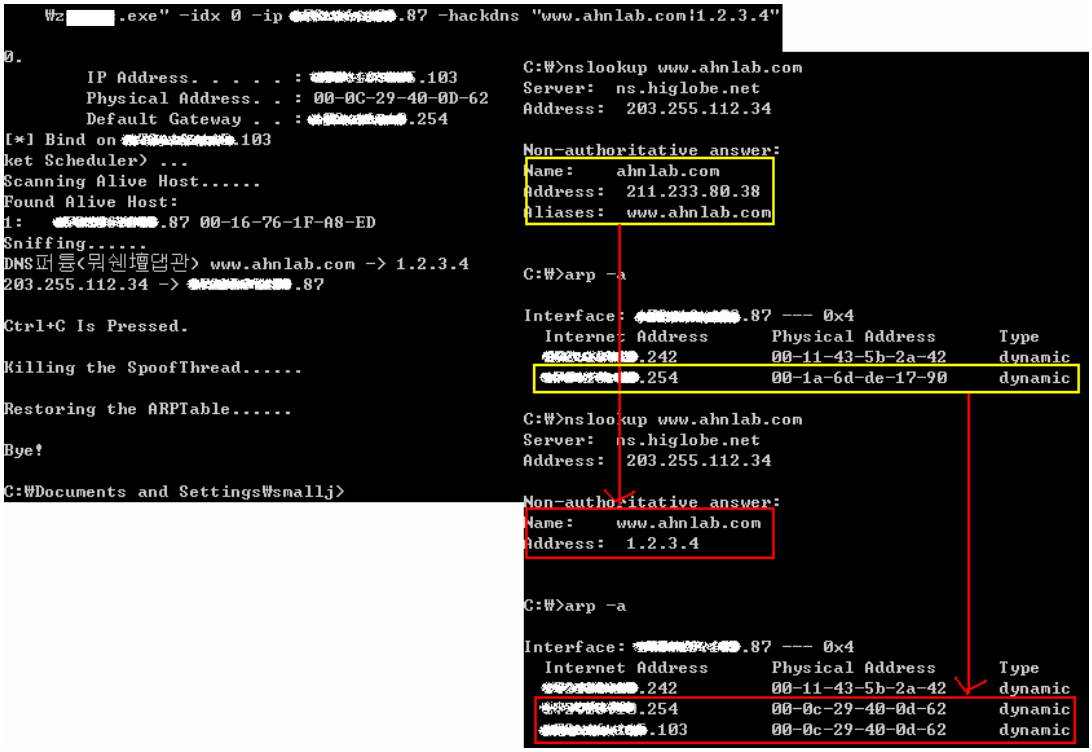
대로 모은 종합세트에 비유할 만하다. 공격도구 zxarps에 포함된 주요 공격 기능을 살펴보자. (공격도구 zxarps는 Win-Trojan/Snif 로 진단됨)

파밍(Pharming)공격: DNS 응답 변조

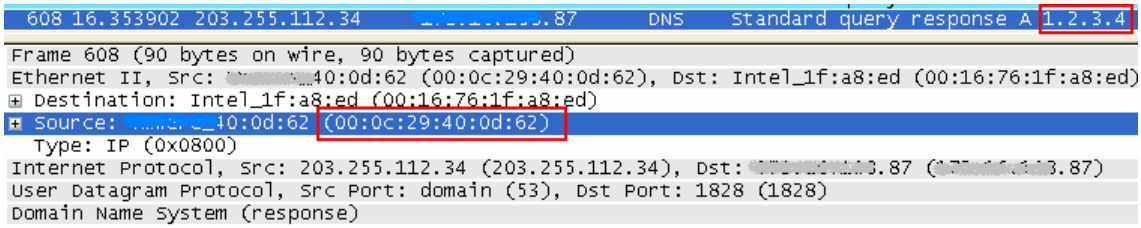
공격자는 DNS 요청에 대한 응답 결과를 쉽게 조작하여 피해자를 자신이 만들어둔 위조된 금융사이트로 유도할 수 있다. 자신도 모르게 입력된 피해자의 금융정보는 고스란히 공격자의 손에 쥐게 된다.

DNS 응답 변조

[그림 4-9]는 공격도구 zxarps를 이용한 웹사이트 도메인 www.ahnlab.com에 대한 DNS 응답결과를 변조하는 과정을 보여준다. 공격자(103번 PC, 00-0c-29-40-0d-62)가 피해시스템 (87번 PC)에서 www.ahnlab.com 웹사이트 도메인에 대해 DNS쿼리 요청/응답을 수행한 결과이다. 공격도구 zxarps를 통해 공격자가 원하는 대로 DNS 응답정보인 www.ahnlab.com의 IP주소가 211.233.80.38 → 1.2.3.4 변경되었음을 확인할 수 있다. 또한, 이 과정에서 ARP Spoofing을 이용하여 피해시스템의 게이트웨이의 MAC주소가 공격자 시스템의 MAC주소로 변경되었음을 확인할 수 있다. 피해시스템의 모든 네트워크 패킷은 공격자 시스템을 경유하여 전달되는 MITM(Man-In-The-Middle) 상태가 된다.



[그림 4-9] 공격도구 zxarps를 이용한 DNS 응답결과 변조 과정

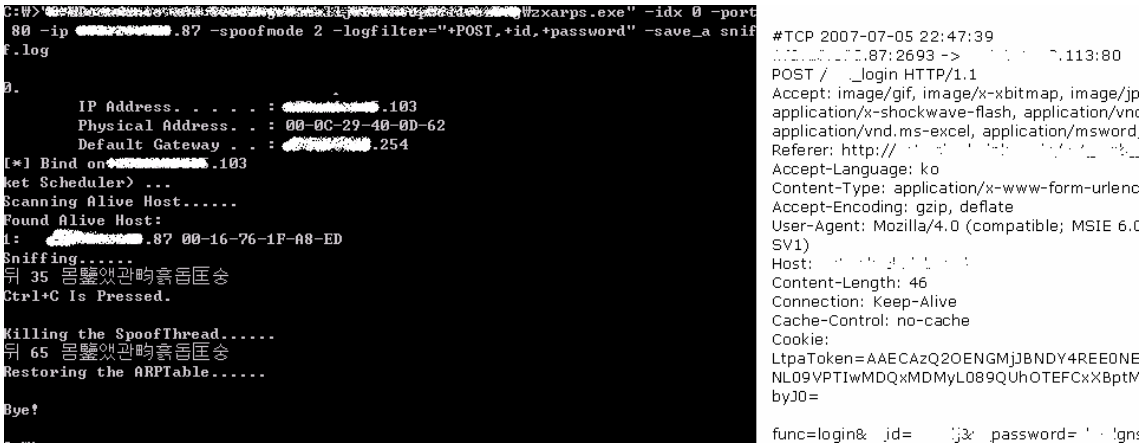


[그림 4-10] MITM 공격의 결과

MITM 공격으로 인해 DNS서버(203.255.112.34)→피해시스템(87번)으로의 DNS 응답 패킷이 공격시스템(103번, MAC: 00-0c-29-40-0d-62)을 경유하는 것을 알 수 있다.

개인정보 가로채기

스니핑하고 있는 피해시스템의 네트워크 트래픽 내부의 페이로드에 대해 가로채고자 하는 특정 문자열을 이용하여 스트링 매칭되는 트래픽 내용만을 추출한 후 그 결과를 로그파일로 저장하는 기능이 있다. 따라서, 암호화되지 않은 TELNET, FTP, Web 서비스의 사용자 로그인 계정 정보 등을 쉽게 가로챌 수 있다. 아래 [그림 4-11]에서와 같이 암호화하지 않은 HTTP 프로토콜과 취약한 인증 메카니즘으로 인해 사용자 정보가 그대로 노출되었다.



[그림 4-11] 공격도구 zxargs를 이용하여 로그인 사용자 정보를 가로채는 과정.

따라서, 인터넷서비스 제공자는 반드시 암호화 프로토콜(SSH, HTTPS 등)을 지원하고, 강력한 인증 메커니즘을 적용하여 단순한 스니핑 공격을 통해서는 고객의 중요 정보가 노출되지 않도록 노력해야 한다.

악성코드 유포를 위한 웹트래픽 변조: Iframe Injection

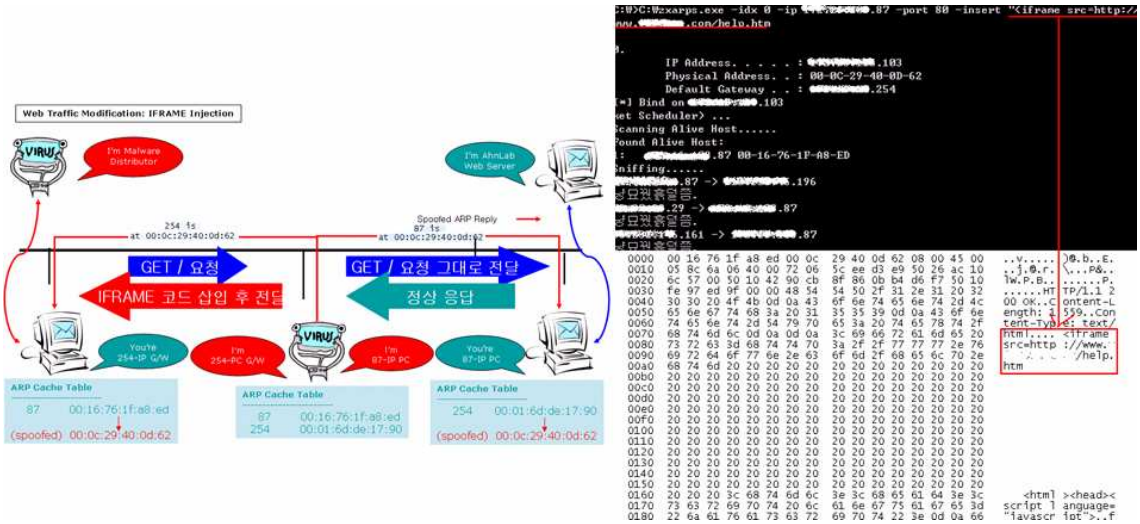
지금까지의 중국발 웹해킹은 자동화된 공격도구를 이용하여 SQL Injection 기법 등을 통해

인지도가 높지만(방문자수가 많은) 보안에 취약한 웹서버를 공격하여 악성코드가 유포되는 사이트로 유도하는 IFrame 코드를 삽입하는 공격 방식이 주류를 이루어왔다. 따라서, 웹 서비스 제공자는 이러한 웹 서버 공격을 효과적으로 차단할 목적으로 웹 방화벽 등을 도입하기도 한다.

2007년 상반기, 웹 플랫폼을 이용한 악성코드 유포 방식에 새로운 변화가 감지되었다. 다양한 보안 장비로 무장하고 있는 웹 서버 자체를 공격하기가 어려워짐에 따라, 웹서버와 웹 클라이언트 사이에 발생되는 웹 트래픽을 대상으로 한 새로운 공격이 시도되었다.

공격자는 피해시스템의 GET 요청에 대한 응답 메시지에 더하여 악성코드를 유포지로 유도하는 IFRAME 코드를 삽입하여 웹 클라이언트에게 전달한다. 웹 클라이언트는 IFRAME 코드에 의해 악성코드 유포지로 유도되고, 해당 사이트에 존재하는 웹 클라이언트 취약점 공격 코드(ANI 취약점, MS06-14 RDS 취약점 등)에 의해 감염되어 2차적인 공격 증상으로 이어지게 된다.

[그림 4-12]는 공격자 C가 동일 LAN 상의 피해시스템 A(87-IP PC)와 게이트웨이 (254-IP G/W)에 위치하여 피해시스템의 GET 요청 패킷의 응답 메시지에 악성코드 유포지로 유도하는 IFRAME 코드를 삽입하여 피해시스템 A에 전달하는 과정을 보여준다.



[그림 4-12] 트래픽에 Iframe 삽입

이는 악성코드 유포와 악성코드 감염에 활용되는 공격패턴이 빠르게 진화하고 있음을 실감하게 해 주는 좋은 사례라고 할 수 있다. 악성코드 감염에 사용되는 주요 웹 클라이언트 취약점은 제로데이 공격(0-day)보다는 아주 오래 전에 패치파일이 제공되는 것이 많으므로, 본인이 관리하는 시스템을 항상 최신의 보안 패치로 유지하는 것이 가장 중요하고, 데스크톱 보안 솔루션을 항상 최신의 것으로 업데이트 하여야 한다.

(3) ARP Spoofing 공격 대응 기술

아직까지 완벽한 ARP Spoofing 대응 기술은 존재하지 않는 것으로 알려져 있다. 아래에 소개된 여러 가지 기술을 혼합하여 ARP Spoofing 공격의 피해로부터 벗어날 수 있도록 적용하여야 한다.

Static ARP 정보 관리

변경 주기가 잦지 않은 주요 네트워크(게이트웨이) 및 시스템(서버) 등에 대한 IP/MAC주소 pair 정보에 대해서는 ARP 정보를 Static 하게 관리하여 ARP Spoofing에 의한 ARP Cache 테이블의 주요 정보의 변조를 미연에 방지한다. ARP Spoofing을 이용한 ARP Cache 테이블 변경에 가장 효과적인 대응 방법이면서, 네트워크 구조 변경이 잦은 기업에게는 일반적인 Dynamic 모드에 비해 유연하지 못하므로 적용시 주의가 필요하다.

각각의 시스템이 부팅할 때마다, 미리 정의된 static ARP table을 구성하도록 한다. 동일한 LAN상의 중요 시스템(스위치, 게이트웨이 등)에 대한 static ARP을 목록화하여 관리한다. 시스템의 수가 적고 변화가 크지 않은 소규모 기업에 적당한 대응 기술로서 시스템의 정상적인 IP/MAC주소 pair 정보의 추가/변경/삭제에 대한 static ARP table 세심한 관리가 요구된다.

다음과 같이 시스템의 arp 명령어의 '-s' 옵션을 사용하여, static ARP 정보를 등록할 수 있다.

```
C:\>arp -a
    Internet Address      Physical Address      Type
    xxx.xxx.xxx.254       00-xx-6d-xx-17-xx     dynamic

C:\>arp -s xxx.xxx.xxx.254 00-xx-6d-xx-17-xx

C:\>arp -a
    Internet Address      Physical Address      Type
    xxx.xxx.xxx.254       00-xx-6d-xx-17-xx     static
```

Switch Port Security

스위치에서 Port Security 기능이 제공될 경우, Mac Flooding이나 MAC Spoofing 등의 공격을 최소화할 수 있다. 스위치 포트마다 최대 허용 가능한 MAC주소 설정할 수 있다. 스위치 포트에 하나 이상의 MAC 정보가 매핑되는 경우 해당 포트의 기능을 차단할 수도 있게 된다.

또한, 특정 스위치 포트마다 접속을 허용하거나 차단할 static MAC 주소를 미리 설정해둔다. 이러한 기능을 통해 공격자가 피해시스템(victim)의 IP주소를 이용하여 자신의 MAC 주소가 스위치의 CAM(Content Addressable Memory) table에 등록되는 것을 방지할 수 있다.

예. Cisco Switch 설정의 예

```
Switch(config)# interface fastethernet 5/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security maximum 5 -> 최대 허용 MAC 주소
Switch(config-if)# switchport port-security mac-address 1000.2000.3000 -> 허용 MAC 주소
Switch(config-if)# switchport port-security violation [protect/restrict/shutdown] -> 규칙위반시 Action
```

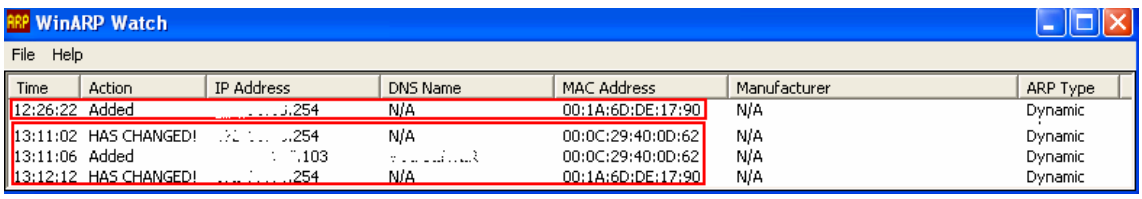
ARP 모니터링 도구 도입

ARP Spoofing 공격을 직접적으로 차단할 수 있는 방법은 아니지만, ARP 모니터링을 통해 공격에 대한 탐지가 가능하다. 일반적으로 ARP 모니터링 도구들은 LAN상의 ARP 패킷들을 수집하여 IP/MAC pair 정보를 데이터베이스화한다. 모니터링 과정에서, ARP Cache 정보의 변경이 탐지되면, 시스템 화면 하단의 트레이 아이콘에 탐지 솔루션의 아이콘이 껌벅거리게 되거나(WinARPWatch), 관리자에게 notify가 가능하여 사후 조치가 가능할 수도 있다.

현재 많이 활용되고 있는 ARP 모니터링 도구는 다음과 같다.

- WinARPWatch 정보 - http://sid.rstack.org/arp-sk/
- arpwatch, http://www-nrg.ee.lbl.gov/
- ettercap의 arpcop plug-in

[그림 4-13]은 WinARPWatch를 이용하여 ARP Spoofing공격을 탐지하는 과정으로 게이트웨이(254번 IP) MAC주소가 변경(HAS CHANGED!)되었음을 탐지해냈고, 새롭게 추가된 공격시스템(103번 IP)와 일치하는 MAC주소(00:0c:29:40:0d:62)임을 알 수 있다.



[그림 4-13] WinARPWatch를 이용하여 ARP Spoofing공격을 탐지하는 과정.

비정상 ARP 패킷을 IDS 시스템을 통해 방어를 고려해볼 수도 있다. 잘 알려진 IDS 시스템의 하나인 snort에도 arpspoof preprocessor가 존재하여 arp spoofing 공격에 대한 탐지 기능을 제공하고 있다.

VLAN 관리

ARP Spoofing 공격은 동일한 LAN 내의 환경에서만 가능한 공격이다. 기업 내부 네트워크의 동일한 LAN상에 존재하는 시스템이 많은 경우, 그만큼 ARP Spoofing 공격자에게 노출된 시스템도 많을 수 밖에 없다. 따라서, 기업 내의 특성에 맞게 시스템의 특성, 보유하고 있는 IP주소 범위 등에 따라 적절히 VLAN으로 나누어 최소한의 시스템이 동일한 VLAN 상에서 관리될 수 있도록 하는 것이 보안상으로도 성능면에서도 도움이 될 것이다.

ARP cache타임 최소화

시스템마다 ARP Cache 테이블의 엔트리를 유지하는 기간이 존재한다. 이 기간은 정보의 사용 여부에 따라 다를 수 있다. 이 ARP cache 유지 시간을 가능한 짧게 하여 ARP Spoofing에 의해 변조된 ARP Cache 내의 IP/MAC pair 정보가 오랫동안 지속되지 않도록 조치하는 것도 하나의 방법이 될 수 있다.

예. Sun Solaris의 ARP Cache 타임 최소화 설정

```
# ndd -set /dev/arp arp_cleanup_interval <time>
```

Secure-ARP (SARP) 설정

ARP 패킷의 보호를 위해 근본적으로 보안에 취약한 ARP 프로토콜 대신, PKI 방식을 이용한 Secure-ARP의 도입을 고려해볼 수 있다. 근본적으로 취약한 ARP 대신 패킷에 대해 인증 기능을 추가해볼 수 있다. 모든 device가 Secure-ARP 프로토콜을 지원해야 하고, 인증서 등의 관리 문제 등으로 실제 네트워크 환경에 적용하기 위해서는 상당한 어려움이 따르게 된다.