情 報 保 護 學 會 誌
第18卷 第3號, 2008. 6

악성 코드 동향과 그 미래 전망

장 영 준*, 차 민 석*, 정 진 성*, 조 시 행*

요 약

2008년으로 컴퓨터 바이러스가 제작된 지 이미 20년이라는 세월을 넘기게 되었다. 이 긴 시간 속에서 컴퓨터 바이러스는 파일 감염을 목적으로 하는 바이러스(Virus)로부터 네트워크를 통한 급속한 확산을 시도하는 웜(Worm) 그리고 데이터 유출과 파괴를 목적으로 하는 트로이목마(Trojan Horse)로 발달해왔다. 최근에는 컴퓨터 사용자의 정보를 무단으로 유출하기 위한 스파이웨어(Spyware)에 이르기까지 다양한 형태로 변화를 이룩해 왔다. 이러한 다양한 형태로의 변화가 진행되는 동안에도 컴퓨터 과학의 발달에 따른 새로운 기술들을 흡수하여 더욱더 정교하고 파괴적인 기능들로 발전을 이루게 되었다. 다양한 형태와 기술적인 발전을 거듭한 악성 코드(Malicious Code)는 컴퓨터 운영체제, 네트워크의 발달로 이룩된 컴퓨터 과학사와 함께 하였다고 볼 수 있다.

악성 코드의 발전은 해가 갈수록 수치적인 면에서는 증가 추세를 이루고 있으며 기술적인 면에서도 더욱더 위험성을 더해 가고 있으며 그 제작 목적 또한 전통적인 기술력 과시에서 금전적인 이익을 취하기 위한 도구로 전락하고 있다. 이렇게 제작 목적의 변질로 인해 악성 코드는 인터넷 공간에서 사이버 범죄를 발생시키는 원인 중 하나로 변모하게 되었다.

본 논문에서는 이러한 발전적인 형태를 띠고 있는 악성 코드에 대해서 최근 동향을 바탕으로 어떠한 악성코드와 스파이웨어의 형태가 발견되고 있는지 그리고 최근 발견되고 있는 악성코드에서 사용되는 소프트웨어 취약점들을 살펴보고자 한다. 그리고 이러한 악성코드의 형태에 따라 향후 발생할 수 있는 새로운 악성 코드의 위협 형태도 다루어 보고자 한다.

Ⅰ. 서 론

최근 안철수연구소로 접수되는 악성 코드들을 살펴보면 양적인 면과 질적인 면에서 크게 변화하고 있다. 특히 양적인 면에서는 예년과 비교해 3 ~ 4배를 훌쩍 뛰어 넘는 수치를 기록하고 있다. 이와 함께 질적인 측면에서도 다양한 공격 및 감염 기법들을 통하여 해킹과 악성 코드의 경계선 자체가 이미 허물어지게 되었다. 이러한 악성 코드의 2006년과 2007년 2년간의 동향들에 대해서 "2. 최근 악성 코드 동향"에서 다루어 보고자 한다. 또한 "3. 최근 스파이웨어 동향"에서는 최근 우리 사회에서 개인 정보 유출이라는 문제를 야기 시키고 있는 스파이웨어의 변화 추이를 살펴보고자 하며 소프트웨어와 운영체제의 취약점을 이용하는 악성 코드들을 통해 이들이 어떠한 취약점들을 통해서 감염이 되는지 어떠한 형태의 침해 사고들이 발생하고 있는지 "4. 시큐리티 동향"에서 살펴보고자 한다. 그리고 "5. 해외 악성코드 동향"에서는 극동 아시아권과 해외 다른 국가들의 악성 코드 동향이 한국과는 다른 어떠한 국지적인 양상을 띠고 있는지 살펴보며 마지막으로 이러한 종합적인 동향들을 통해서 향후 발생할 수 있는 악성 코드의 위협에는 어떠한 것들이 있는지 "6. 미래 전망"에서 다루어보고자 한다. 본 논문에서 다루지 않은 2008년 상반기 동향의 전반적인 흐름은 2007년 동향과 유사함을 미리 밝힌다.

Ⅱ. 최근 악성 코드 동향

2006년은 넷스카이(Win32/Netsky.worm), 베이글(Win32/Bagle.worm) 그리고 마이톱(Win32/Mytob.worm)과 같은 전자 메일의 첨부 파일로 전파되는 전통적인 매스 메일러(Mass Mailer) 웜들의 지속적인 강세와 함께 파일 감염을 노리는 바이럿(Win32/Virut) 바이러스의 등장과 함께 해당 바이러스에 의한 피해신고가 8월부터 12월까지 폭발적으로 증가하는 등 전체 악성 코드 피해 신고가 급증했던 한 해였다고 평가 할 수 있다.

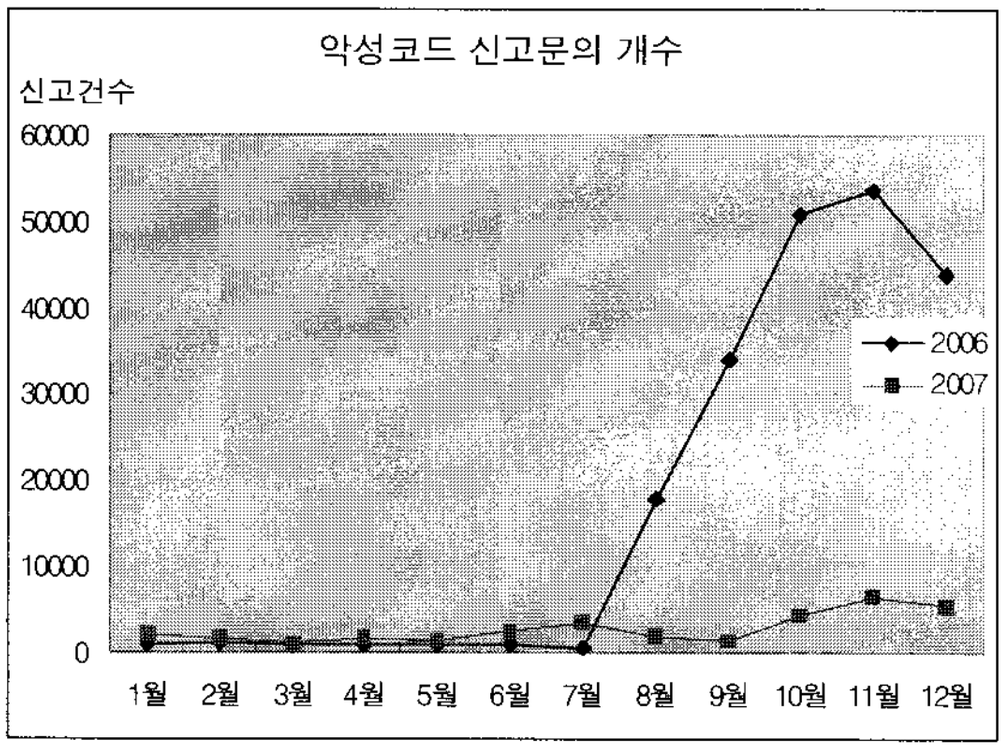
* 안철수연구소 ASEC(AhnLab Security E-response Center)팀, ({zhang95},{jackycha},{jsjung},{shcho}@ahnlab.com)

그러나 2007년에는 2006년까지만 해도 악성 코드 피해통계에서 항상 상위권을 점유했던 매스 메일러(Mass Mailer) 웜들의 전체적인 감소와 함께 바이럿(Win32/Virut) 바이러스의 피해 신고 감소 등으로 인해 전반적인 악성 코드 피해신고가 급감했던 한 해라고 볼 수 있다.

2.1 악성코드의 피해 통계

〔표 1〕 2006년과 2007년 국내 악성 코드 피해 건수

	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	합계
2006	914	1054	833	825	729	808	668	17755	84174	50771	53639	43902	206072[1]
2007	2057	1558	1111	1617	1284	2321	3536	1775	1305	4265	6454	5352	31653



〔그림 1〕 2006년과 2007년 악성 코드 신고 건수

[그림 1]을 통해서 2007년의 악성 코드 피해 건수가 2006년보다 감소했음을 확실히 알 수가 있다. 앞서 설명했듯이 바이럿(Win32/Virut) 바이러스의 피해 건수가 급감함에 따라 2007년 악성 코드 피해 건수도 2006년에 비해 감소하였다. 2006년과 2007년을 아울러서 가장 많은 악성 코드 피해 신고가 되었던 악성 코드들의 Top 20을 비교해 봄으로써 2006년까지 월별 악성 코드 피해 Top 10에서 전통적으로 강세를 보였던 매스 메일러(Mass Mailer)형의 웜들이 2007년 들어서 왜 몰락할 수밖에 없었는지에 대해서 알아보자.

[표 2]를 보면 2006년의 경우 바이럿(Win32/Virut)과 그의 변종인 바이럿(Win32/Virut.B) 그리고 일부 바이러스를 제외한 대부분이 매스 메일러(Mass Mailer) 웜들임을 알 수가 있는데 그 당시 제작자들 간의 자존심 싸움 및 제작 기술 과시로 인해 수많은 매스 메일러(Mass Mailer) 웜들이 제작됨으로 인해 2006년 악성

〔표 2〕 2006년과 2007년 악성 코드 TOP 20

2006 년		
순위	악성코드 명	건수
1	Win32/Virut	154,114
2	Win32/Virut.B	38,497
3	Win32/Netsky.worm.Gen	670
4	Win32/Bagle.worm.19666	551
5	Win32/Mytob.worm.Gen	537
6	Win32/Bagle.worm.19834	355
7	Win32/Perite	329
8	Win32/Bagle.worm.40668	278
9	Win32/Bagle.worm.84128	177
10	Win32/Netsky.worm.29696	165
11	Win32/Bagle.worm.88642	127
12	Win-Trojan/Xema.variant	83
13	Win32/Bagle.worm.95369	65
14	Win32/Tenga.3666	61
15	Win32/Mytob.worm.46766.C	58
16	Win32/Maslan.C	55
17	Dropper/Maslan.60926	52
18	Win32/Stration.worm.150844	45
19	Win-Trojan/Delphiexecute.21e64	39
20	Win32/Maslan.worm.63680	35

2007 년		
순위	악성코드 명	건수
1	Win-Trojan/Xema.variant	1448
2	Win32/Virut	351
3	Win32/IRCBot.worm.variant	341
4	Dropper/QQPass.23599.B	298
5	Dropper/QQPass.23599.D	293
6	Dropper/OnlineGameHack.23087	272
7	Win-Trojan/KorGameHack.17920.BR	272
8	Win-Trojan/KorGameHack.28624.AI	267
9	Win-Trojan/KorGameHack.14848.FO	195
10	Win-Trojan/KorGameHack.6480	149
11	Win-Trojan/Downloader.38400.I	141
12	Dropper/OnlineGameHack.15956	130
13	Win-Trojan/OnlineGameHack.15360.I	120
14	Win-Trojan/Downloader.169984.D	118
15	Win-Trojan/KorGameHack.19456.BM	113
16	Win-Trojan/KorGameHack.7295	102
17	Win-Trojan/KorGameHack.43072	96
18	Dropper/OnlineGameHack.29743	95
19	Win-Trojan/KorGameHack.12800.EI	88
20	Win-Trojan/KorGameHack.15064	88

코드 피해 Top 20의 대부분을 매스 메일러(Mass Mailer) 웜들이 장식하게 되었다.

하지만 2007년에는 바이럿(Win32/Virut) 바이러스만이 2007년 Top 20에서 2위로 그 명맥을 유지하고 있을 뿐 대부분이 정보 유출 목적과 연관성이 있는 트로이목마 계열의 악성 코드로 이는 2006년과 비교했을 때 확연하게 차이를 보이고 있다. 그 원인은 『**IT** 인프라가 사회전반에 미치는 영향과 그에 따른 악성 코드 제작자의 성향변화』로 요약할 수 있다. 불과 몇 년 전만 해도 IT인프라가 정치, 사회, 경제활동에 미치는 영향은 그다지 크지 않았으나 지금은 잘 발달된 IT 인프라를 기반으로 정치, 사회, 경제 활동이 행해지고 있기 때문에 악성 코드 제작자들도 상호간에 자존심 싸움 및 제작 기술 과시에서 탈피하여 약 3년 전부터 실리적인 금전적 이득을 취하기 위한 목적으로 이동하였으며 2007년에는 그 성향이 더욱 심화 되었다고 볼 수 있다.

[표 2]에 보인 2007년 악성 코드 피해 Top 20 악성 코드의 총 피해건수는 4,624 건으로 2007년 한 해 악성 코드 피해건수 30,996건에서 차지하는 비중이 2006년에 비하면 그다지 크진 않으나 이를 반대로 생각해보면 정보 유출과 연관성이 있는 트로이목마의 다양한 신종 및 변종이 양산되었다고 볼 수 있다.

따라서 2006년에 발생한 바이럿(Win32/Virut) 바이러스의 피해 신고를 제외한다면 2007년의 경우 피해신고가 급감한 것이 아니라 위에서 언급한 이유로 인해 오히려 2006년보다 악성 코드 피해신고가 급증했다고

〔표 3〕 2007년 악성 코드 유형별 현황

	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월
웜	109	228	200	259	127	299	994	145	82	75	98	124
트로이목마	771	1057	659	1093	866	1672	2343	615	782	891	1489	1596
백도어	28	91	45	27	31	84	97	9	4	2	9	4
스파이웨어	180	130	151	148	145	245	180	103	113	142	159	178
애드웨어	52	88	29	38	64	17	35	28	17	38	76	69
스니퍼	33	16	27	54	30	48	42	31	33	22	40	32

볼 수 있다.

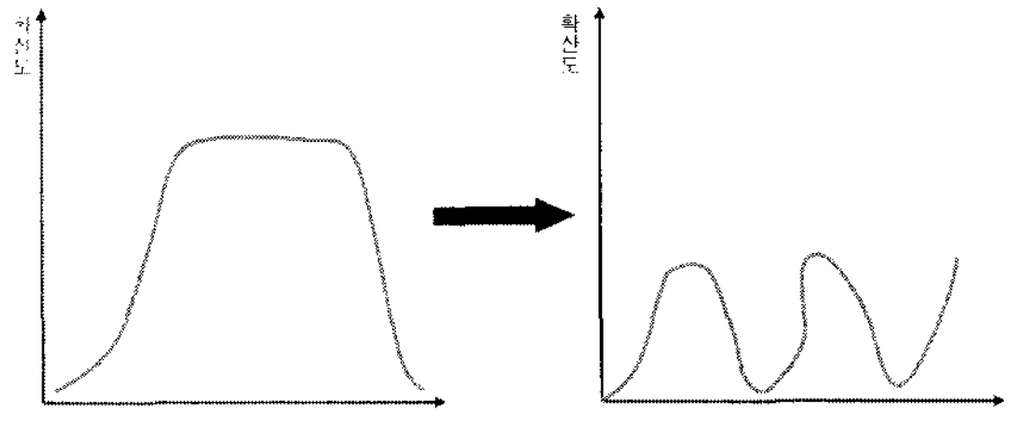
또한 [표 2], [표 3]을 통해서 국내와 외국의 악성 코드 동향에 대해서 어느 정도 파악해 볼 수 있다. 국내의 경우는2007년 악성 코드 피해 Top 20에 나열된 대부분의 악성 코드가 특정 온라인 게임의 사용자 정보를 유출해 금전적인 이득을 취하기 위한 목적을 가지고 있는 온라인 게임 정보 유출형 트로이목마라는 것이다.

온라인 게임 정보 유출형 트로이목마가 2007년 한 해 동안 많이 발견된 원인은 한국의 경우 다른 나라에 비해 잘 발달된 국내 IT 인프라를 기반으로 다양한 온라인 게임이 개발되었고 이들 온라인 게임에서 사용하는 아이템들이 실제로 고가에 거래되고 있기 때문이다. 그리고 온라인 게임 시장의 규모가 수천억 원 대에 이른다는 통계자료도 이를 뒷받침한다.

국내와는 다르게 외국의 경우는 여러 가지 제약 조건으로 인해 국내에 비해 온라인 게임 시장이 활성화되지 않은 관계로 주로 봇 넷(BotNet)을 이용한 스팸 메일(Spam Mail), 피싱(Phishing), 그리고 트로이목마를 이용한 온라인 뱅킹의 사용자 정보 탈취 등이 주류를 이루고 있어 확연한 차이를 보이고 있다. 하지만 국내외를 떠나 악성 코드 배포의 목적은 금전적인 이득을 취하기 위한다는 공통점이 있다는 것을 여러 사례를 통해서 알 수 있었다. 이로 인해 앞서 설명한 것처럼 IT 인프라가 사회전반에 미치는 영향과 그에 따른 악성 코드 제작자의 성향 변화로 인해 악성 코드의 라이프 사이클(Life Cycle) 또한 변해 왔다.

[그림 2]에서처럼 악성 코드의 라이프 사이클(Life Cycle)은 크게 보면 전자 메일, I.M(Instant Messenger), 취약점, P2P(Peer to Peer) 등을 통해서 확산을 시도하는 웜 형태의 악성 코드가 등장하면서 변화를 이루었으나, 웹 해킹과 악성 코드의 결합 및 유포가 이슈화 되면서 다시 한번 더 변화를 이루게 된다.

[그림 2]와 같이 악성 코드의 확산력은 떨어졌으나 국지성, 복합성, 물량화 등으로 인해 그래프상의 반복 주기가 짧아 졌음을 알 수가 있다. 이는 안티 바이러스

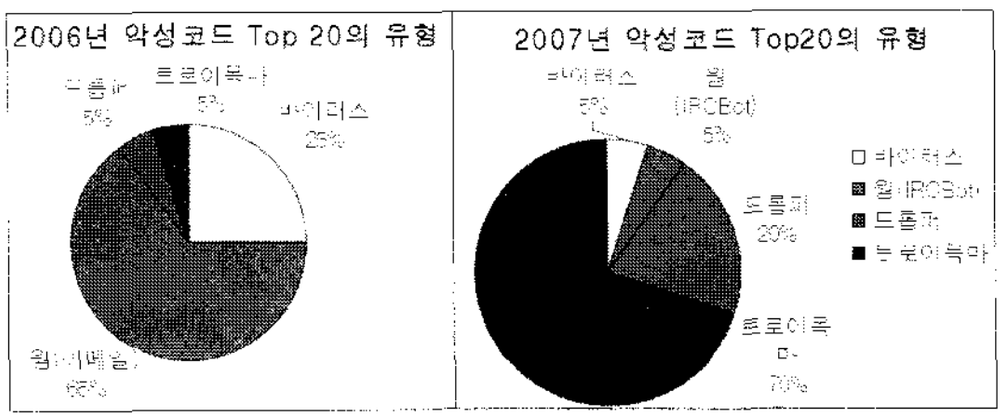


〔그림 2〕 악성 코드의 라이프 사이클(Life Cycle) 변화

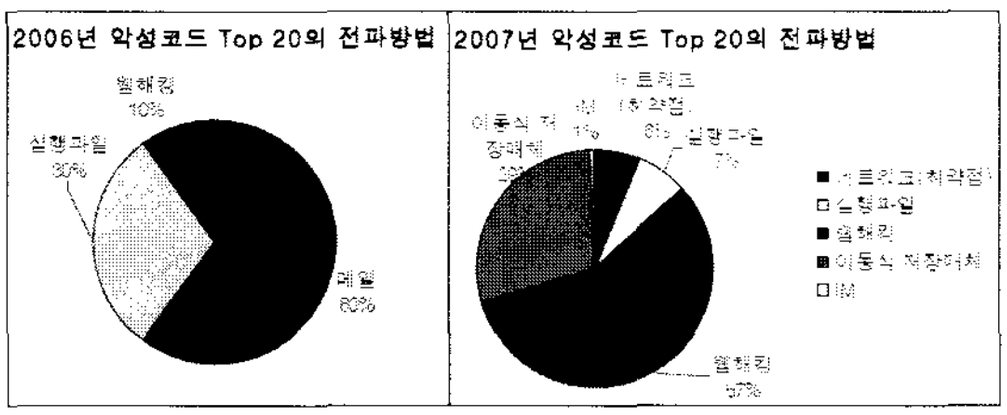
(Anti-Virus) 소프트웨어의 악성 코드 대응 기술력 향상 및 짧아진 스캐닝 엔진의 배포 주기 그리고 IPS (Intrusion Prevention System), UTM(Unified Threat Management)과 같은 네트워크 장비에서 안티 바이러스(Anti-Virus) 기술을 차용하여 대응 방법론에서 변화를 이룩했기 때문이다.

그리고 악성 코드 제작자들 역시 과거의 전통적인 기술력 과시에서 금전적인 이득을 위한 제작 목적의 변질로 인해 악성 코드의 광범위한 확산보다는 각국의 IT 환경에 맞는 국지적인 특징을 가진 악성 코드를 제작하게 되었다. 이러한 국지적인 특징에 맞는 악성 코드 제작으로 인해 다양하고 끊임없이 신종 및 변종 악성 코드를 제작하게 되었다. 이러한 현재의 악성 코드 제작 특성으로 인해 악성 코드의 라이프 사이클(Life Cycle) 주기가 짧아 졌다고 볼 수 있는 것이다. 그러한 실례로 2007년 악성 코드 피해 Top 20의 대부분을 차지하고 있는 온라인 게임 정보 유출형 트로이목마를 들 수 있다.

[그림 3]에 나타난 2006년과 2007년의 악성 코드 Top 20의 유형을 비교해 보더라도 2006년과 2007년이 확실히 다르다는 것을 알 수가 있다. 우선 2006년 악성 코드 Top 20의 유형에서 각각 65%, 25%를 점유했던 웜(이메일)과 바이러스의 경우, 2007년 악성 코드 Top 20에서는 웜(이메일)의 존재가 사라지면서 그 자리를 금전적인 이득을 목적으로 한 악성 코드가 대신하고 있다. 그리고 바이러스의 점유율은 5%로 급감한 반면 트



〔그림 3〕 2006년 vs. 2007년 악성 코드 Top 20의 유형



〔그림 4〕 2006년과 2007년 악성 코드 Top 20의 전파방법

로이목마와 드로퍼(Dropper)의 점유율은 각각 70%, 20%로 급증했다.

[그림 4] 역시 [그림 3]과 같이 악성 코드 Top 20의 전파방법에서 확연한 차이를 보이고 있다. [그림 4]에서 2007년 악성 코드 Top 20의 전파방법을 보면 웹을 통한 전파방법이 2006년에 비해서 급증했음을 알 수가 있다.

과거 네트워크가 발달하지 않은 1990년대의 경우 악성 코드 제작자들은 악성 코드의 빠른 전파를 위해 파일 감염 기능의 바이러스를 제작하여 플로피 디스크 등을 통해 전파하게 되었다. 그 이 후 1990년대 후반과 2000년대 들어 네트워크가 보편화되자 악성 코드 제작자들은 빠른 전파를 위한 수단으로 네트워크와 전자 메일을 통해 유포되는 웜을 제작하였고 현재 웹이 발달한 시대를 맞이한 이후 악성 코드 제작자들은 악성 코드의 배포 수단으로 웹 서비스를 제공하는 시스템의 취약점이나 취약한 웹 브라우저를 통해 트로이목마를 대규모로 유포하게 되었다.

이렇게 악성 코드 제작자들은 항상 시대의 흐름에 따라 자신이 제작한 악성 코드가 가장 빠르게 가장 많이 전파될 수 있는 도구를 선택하여 왔으며 이는 간편한 외장형 저장 장치가 악성 코드 전파의 도구로 사용되는 것으로 예를 들 수가 있다.

이렇게 웹을 통한 전파 방법은 자동화된 공격 툴에 의해 SQL Injection과 XSS(Cross Site Scripting) 그리고 웹 게시판에 존재하는 취약점 등을 통해서 취약한 웹 서버의 웹 페이지에 iframe을 삽입하거나 파일을 업로드 하는 경우가 대부분이다. 그리고 시스템 관리자로 하여금 쉽게 대응할 수 없도록 iframe을 조각내거나 정상 서비스되는 플래시 파일에 iframe을 삽입하는 경우도 있었다.

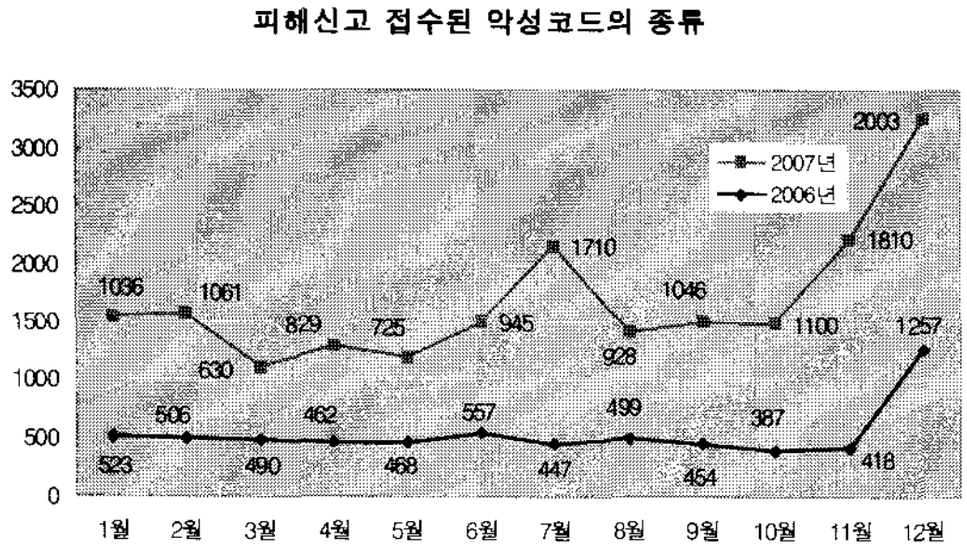
웹을 통해 유포되는 악성 코드가 클라이언트에서 감염되기 위해서 사용되는 취약점은 대부분 인터넷 익스플로러에 존재하는 것들로 다음과 같다.

- MS03-014 Outlook Express 누적 패치
- MS05-001 HTML 도움말의 취약점으로 인한 코드 실행 문제 (890175)
- MS05-026 HTML 도움말의 취약점으로 인한 원격 코드 실행 문제 (896358)
- MS06-001 그래픽 렌더링 엔진의 취약점으로 인한 원격 코드 실행 문제
- MS06-014 MDAC(Microsoft Data Access Components) 기능의 취약점으로 인한 원격 코드 실행 문제점 (911562)
- MS06-040 서버 서비스의 취약점으로 인한 원격 코드 실행 문제점(921883)
- MS06-046 HTML 도움말의 취약점으로 인한 원격 코드 실행 문제 (922616)
- MS06-057 Windows 탐색기의 취약점으로 인한 원격 코드 실행 문제점 (923191)
- MS07-017 GDI의 취약점으로 인한 원격 코드 실행 문제점 (925902)

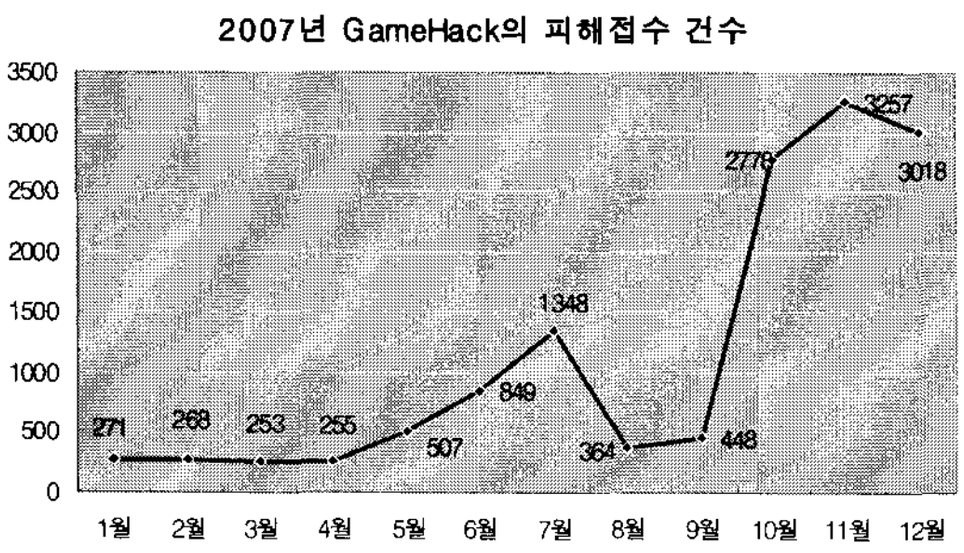
[그림 4]를 보면 2007년 악성 코드 Top 20의 전파방법 중에 이동식 저장매체가 눈에 띄는데 이는 이동식 저장매체의 보편화와 이동식 저장매체를 시스템에 접속할 경우 윈도우 운영체제에서 기본적으로 자동 실행된다는 점에 착안하여 악성 코드 유포의 중요한 수단으로 사용되었기 때문이다. 이러한 사례의 대표적인 악성 코드로는 오토런(Win32/Autorun.worm) 웜을 예로 들 수 있다.

인스턴트 메신저(Instant Messenger)를 통한 확산이 극히 미비하나 여전히 중요한 악성 코드의 전파 수단으로 사용되고 있다. 그리고 2007년 악성 코드 피해 Top 20의 순위에 들지는 못 했지만 젤라틴(Win32/Zhelatin.worm) 웜이 이메일을 통해 확산 되는 매스 메일러(Mass Mailer) 웜의 명맥을 겨우 유지하고 있으며 한동안 발견되지 않았으나 크리스마스와 신년 인사 등과 관련하여 다시 집중적으로 발견되고 있다.

[그림 5]를 보면 2006년보다 2007년도에 피해신고 접수된 악성 코드의 종류가 평균 2배 증가했음을 알 수 있는데 이에 대한 원인으로는 앞서 언급한 바와 같이 잘 구축된 IT인프라와 악성 코드 제작자들의 성향 변화로 요약할 수 있다. 그리고 이동식 디스크의 보편화 등으로 인해 전파 방법 면에서도 많은 변화가 있었기 때문이다.



〔그림 5〕 피해신고 접수된 악성 코드의 종류



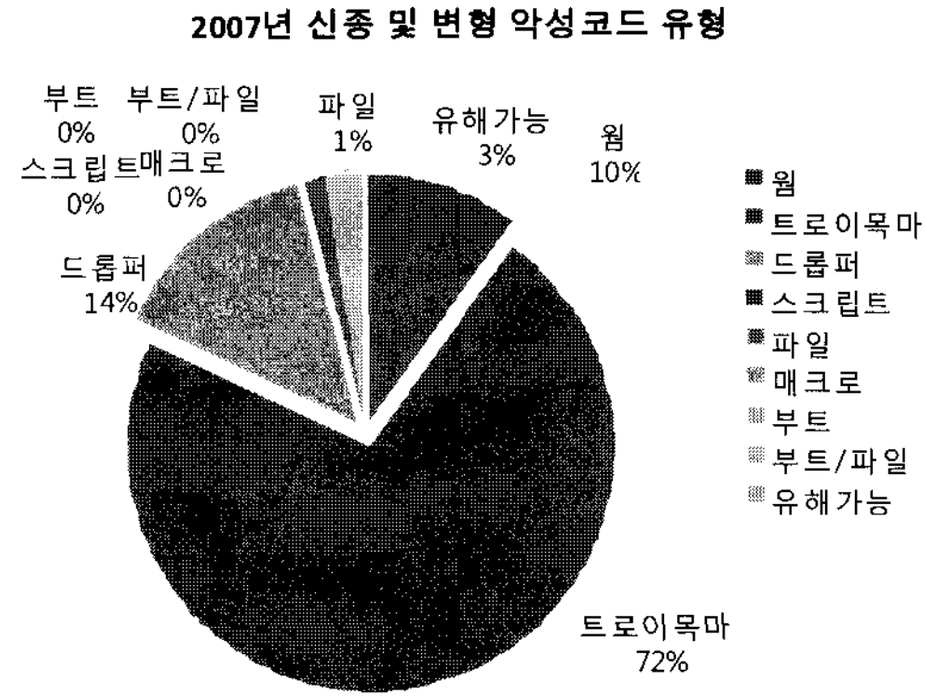
〔그림 6〕 온라인 게임 정보 유출 트로이목마의 피해접수 건수

[그림 6]을 보면 10월부터 12월 사이에 온라인 게임 정보 유출 트로이목마 및 드로퍼(Dropper)에 의한 피해가 집중적으로 접수되었음을 알 수가 있다. 이는 여전히 유효한 웹 해킹을 이용한 악성 코드 유포와 함께 ARP 스푸핑(ARP Spoofing) 그리고 이동식 저장 매체를 통한 확산 방법이 추가되면서 이를 통해 확산되는 악성 코드에 감염될 경우 또 다른 다수의 온라인 게임 정보 유출 트로이목마를 다운로드 하기 때문이다.

2.2 악성 코드의 신종 동향

2006년 안철수연구소는 클라이언트를 대상으로 감염 활동을 하는 악성 코드의 증가에 대해서 언급하였다. 대표적으로 실행파일을 감염시키는 전통적인 파일 바이러스와 온라인 게임 정보 유출 악성 코드가 그것이다. 2007년에도 이러한 악성 코드들의 동향은 전체적으로 크게 달라진 것은 없으나 패러다임은 서서히 변화하고 있다. 예로 작년에 기승을 부렸던 단순한 형태의 바이러스는 급격히 감소하고 진단 및 치료하기가 어렵고 복잡한 형태로 변모 하였다.

다음은 2007년 안철수연구소가 고객으로부터 접수한



〔그림 7〕 2007년 국내 발견 신종 및 변형 악성 코드 유형

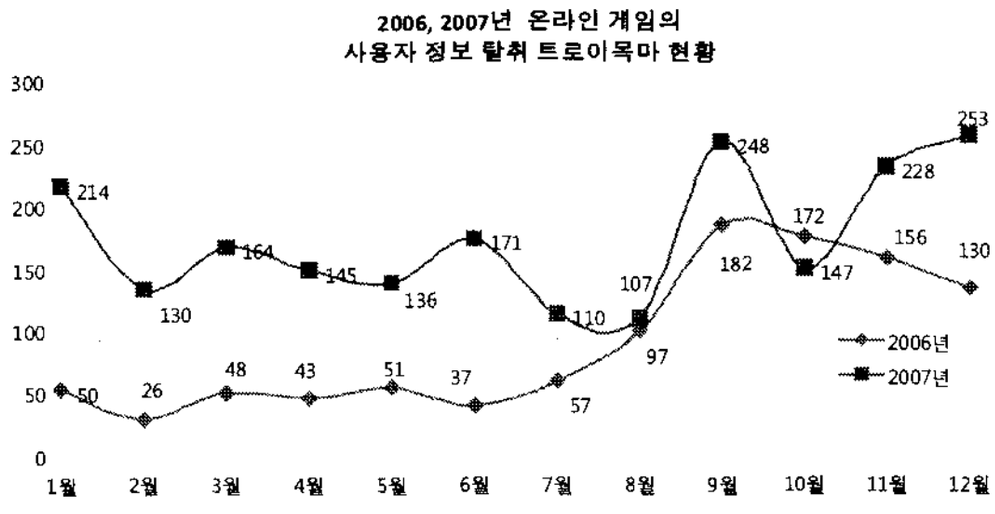
샘플에 대한 악성 코드 유형별 현황이다.

트로이목마의 비율이 매우 높으며, 온라인 게임 정보 유출 트로이목마의 비율이 높은 편이다. 온라인 게임 정보 유출 악성 코드의 대상은 국내 온라인 게임에서 중국이나 대만의 온라인 게임을 대상으로 하는 등 그 양상이 변화 하고 있다.

그러나 국내의 취약한 웹 서버들이 악성 코드를 다운로드 받을 수 있는 숙주로 사용되고 있는 것은 여전하다. 대상이 중국이나 대만의 현지 온라인 게임으로 변화했다는 것은 여러 가지 이유가 있겠지만 현지 온라인 게임 업체들의 게임 보안 솔루션을 도입하지 않았거나 또는 이를 우회 할 수 있도록 되어 있는 것으로 보인다.

다음은 해당 트로이목마 중에서 국내에 주로 이슈를 발생 하는 온라인 게임 정보 유출 트로이목마의 유형에 대하여 2006년 2007년의 수치를 비교해 보았다.

온라인 게임 정보 유출 트로이목마는 작년 동기 대비 96% 증가하였다. 국내의 경우 게임 보안 솔루션의 도입 또는 로그인 계정에 대한 보안 강화로 인하여 해당 악성 코드가 주춤 하고 있는 것으로 판단된다. 무엇보다



〔그림 8〕 2006년 및 2007년 온라인 게임 정보 유출 트로이목마 현황

도 중국 및 대만 현지의 온라인 게임 이용자 증가와 더불어 인터넷 사용자의 증가도 악성 코드 패러다임 변화에 어느 정도 기여 한 것으로 보인다.

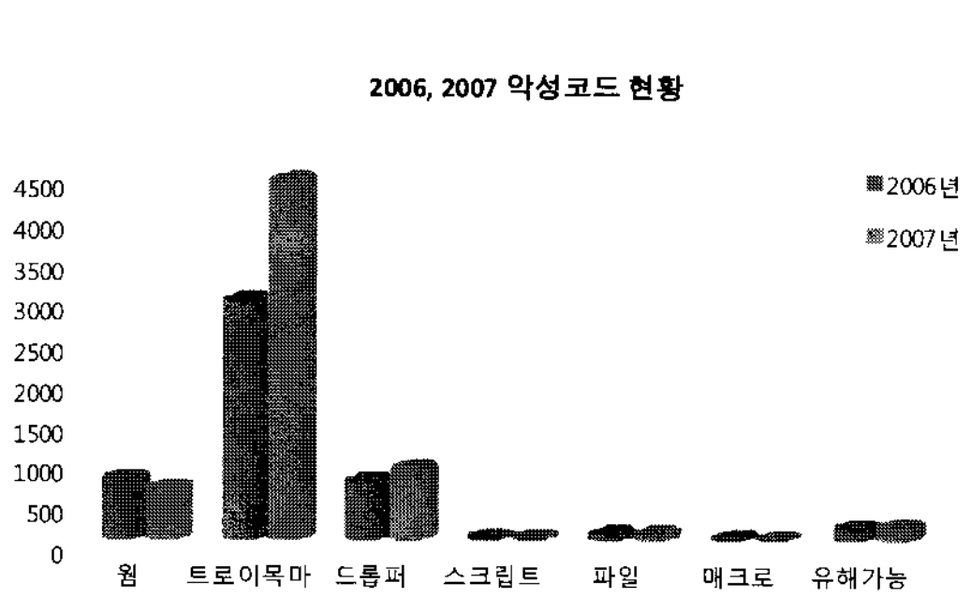
2007년 중국산 악성 코드의 또 다른 특징으로는 대량 다운로드 증상을 갖는 트로이목마와 ARP 스푸핑(ARP Spoofing)을 이용한 감염기법을 꼽을 수 있다. 대량 다운로더는 한번에 20개 이상의 악성 코드를 내려 받는다. 내려 받은 악성 코드는 다시 또 다른 악성 코드를 다운로드 한다. 이것은 대표적으로 온라인 게임 정보 유출 악성 코드를 설치하거나 다수의 애드웨어(Adware)를 설치하는 등 시스템을 복합적으로 감염시키고 있다. 이렇게 된 시스템은 마치 융단폭격을 맞은 것처럼 악성 코드에 의해 쑥대밭이 되어 버리고 이를 다시 복구하기에는 어렵고 긴 시간이 소요된다.

ARP 스푸핑(ARP Spoofing) 자체는 오래된 공격기법이지만 이를 악성 코드 전파에 접목시킨 것은 올해 큰 문제가 되었다. 해당 감염기법은 스푸핑(Spoofing)을 하는 시스템이 마치 게이트웨이(Gateway)가 되어 네트워크 트래픽을 가로채고 이를 다시 요청 시스템에 돌려줄 때 보안이 취약한 웹 브라우저를 사용하고 있다면 악성 코드에 감염 될 수 있다. 즉, 내가 감염됨으로써 주변의 다른 시스템들도 유해 사이트나 악성 코드가 숨겨진 웹 사이트를 방문하지 않아도 취약점이 있는 웹 브라우저를 사용하면 악성 코드에 감염 될 수 있다.

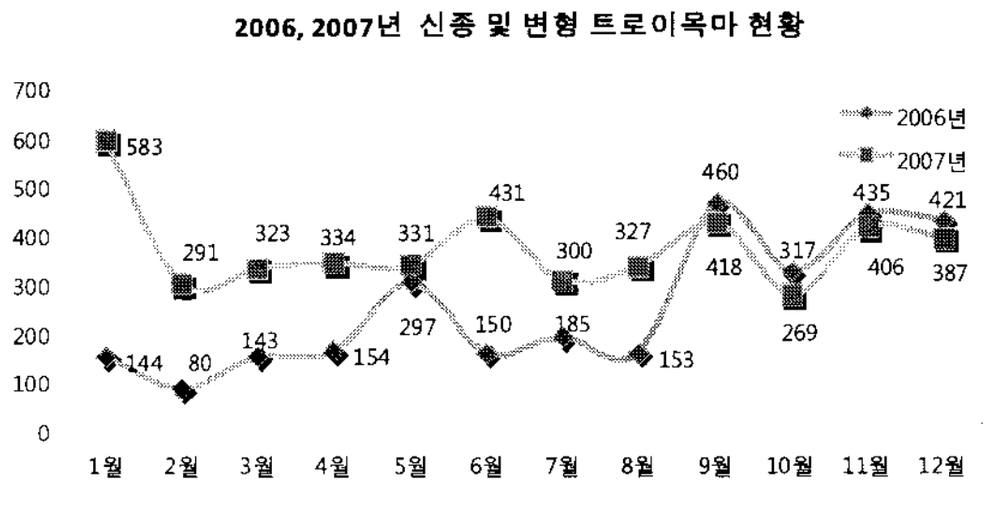
다음은 2006년과 2007년을 비교한 신종 및 변형 악성 코드 현황이다.

2007년은 2006년 대비 33% 의 악성 코드가 증가하였다. 많이 증가한 악성 코드는 트로이목마와 드로퍼(Dropper)로 각각50%, 22% 증가하였다.

2007년 발견된 악성 코드의 특징 중 하나가 악성 코드의 생존시간 고도화이다. 이를 세분화 한다면 은폐기법 및 자기보호 고도화로 나눌 수 있다.



〔그림 9〕 2006년 및 2007년 악성 코드 현황



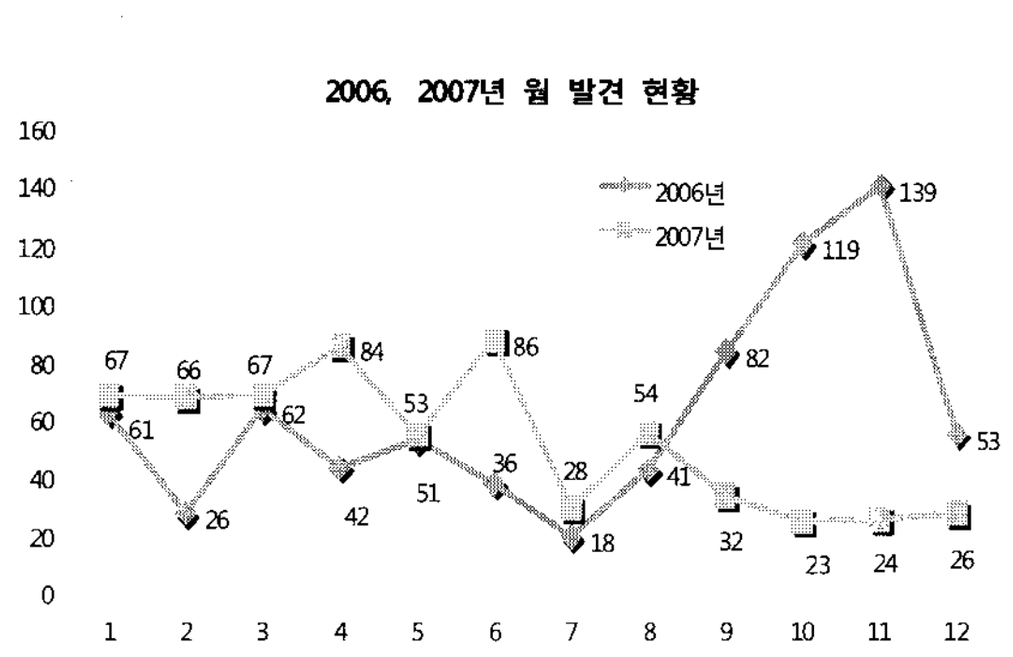
〔그림 10〕 2006년 및 2007년 신종 및 변형 트로이목마 발견 현황

은폐기법의 고도화는 이미 2006년부터 전망되었고, 2007년부터 현실화 되었다. 특히 시스템 파일 드라이버 또는 네트워크 드라이버 내 DRIVER OBJECT의 DISPATCHER TABLE 정보를 후킹(Hooking)하는 형태는 무력화하기 매우 어렵다.

이는 과거 악성 코드 제작자들이 자신의 기술력 과시를 위한 수단으로 은폐 기법을 사용하였으나 현재에는 악성 코드의 자기 보호 수단으로 자신이 발견 되어도 제거하지 못하게 하거나 마치 제거된 것처럼 속여 생존 시간을 극대화 한 것도 눈에 띈다.

악성 코드 유형 중 웜은 전년 대비 -13% 감소하였으며 그 중 가장 많이 감소된 웜은 악성 IRCBot 웜이다. 해당 웜의 감소 원인으로는 더 이상 원격에서 공격이 가능한 윈도우 취약점 보고가 없으며 C&C (Command & Controls)라고 불리는 공격자가 명령을 내리거나 제어 할 수 있는 호스트(Host)가 정보 보호 기관들의 노력으로 대부분 차단되는 등의 효과가 어느 정도 기인 한다고 생각 된다.

다음은 2006년과 2007년을 비교한 현황으로 특히 하반기 웜 유형의 수치가 감소하였다는 것을 알 수 있다.



〔그림 11〕 2006년 및 2007년 신종 및 변형 웜 발견 현황

물론 이 데이터는 국내 고객 접수 샘플만을 대상으로 하였으며 국내에 잘 보고 되지 않는 젤라틴(Win32/Zhelatin.worm) 웜 등은 국내 발견, 보고된 형태만 포함되었고 국외로부터 접수된 유형은 제외 하였다.

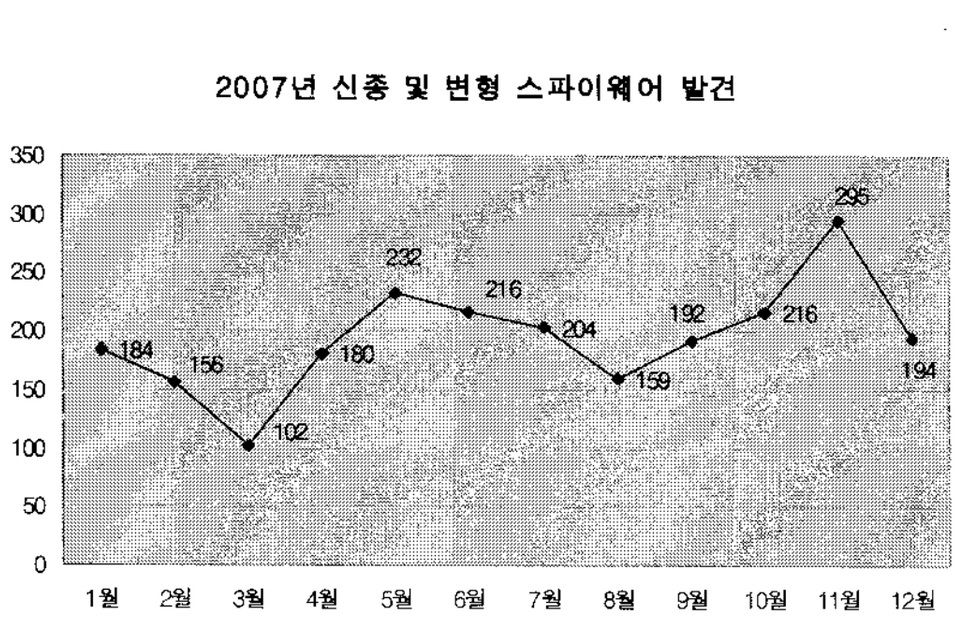
2007년은 특히 Autorun.inf 를 이용하여 자신을 자동으로 실행하는 형태의 악성 코드가 큰 폭으로 증가 하였다. 이중에서도 웜 유형은 오토런(Win32/Autorun.worm) 웜으로 명명 되었는데 새로운 유형으로 자리매김 하였다. 대표적으로 이동식 저장장치를 노리고 있으며, 이는 마치 과거에 플로피 디스켓에 부트 바이러스가 감염되는 것과 유사하다. 더 위험한 것은 윈도우 운영체제에서 이동식 저장장치로 인식되는 모든 장치가 감염대상이 될 수 있어 매우 위험하다. 이 악성 코드는 윈도우의 자동실행기능의 허점을 이용한 것이며 근래의 중국산 악성 코드 대부분은 이 증상을 포함하여 자신의 감염대상을 넓히려 하고 있다.

Ⅲ. 최근 스파이웨어 동향

3.1 스파이웨어의 신종 및 변형 동향

〔표 4〕 2007년 신종 및 변형 스파이웨어 발견 증감 현황

	스파이웨어	애드웨어	트랩퍼	다운로더	다이얼러	웜/바이러스	히스톨로잉	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
7월	63	50	17	65	4	5	0	0	0	204
8월	64	31	6	52	4	2	0	0	0	159
9월	91	37	12	40	6	6	0	0	0	192
10월	98	42	14	51	5	6	0	0	0	216
11월	99	61	15	112	3	5	0	0	0	295
12월	86	32	22	43	1	3	1	0	1	194



〔그림 12〕 2007년 신종 및 변형 스파이웨어 발견 증감 현황

[그림 12]는 2007년 월별 신종 및 변형 스파이웨어 발견 현황을 보여주는 그래프이다. 1월에서 12월까지 다소 기복을 보이는 가운데 전체적으로는 증가하는 모양을 볼 수 있다. 2007년 신종 및 변형 스파이웨어 발견 현황의 가장 뚜렷한 특징으로는 상반기에 온라인 게임 정보 유출의 스파이웨어가 많이 발견된 반면에 하반기로 접어들면서 국내에서 제작 배포되는 애드웨어의 수가 상대적으로 많이 늘어난 것을 들 수 있다.

2007년 상반기는 중국발 해킹에 의한 웹사이트 변조와 이를 통한 온라인 게임 정보 유출 목적의 스파이웨어 제작이 가장 활발한 시기였으나 하반기에 접어들면서 신종 및 변형의 제작 배포는 다소 감소하였으나 여전히 큰 피해를 입히고 있다. 이들 온라인게임 계정 유출 스파이웨어는 제작 초기에는 국내 유명 게임만을 대상으로 한 반면 최근에 발견되는 것들은 국내 온라인게임 뿐만 아니라 중국 및 대만의 유명 온라인게임 또한 대상으로 하고 있다. 그리고 보안 프로그램으로부터 진단되는 것을 회피하기 위해 다양한 변형이 양산되는 것도 이들 스파이웨어의 특징 볼 수 있다.

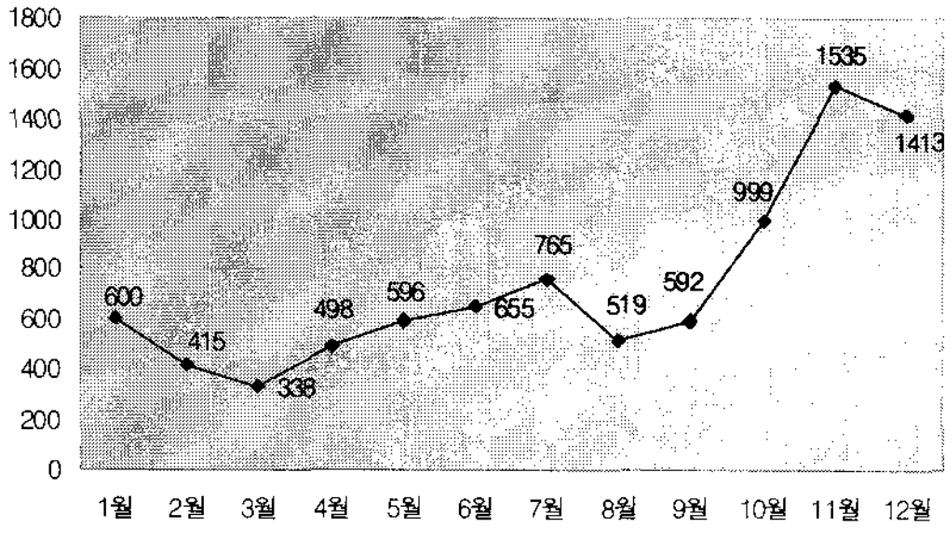
2007년 초까지 다소 주춤하던 국내 애드웨어 제작은 기존의 불특정 웹 사이트에서 Active X 컨트롤을 이용한 설치 방법에서 다운로더(Downloader)를 이용한 번들(Bundle) 설치 방법으로 변화함에 따라 하반기부터 증가하기 시작하였으며, 이들 애드웨어의 번들(Bundle) 설치만을 목적으로 하는 다운로더(Downloader)의 수치도 상반기에 비해 하반기에 증가한 양상을 보인다. 2007년 상반기까지는 2006년에 이어 허위 안티-스파이웨어의 제작 배포가 활발하였으며, 하반기에 접어들면서 유명 쇼핑몰과 제휴하여 적립금을 제공하는 리워드(Reward) 프로그램의 제작 배포가 활발하였다. 이들 리워드 프로그램은 툴바나 BHO 형태로 불특정 웹사이트에서 사용자 동의 없이ActiveX 컨트롤을 이용하여 설치되거나 다운로더에 의한 번들로 설치되며, 찾아가지 않는 적립금을 주요 수익원으로 한다. 리워드 프로그램과 함께 제휴 쇼핑몰의 바로가기를 생성하는 숏컷(Short-cut) 계열의 애드웨어 설치 피해도 많이 발견되었다.

3.2 스파이웨어의 피해 동향

[표 5]와 [그림 13]은 2007년 스파이웨어 피해신고 현황을 나타낸다. 9월까지 월 평균 500건 정도이던 피해신고 건수가 10월부터 급증하여 월평균 약 1300건의

〔표 5〕 2007년 스파이웨어 피해 현황

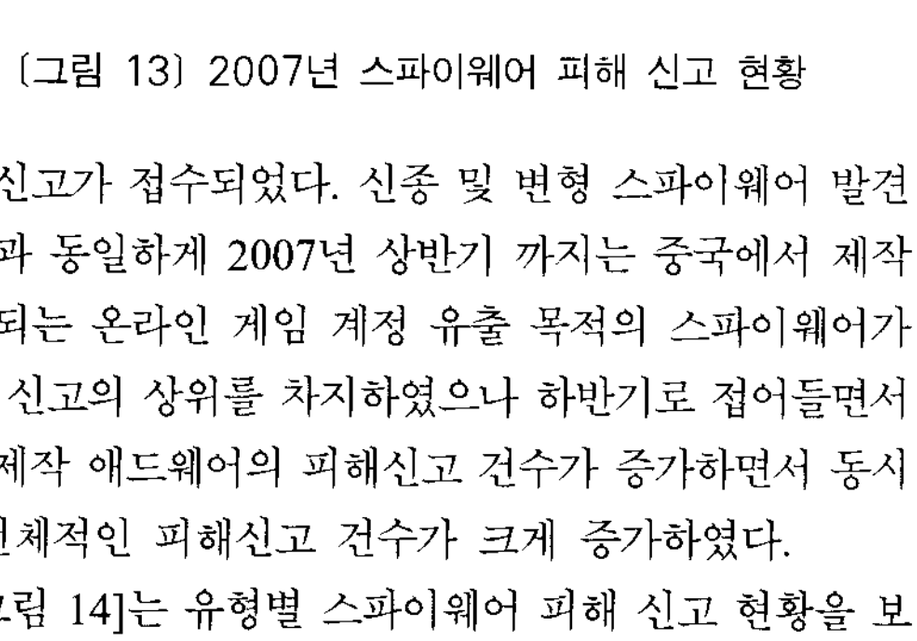
	스파이웨어	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
1월	247	137	93	96	18	11	2	0	1	600
2월	188	81	24	96	6	17	3	0	1	415
3월	123	100	25	69	1	14	6	0	0	338
4월	263	94	62	81	2	23	7	6	0	498
5월	320	109	22	122	3	10	2	8	0	596
6월	279	166	46	139	8	16	0	1	0	655
7월	261	183	55	232	10	20	8	1	0	765
8월	197	105	43	156	12	6	0	0	0	519
9월	291	119	35	132	9	7	0	0	0	592
10월	682	131	38	180	7	11	0	0	0	999
11월	480	354	147	525	8	25	1	0	0	1535
12월	325	446	184	461	4	8	4	0	1	1413



〔그림 13〕 2007년 스파이웨어 피해 신고 현황

피해신고가 접수되었다. 신종 및 변형 스파이웨어 발견 현황과 동일하게 2007년 상반기 까지는 중국에서 제작 배포되는 온라인 게임 계정 유출 목적의 스파이웨어가 피해 신고의 상위를 차지하였으나 하반기로 접어들면서 국내제작 애드웨어의 피해신고 건수가 증가하면서 동시에 전체적인 피해신고 건수가 크게 증가하였다.

[그림 14]는 유형별 스파이웨어 피해 신고 현황을 보여준다. 스파이웨어에 의한 피해 신고 건수가 가장 많았



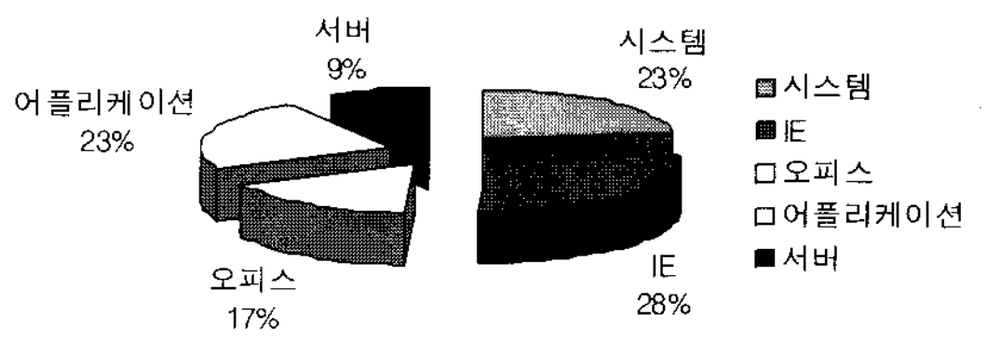
〔그림 14〕 2007년 유형별 스파이웨어 피해 현황

으며, 전체 피해신고의 약 40% 정도를 차지하고 있는 가운데 다운로더와 애드웨어가 그 다음으로 많은 피해를 입힌 것으로 나타났다. 온라인게임 계정 유출 스파이웨어의 피해는 2008년에도 지속될 것으로 생각되며, 2007년 하반기와 같은 추세가 지속된다면 2008년 상반기에는 국내 제작 애드웨어의 피해가 더욱 증가할 것으로 예상된다.

Ⅳ. 최근 시큐리티 동향

2006년의 경우 마이크로소프트사에서 발표한 보안 업데이트는 78개 이었던 것에 반해, 2007년 마이크로소프트사에서 발표한 보안 업데이트는 총 69개 이었다. 또한 긴급 보안 패치는 2006년에 49개였으나 2007년에는 43개로 감소하였다. 2007년 3월 마이크로소프트사에서 보안 패치를 발표하지 않아, 이러한 격차가 약간 벌어지게 된 것으로 파악된다.

2007년에 발표된 마이크로소프트사의 보안 패치를 분류 현황을 분석하면 아래와 같다.



〔그림 15〕 2007년 마이크로소프트 보안 패치 분류 현황

위의 [그림 15]를 보면, 2007년의 마이크로소프트 보안 패치의 주요 특징으로 어플리케이션 취약점을 들 수 있으며, 어플리케이션, 오피스와 인터넷 익스플로러에 관련된 보안패치가 전체 보안 패치 중 68%를 차지하고 있는 것을 알 수 있다. 특히 인터넷 익스플로러의 취약점이 전체 28%를 차지하고 있어 인터넷 익스플로러 취약점이 웹사이트 해킹 후에 악성 코드 유포에 많이 사용되고 있다. 2007년에 발표된 인터넷 익스플로러의 주요 취약점 목록을 살펴보면 아래와 같다.

인터넷 익스플로러 관련 보안 패치의 큰 특징은 하나의 패치 목록 안에 여러 개의 취약점에 대한 패치가 포함되어 있다. [표 6]의 목록 중에 악성 코드 유포에 자주 사용되는 취약점은 MS07-017 GDI ANI 파일 관련

〔표 6〕 2007년 인터넷 익스플로러 주요 취약점

MS07-004 벡터 표시 언어의 취약점으로 인한 원격 코드 실행 문제점(929969)
MS07-008 HTML 도움말 ActiveX 컨트롤의 취약점으로 인한 원격 코드 실행 문제점 (928843)
MS07-016 Internet Explorer 누적 보안 업데이트(928090)
MS07-017 GDI의 취약점으로 인한 원격 코드 실행 문제점 (925902)
MS07-027 Internet Explorer 누적 보안 업데이트 (931768)
MS07-033 Internet Explorer 누적 보안 업데이트(933566)
MS07-042 Microsoft XML Core Services의 취약점으로 인한 원격 코드 실행 문제점 (936227)
MS07-045 Internet Explorer 누적 보안 업데이트(937143)
MS07-057 Internet Explorer 누적 업데이트 (939653)
MS07-069 Internet Explorer 누적 업데이트(942615)

취약점으로, 현재까지도 많이 악용되고 있는 실정이다.

어플리케이션 관련 취약점들의 대부분은 사용자들이 많이 사용하는 프로그램을 대상으로 하고 있으며, 악성 코드 유포 및 특정 목적을 위한 공격에 사용되고 있다. 이 중에서 기업 및 특정 시스템들을 공격하는 데는 오피스 관련 취약점들이 많이 이용되고 있는 것으로 파악된다

2007년 발표된 전체 오피스 취약점 관련 주요 목록을 살펴보면 아래와 같다.

2007년 9월에 발표된 마이크로소프트 오피스 2003 서비스팩 3 가 출시된 이후에 오피스 관련 취약점 또한 점차 줄어들고 있으나, 11월에 마이크로소프트 Access 에서 사용하는 MDB 파일에 대한 공격 코드가 발표되어 계속적인 주의가 필요하다. 오피스 취약점들을 사용하는 악성 코드의 대부분이 메일이나 웹을 감염 수단으로 사용하기 때문에 신뢰하지 않는 사람으로부터 오피스 파일이 첨부된 전자 메일이 수신된 경우에는 특히나 주의가 필요하다. 또한, 오피스에 대한 보안패치는 반드시 마이크로소프트에서 제공하는 오피스 홈페이지를 통해 보안 업데이트를 적용하여야만 클라이언트 시스템의 보안성을 강화할 수 있다.

악의적인 공격자는 어플리케이션 취약점을 이용하여, 악성 코드가 포함된 조작된 파일을 대량 메일로 전송하는 방식의 공격이 이루어지며, 악성 코드 유포에 빈번하게 이용되었다. 비단 MS사의 어플리케이션 취약점뿐만 아니라, Apple Mac OS X, Active X, 이미지 뷰어, 웹 브라우저, 전자 메일 클라이언트, 오피스, 메신저, 데이터베이스 등을 대상으로 공격이 다양화 되고 있는 실정이다.

〔표 7〕 2007년 마이크로소프트 오피스 제품 주요 취약점

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)
MS07-026 Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점 (934873)
MS07-036 Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점(936542)
MS07-037 Microsoft Office Publisher의 취약점으로 인한 원격 코드 실행 문제점(936548)
MS07-044 Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점(940965)
MS07-060 Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점(942695)

4.1 침해 사고 동향

2007년 1월부터 12월까지 상반기 악성 코드 유포를 위해 침해 사고가 발생한 웹 사이트 및 배포지 수의 평균은 131건 중 50건을 차지하고 있다. 탐색 사이트 별 침해 사이트 비율은 0.37%로 1000개의 사이트 중 적어도 3개 이상이 악의적인 중국 해커에 의해 침해되고 있는 것으로 볼 수 있다.

2007년 발표된 취약점 중 인터넷 익스플로러를 사용해 악성 코드를 배포하는데 사용된 주요 취약점은 MS07-007과 MS07-017 총 2개이다. MS07-007 취약점의 경우 일부 플랫폼에만 적용 가능한 이유 등으로 인해 악성 코드 배포를 위해 거의 사용되지 못했던 데 반해 MS07-017 취약점의 경우 모든 플랫폼에 적용 가능하고 취약점을 이용한 악성 코드 배포도 매우 쉽기 때문에 현재 가장 큰 비중을 차지하고 있다.

실제로 2007년 악성 코드를 배포하기 위해 사용되는 취약점 별 비율을 살펴보면 MS07-017 취약점이 전체 245건 중 88건으로 전체의 약 36%이상을 차지하고 있다. 따라서 2008년에도 인터넷 익스플로러와 관련한 새로운 취약점이 발표되기 전까지 주로 사용되는 취약점은 MS07-017이 될 것으로 전망된다. 또한 2007년 후반기부터 점점 대중적으로 널리 사용되는 Active X 객체의 취약점을 이용한 악성 페이지도 조금씩 발견되고 있다. 그 동안 공격자가 사용하는 취약점은 윈도우 운영체제와 인터넷 익스플로러에 집중되었으나 Active X객체가 많이 쓰이고 있는 국내 웹 사용 환경의 특성상 Active X객체의 취약점을 이용한 사례도 간간히 발견되고 있다.

그리고 엠팩(Mpack)이나 아이스팩(IcePack)과 같은 웹 익스플로잇 툴킷(Web Exploit Toolkit)이 대중화되면서 이를 이용한 침해 사고의 사례도 조금씩 발견되고 있다. 웹 익스플로잇 툴킷을 사용 할 경우 손쉽게 악성 웹 페이지 제작이 가능할 뿐만 아니라 안티 바이러스(Anti-Virus) 소프트웨어의 진단을 회피하기 위한 고도화된 알고리즘을 사용할 수 있어 이를 이용한 공격코드 또한 점점 증가할 것으로 전망된다.

V. 해외 악성 코드 동향

2006년 이후의 악성 코드 동향을 보면 2000년 초반처럼 특정 악성 코드가 세계적으로 널리 퍼지는 경우는 드물다. 2007년 각국에 존재하는 주요 안티 바이러스(Anti-Virus) 업계에서 밝힌 피해 리포트를 바탕으로 할 때 해당 업체에 진단하지 못하는 악성 코드나 해당 업체에는 신고 되지 않은 악성 코드에 대해서는 통계에 포함되지 않는 한계가 있어 실제 사용자 감염 결과와는 다소 다를 수 있지만 유행하는 악성 코드의 국가별 그리고 지역별 차이를 알 수 있다.

이러한 이유는 앞서 언급한 바와 같이 악성 코드 제작자들의 목적이 금전적인 이득을 취하는 것으로 변질됨에 따라 각 국의 IT 문화 그리고 IT가 사회 전반에 미치는 영향에 따라서 제작되는 악성 코드의 유형이 국지적이자 지역적으로 달라지는 전형적인 특성을 그대로 나타내고 있다. 이러한 사항은 남미 지역의 온라인 뱅킹 정보를 유출하는 뱅커(Win-Trojan/Banker) 트로이목마와 반로드(Win-Trojan/Banload) 트로이목마가 한국을 위시한 극동 아시아권에서는 전혀 발견되지 않는 것을 사례로 들 수가 있다.

이러한 지역적이자 국지적인 특성은 전 세계적인 동향의 큰 줄기를 이루어 나가고 있는 상황이다. 이러한 특성을 바탕으로 한국과 가까운 이웃 나라인 일본과 중국의 악성 코드 동향부터 살펴보도록 하자

5.1 일본의 악성 코드 동향

2007년 일본에서 이슈가 되었던 것들은 트로이목마 감염 피해가 전년도에 비해 크게 증가한 것과 파일 공유 프로그램으로 인한 피해가 여전히 사회 문제화 되고 있는 점을 들 수 있다. 피싱으로 인한 피해가 꾸준히 증가하여 사회적인 이슈가 되고 있는 것 또한 2007년 일본의 악성 코드 동향과 관련하여 주목할 만한 점이다.

최근에는 웹 서버의 취약점을 이용하여 웹 사이트에 악성 코드를 다운로드 할 수 있는 악성 스크립트를 삽입하여 사용자들이 이를 다운로드 하도록 하는 형태의 악성 코드들이 많이 발견되고 있으며 이로 인한 피해가 많은 것으로 보고되고 있다.

위의 [표 8]은 일본 트렌드마이크로(www.trendmicro.co.jp)에서 발표한 2007년 악성 코드 피해보고 리포트의 내용 중 일부를 발췌한 것이다. 피해 집계된 내용에서 볼 수 있듯이 순위에 링크된 대부분의 악성 코드가 백도어 등의 트로이목마 형태이다. 이러한 트로이목마의 공통된 특징은 직, 간접적으로 개인 정보를 불법으로 취득하는 것을 목적으로 하므로 사용자의 주의가 필요하다.

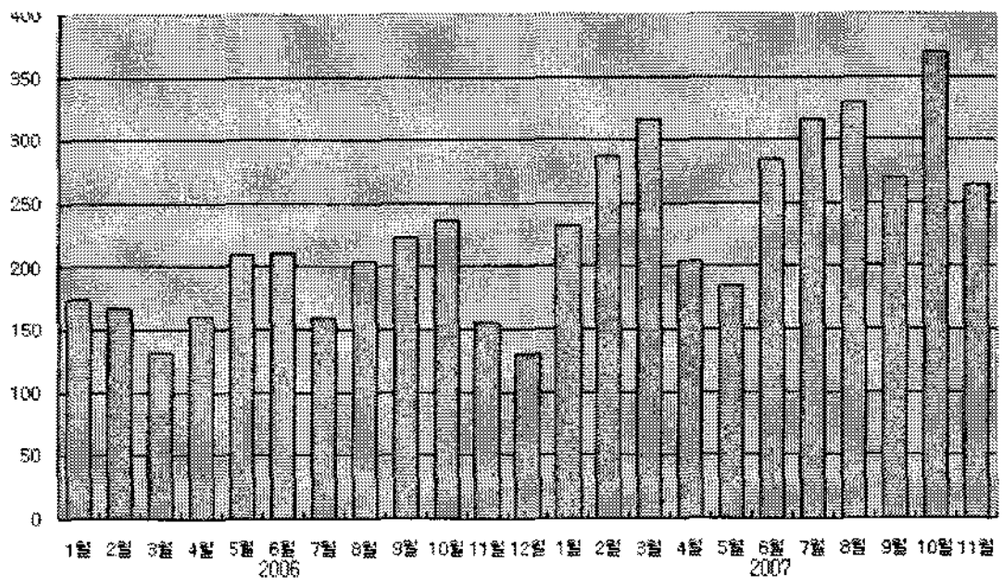
트로이목마 이외에도 아이알씨 봇(Win32/IRCBot.worm) 웜 이나 에스디 봇(Win32/SDBot.worm)웜 과 같은 악성 IRCBot에 의한 피해 또한 많이 발생한 것을 볼 수 있다. 봇 넷(BotNet)에 의한 네트워크상의 피해는 일본 내에서도 심각한 문제로 대두되고 있다. 일본에서는 악성 봇(Bot)에 대한 피해 예방을 위해 정부 기관과 통신사 ISAC이 주축이 되어 운영되는 사이버 클린 센터(www.ccc.go.jp)와 같은 단체가 만들어지는 등의 노력을 하고 있다.

일본에서 거짓으로 작성된 청구서로 인한 문제는 피싱이나 보이스 피싱과 같은 온라인 사기가 전 세계적으로 이슈화가 되기 전부터 온/오프라인상의 문제가 되어 왔다.

아래의 [그림 16]은 일본의 IPA에서 월별로 집계한 부당청구 관련 상담 통계이다. 피해 건수가 시간이 갈수록 점점 늘어나고 있는 것을 알 수 있는데 일본에서는

〔표 8〕 일본 트렌드마이크로(Trendmicro)의 2007년 바이러스 피해보고 리포트

순위	악성코드명	악성코드 유형	피해건수	발견일시
1	BKDR_AGENT	백도어	326 건	2003 년 8 월
2	TROJ_VUNDO	트로이목마	333 건	2004 년 11 월
3	JAVA_BYTEVER	기타	279 건	2003 년 5 월
4	TROJ_DLOADER	트로이목마	245 건	2004 년 7 월
5	TROJ_ZLOB	트로이목마	228 건	2005 년 11 월
6	BKDR_HUPIGON	백도어	214 건	2005 년 2 월
7	WORM_SDBOT	웜	207 건	2003 년 10 월
8	WORM_RBOT	웜	203 건	2004 년 3 월
9	ADWARE_BESTOFFERS	애드웨어	165 건	2006 년 7 월
10	EXFL_ANICMOO	기타	146 건	2007 년 3 월



〔그림 16〕 2006년 및 2007년 월별 부당청구 관련 피해 상담 통계

출처를 알 수 없는 업체로부터 발송된 사용료를 납부하라는 엽서에서부터 불법 소프트웨어에 이르기까지 다양한 형태로 사용자를 유인하는 행위들이 발생하고 있다. 최근에도 원 클릭 이라는 소프트웨어에 의해 성인사이트로 등록이 되고 이를 악용한 부당 청구로 인한 피해가 다수의 사용자들에게 발생하여 이슈가 된 사례가 있다.

안티니 (Win32/Antinny.worm) 웜은 P2P (Peer to Peer) 프로그램의 설정을 바꾸는 것과 같은 동작을 수행함으로써 개인 정보를 유출하게끔 유도하는 악성 코드이다. 일본에서는 위니(Winny)라는 P2P 기반의 파일 공유 프로그램을 많이 사용하고 있는데 이 역시 안티니 (Win32/Antinny.worm) 웜에 감염된 시스템으로 인해 기밀 정보가 위니(Winny)를 이용하여 무작위로 배포되었으며 그 중에는 군사 기밀이나 기업 기밀 정보가 공개는 경우도 있어서 사회적인 이슈가 되었다.

5.2 중국의 악성 코드 동향

중국의 2007년 악성 코드 동향을 되돌아보면 2006년도부터 진행되었던 악성 코드의 국지화와 금전적인 목적을 위한 감염 시도가 더욱 심화되고 있는 실정이다.

2007년 중국의 악성 코드 동향에서 가장 큰 변화로 꼽을 수 있는 것이 악성 코드를 감염시키기 위해 새로운 감염 기법의 등장으로 볼 수가 있다. 외장형 저장장치가 보편화되면서 이러한 저장 매체는 웜 또는 트로이목마와 같은 악성 코드 형태의 구분 없이 중국뿐만 아니라 한국에서도 많은 문제점을 야기하며 첫 번째로 꼽을 수 있는 감염 기법의 변화로 볼 수 있다.

2007년 2월에서 3월경부터 등장하기 시작한 외장형 저장 장치를 이용한 감염 기법은 예전 플로피 디스크를 이용하던 시절을 연상시킬 정도로 심각한 문제로 대두되었다. 이러한 문제는 위 [표 9]의 강민(JiangMin) 2007년 악성 코드TOP 10에서 Checker/Autorun(V3 진단명 - TextImage/Autorun)이 1위를 차지하고 있다는 면에서 충분히 알 수가 있다.

〔표 9〕 중국 강민(JiangMin) 2007년 악성 코드 TOP10

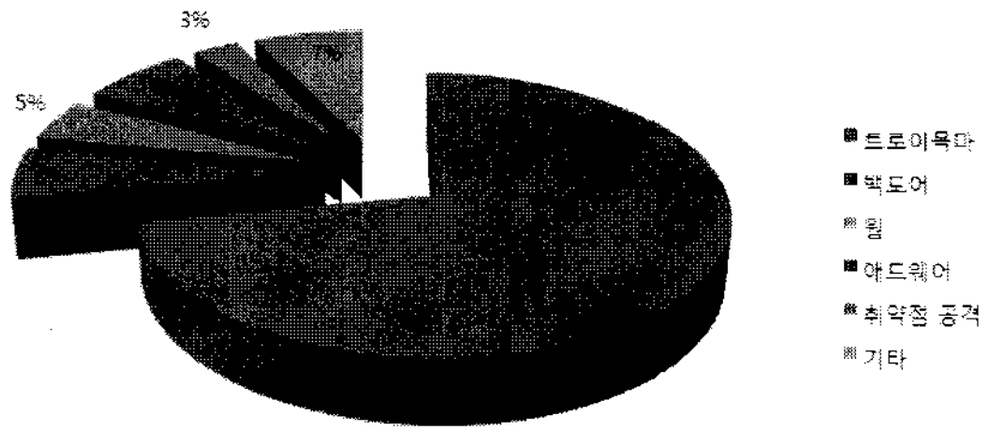
순위	JiangMin	점유율	수치
1	Checker/Autorun	3.54%	1221695
2	Exploit.ANIfile.b	2.18%	751630
3	Trojan/PSW.QQPass.qhf	0.84%	289433
4	Adware/Clicker.je	0.75%	261378
5	Adware/Adload.ad	0.47%	163005
6	Trojan/PSW.GamePass.frl	0.47%	162473
7	Adware/Agent.p	0.43%	149346
8	Trojan/PSW.GamePass.acuh	0.41%	141787
9	Adware/Boran.e	0.37%	128305
10	Trojan/Agent.psm	0.36%	126660

그 다음으로 심각한 위협으로 발전한 감염 기법을 본다면 바로 웹을 통한 악성 코드의 감염을 들 수가 있다. 이는 중국 내에서 만의 문제가 아니라 전 세계적인 하나의 큰 흐름으로 발전하고 있는 실정이며 이러한 웹을 통한 감염 기법의 심화는 Exploit.ANIfile.b(V3 진단명 - Win-Trojan/ANIExploit.Gen)가 2위를 차지하고 있다는 것만으로도 충분히 알 수가 있다.

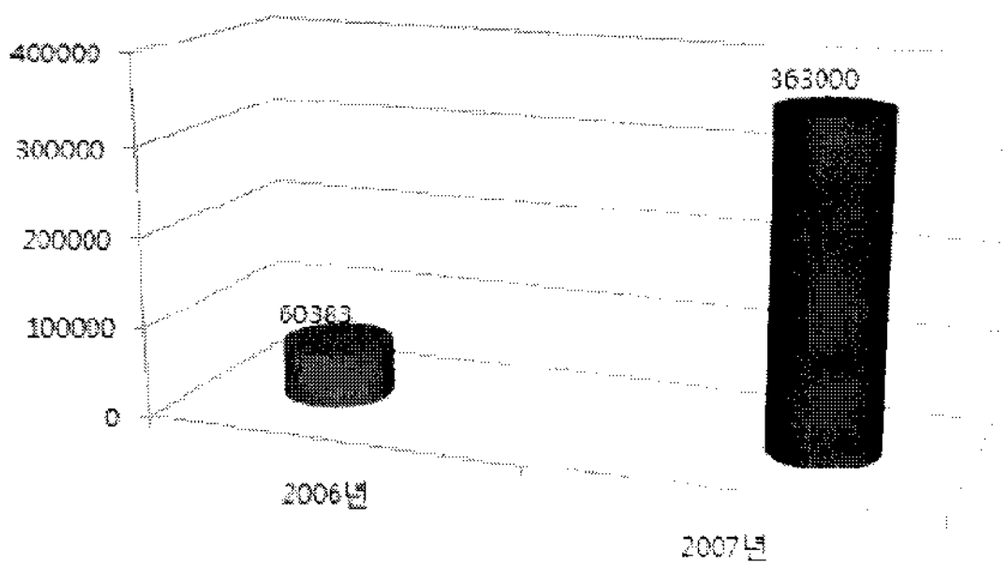
2007년의 중반 경부터 등장하기 시작한 ARP 스푸핑(ARP Spoofing)을 이용한 감염기법은 악성 코드를 감염시키기 위해 존재하는 악의적인 웹 사이트를 직접적으로 방문하지 않아도 악성 코드에 감염될 수 있다는 점을 보여준 사례라고 할 수 있다.

감염 기법 면에서 본다면 앞서 서술한 3가지 기법들이 2007년 중국 악성 코드 동향의 큰 축이었다면, 악성 코드 형태별로 본다면 사용자 정보를 탈취하는 트로이목마가 가장 심각한 위협으로 볼 수가 있다. 이러한 형태의 악성 코드는 2005년경부터 등장하기 시작하였지만 2007년의 경우를 본다면 공격 대상이 한국에서 개발된 온라인 게임에서 벗어나 중국에서 개발된 온라인 게임으로 목표가 변경되고 있는 실정이다. 특히 Trojan/PSW.QQPass.qhf(V3 진단명 - Win-Trojan/QQPass.Gen), Trojan/PSW.GamePass.frl(V3 진단명 - Win-Trojan/OlineGameHack)와 Trojan/PSW.GamePass.acuh (V3 진단명 - Win-Trojan/OnlineGameHack)이 각각 3위, 6위와 8위를 차지하고 있다 점에서 중국 내에서의 온라인 게임을 공격 대상으로 한 트로이목마는 2007년에 가장 활동이 활발했다고 볼 수 있다.

이러한 공격 대상의 변화에 대한 원인은 크게 2가지로 볼 수가 있는데 첫 번째로 국내 온라인 게임 개발 업체가 다양한 보안 기능 강화와 중국 내에서 개발된 온라인 게임의 아이템 거래 활성화로 볼 수 있다. 최근에 알려진 바에 따르면 중국 내에서는 이미 온라인 게임 아이템을 거래 할 수 있는 웹 사이트가 약 4만여 개에 이르며 중국인들이 가장 많이 사용하고 있는 QQ메신저를 통해서 QQ머니라는 사이버 머니 역시 불법적으로 거래가 활성화되고 있다고 한다. 이러한 심각성은 2007년 2월 델보이(Win32/Dellboy) 바이러스의 제작자로 알려진 리 준의 구속은 악성 코드 판매와 온라인 게임



〔그림 17〕 중국 강민(JiangMin)의 2007년 악성 코드 형태별 분포



〔그림 18〕 강민(JiangMin) 2007년 악성 코드 증가치

사용자 정보 유출을 위한 트로이목마 유포가 상업적으로 얼마나 많이 이용되고 있는지를 충분히 잘 보여주고 있는 사례로 들 수가 있다.

악성 코드의 형태면에서는 2006년에 이어 2007년 역시 트로이목마가 절대 다수를 차지하고 있다. 이는 앞서 기술한 바와 같이 온라인 게임 아이템 탈취와 사용자 정보 탈취를 통해서 불법적인 재화의 거래가 가장 크게 작용하고 있기 때문이라고 볼 수 있다. 또 한 가지 2007년도 악성 코드 형태면에서 특이점은 광고를 목적으로 제작되는 애드웨어 역시 크게 증가 한 것을 알 수 있다.

중국 로컬 백신 업체인 강민(JiangMin)의 발표에 따르면 2007년 한 해 동안 발견된 중국 내 악성 코드는 총 363,000건으로 2006년 한 해 동안 발견된 60,383건보다 6배에 이르고 있다고 한다. 이는 전 세계적으로 발견되는 악성 코드가 수치적인 면에서 급격하게 증가하고 있는 현상 역시 중국 내에서도 동일하게 이루어지고 있다는 것을 잘 알려주고 있다.

5.3 세계의 악성 코드 동향

우리나라는 온라인 게임 계정 탈취 트로이목마가 기승을 부리고 있지만 다른 나라에서 악성코드 통계에서는 순위권에 없거나 몇몇 업체의 하위권에 분포할 뿐이었다. 온라인 게임 계정 탈취 프로그램도 한국의 온라인 게임과 게임 속 아이템이 현금화되는 지역에서 많이 볼 수 있다.

다만 한 가지 확실한 점은 지역별로 유행하는 악성코드 성향이 있지만 악성코드 수가 전반적으로 급격히 증가하고 있다는 점이다. 안철수연구소는 2007년 한 해 동안 약 50만개의 신종 악성코드를 추가했다. 다른 해외 보안 업체 동향 역시 마찬가지 인데 핀란드 F-시큐어(F-Secure)사의 통계에 따르면 2007년까지 발견된 악성코드는 50만개 이며 2006년까지 발견된 약 23만개에서 넘어선 수치로 이는 과거 20여 년간 발견된 악성코드 수 보다 2007년 한 해 동안 발견된 수가 더 많다는 사실이다. 시만텍의 발표 자료에 따르면 2008년 4월 현재까지 발견된 악성코드 수는 100만개를 돌파했으며 2007년 한 해 동안 71만 1천 912개 이상의 악성코드를 찾아냈으며 이는 12만 5천 243개에 불과한 2006년에 비해 468% 증가한 수치라고 한다. 심지어 2007년 말까지 약 550만개의 악성코드가 발견되었다고 AV-TEST는 밝히고 있다.

2007년까지 발견된 악성코드가 최소 50만개에서 최대 100만개까지 존재하는 것으로 보인다. 50 만개 이상 차이가 나는 건 유사 변형이 계속 제작되고 있고 업체마다 변형에 대한 분류가 다르기 때문에 통계가 부정확해진 것으로 보인다. 하지만, 확실한 건 2008년뿐 아니라 당분간 악성코드 증가 수는 줄지 않을 것으로 보인다.

Ⅵ. 미래 전망

앞서 살펴본 악성코드 동향과 시큐리티 동향들을 종합하여 보았을 때 안철수연구소에서는 2008년 전망으로 다음을 선정하였다.

- ▶ 가상화 기술 이용 등 악성 코드 은폐 기법의 고도화
- ▶ 웹 해킹 증가
- ▶ 사이버 블랙마켓의 활성화
- ▶ 스파이웨어의 악성 코드화
- ▶ 애플리케이션 취약점 공격 증가
- ▶ 이동저장장치 노린 악성 코드 기승
- ▶ UCC와 SNS 등 웹2.0 서비스 통한 악성 코드 전파 가속화

6.1 가상화 기술 이용 등 악성 코드 은폐 기법의 고도화

악성 코드 제작자는 악성 코드를 은폐하기 위해 다양한 방법을 사용한다. 그 중 향후에 등장할 기법으로 가상화 기술(실제로 지니고 있는 물리 구조에 적당한 계층을 개입시킴으로써 더 일관성 있고 편리한 논리 구조를 갖게 하는 것)을 들 수 있다. 가상화 기술을 이용한 악성 코드는 아직 발견되지 않았지만 2005년에 개념을 증명할 정도의 루트킷(Rootkit)이 나온 바 있다. 당시에는 탐지가 어렵지 않고 동작에 불확실성이 있어 실제로 피해가 발생하지는 않았다. 하지만 자체 가상 머신을 가지고 해당 가상 머신에서만 동작하는 코드를 구현해 실행 압축을 해제하기 어렵게 만든 악성 코드가 존재하기도 하는데 이런 악성 코드는 보안 제품을 무력화할 수 있다. 2008년에는 이런 기법을 악용한 은폐 및 자기보호, 탐지하기 어렵게 더욱 고도화된 악성 코드가 급증할 것으로 예상된다.

6.2 웹 해킹 증가

웹 애플리케이션의 취약점을 이용해 해킹하거나 DDoS(Distributed Denial of Service) 공격을 하는 일이 더욱 증가할 것으로 전망된다. 많은 웹 사이트가 보안에 대해 고려되지 않고 개발되어 적용되기 때문에 보안에 취약한 상태에서 공격에 무방비 상태로 당할 가능성이 높다. 이를 통해 악성 코드와 스파이웨어를 유포하거나 해당 웹 페이지로 유도하는 일이 전년에 이어 지속 발생할 것으로 보인다. 또한 DDoS 공격은 금전을 요구하기 위한 수단으로 이용되는 일이 더욱 많아질 것으로 예측된다.

웹사이트 공격은 인터넷의 필수인 웹 서버를 공격하여, 수많은 사용자가 피해를 볼 수 있으며 방화벽을 우회할 수 있기 때문에, 방지책으로는 웹 서버 보안 패치 및 웹 어플리케이션의 보안 코딩(Secure Coding)이 필요하다. 일반 사용자들의 경우 해당 시스템의 보안 패치가 필수적이다. 이러한 웹 사이트 기반 공격은 2008년에도 지속적으로 증가하리라 예상된다.

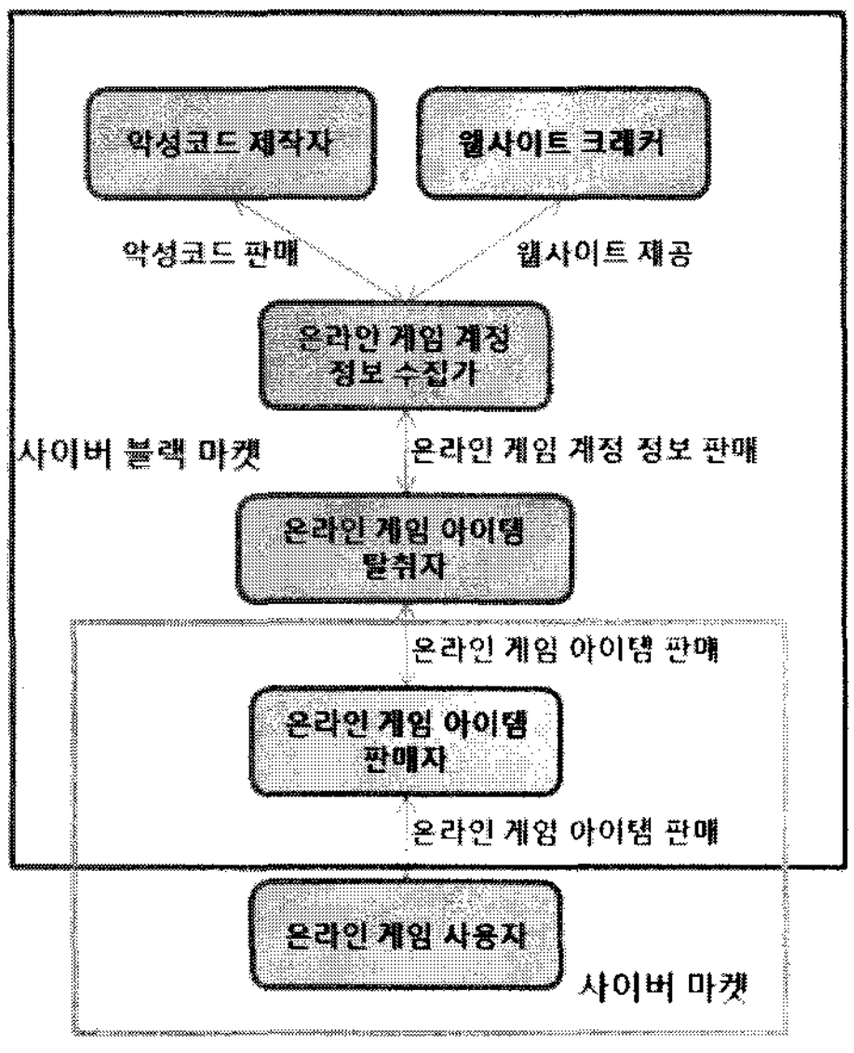
6.3 사이버 블랙마켓의 활성화

가상의 재화를 현금으로 교환하는 '사이버 블랙마켓'의 규모가 커질 것으로 전망된다. 여기서는 신상 정보 및 신용카드 정보, 온라인 게임 계정 등이 거래되고 있으며, 악성 코드가 판매되는가 하면 피싱, DDoS 공격 등을 대가를 받고 해주는 것으로 알려져 있다. 이에 따라 여기서 거래 가치가 높은 악성 코드나 해킹이 더욱 기승을 부릴 것으로 보인다. 또한 금전적 이익을 위해 불특정 다수를 공격하는 것보다 특정 타깃을 노리는 국지적 공격이 증가할 것이다.

2005년 여름을 즈음하여 중국에서 제작된 것으로 추정되는 온라인 게임 계정 정보를 탈취하는 악성 코드가 한국에서 급증하기 시작하였다. 이렇게 급증하게 된 주요한 원인에는 한국에서 제작된 온라인 게임 중 해당 게임에서 사용되는 아이템이 현금 거래가 가능하다는 것에서 비롯된 것으로 알려졌다. 실제 이렇게 악성 코드에 의해 불법적으로 탈취된 온라인 게임의 아이템이 얼마나 많이 어떻게 거래되는지는 분명하게 알려져 있지 않았다. 그러나 최근 연구되어 발표되는 정보 보호 관련 논문들 중 일부에서는 가장 주요한 원인이 사이버 재화들이 불법적으로 거래되는 사이버 블랙마켓이 급격하게 성장하였기 때문으로 이야기하고 있다. 특히 사이버 블랙마켓이 가장 활성화된 국가로는 중국과 러시아 그리고 루마니아를 지목하고 있는데 한국의 경우에는 중국에서 활성화된 사이버 블랙마켓의 영향력이 크게 미친다고 볼 수 있다.

중국의 사이버 블랙마켓에서 주요하게 거래되고 있는 것은 앞서 이야기한 바와 같이 온라인 게임 아이템들이다. 이를 탈취하기 위해서 중국의 사이버 블랙마켓은 크게 악성 코드 제작자, 웹 사이트 크래커, 온라인 게임 계정 정보 수집가와 온라인 게임 아이템 탈취자의 4가지 역할을 가진 인력 또는 조직이 중심이 되어 활동하고 있다.

[그림 19]와 같은 순환 구조를 가진 중국의 사이버 블랙마켓에서는 온라인 게임 사용자 정보를 탈취하는 악성 코드가 최저 한화 1300원 에서 최고 한화 130만원에 거래되고 있으며 이를 이용해 수집한 사용자 정보는 1개당 평균 한화 1300원 선에서 거래되고 있는 실정이다. 그리고 규모 면에서는 2007년 상반기 동안만 중국 내 약 40,000개의 온라인 게임 아이템 거래상들에 의해 평균 한화 2000원 선에서 약 1,220,000개의 온라인 아이템이 거래된 것으로 알려져 있어 얼마나 빠른 속도로 중국의 사이버 블랙마켓이 성장하고 있는지를 예측할 수 있다. 이러한 추세로 본다면 2008년 역시 온라인 게임 사용자 정보를 탈취하기 위한 악성 코드는 지속적으로 발견될 가능성이 상당히 높을 것으로 예측

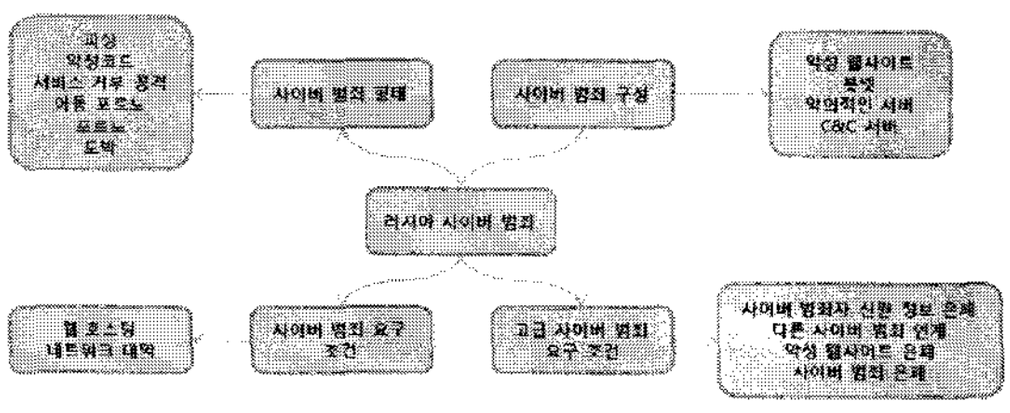


〔그림 19〕 중국 사이버 블랙마켓의 구조

된다. 이외 2008년 상반기 발생한 옥션의 1천 만 명 개인정보 유출 사건에 고용된 중국인 해커가 있다는 얘기도 나오고 있으며 중국에서 한국 사람들의 주민등록 번호가 공공연하게 거래되고 있다.

러시아와 루마니아의 사이버 블랙마켓은 중국이 온라인 게임 아이템 판매를 통한 현금 획득을 중심으로 움직이고 있는 것과는 다르게 사이버 상에서 현금을 획득할 수 있는 어떠한 형태의 재화들 모두가 거래된다는 면에서 중국의 것보다 확장된 형태를 갖추고 있다. 이로 인해 러시아의 사이버 블랙마켓은 사이버 범죄의 형태를 띠고 있어 그 심각성이 크다고 볼 수 있다.

이러한 러시아의 사이버 블랙마켓의 구조를 도식화한 것이 [그림 20]과 같다. [그림 20] 중 "사이버 범죄 형태"를 보면 중국의 사이버 블랙마켓과는 다르게 피싱과 악성 코드에서부터 포르노 및 도박 웹 사이트까지 온라인에서 수익을 거둘 수 있는 모든 불법적인 재화들이 이용되고 있는 것을 알 수 있으며 특히나 "고급 사이



〔그림 20〕 러시아 사이버 범죄의 구조

〔표 10〕 러시아 사이버 블랙마켓에서 거래되는 재화들과 판매가 (출처 : 시만텍)

판매물	판매가
미국 신용카드 정보	$1 ~ $6
영국 신용카드 정보	$2 ~ $12
29,000개의 이메일 계정	$5
온라인 뱅킹 계정	$300
야후 메일 쿠키 익스플로잇	$3
야후 또는 핫메일 계정	$3
좀비 시스템	$6 ~ $20
피싱 웹 사이트	$3 ~ $5
검증된 페이팔(PayPal) 계정	$50 ~ $500
검증되지 않은 페이팔(PayPal) 계정	$10 ~ $50
스카이프(SkyPe) 사용자 계정	$12
월드 오브 워크래프트 사용자 계정	$10

버 범죄 요구 조건"에서는 오프라인의 실제 범죄자들이 자신들의 범죄를 은폐하거나 범죄 조직을 구성하는 것과 동일한 형태를 띠고 있다.

러시아와 루마니아의 사이버 블랙마켓에서는 온라인 게임 아이템과 온라인 게임 사용자 정보가 주되게 거래되는 중국의 사이버 블랙마켓과는 다르게 앞서 이야기한 바와 같이 온라인상에서 현금을 획득할 수 있는 어떠한 형태의 가상 재화를 모두 판매되고 있다. 이렇게 판매되고 있는 거래 물들은 [표 10]에서와 같이 신용카드 정보에서 악성 코드에 감염된 좀비(Zombie) 시스템까지 다양하게 거래되고 있어 그 규모면 에서는 중국의 사이버 블랙마켓을 훨씬 뛰어넘는 형태를 보인다고 할 수 있다.

2008년 중요하게 관심을 가지고 지켜보아야 할 대상 중 하나가 바로 중국과 러시아 그리고 루마니아의 사이버 블랙마켓일 것이다. 이제까지 발생한 보안 사고들은 호기심이나 충동에 의한 것들이었다면 2008년에는 사이버 블랙마켓에서 현금으로 거래를 위한 대가성 보안 위협이 크게 증가를 할 것으로 예측된다. 특히나 러시아와 루마니아의 사이버 블랙마켓을 통해 온라인상에서 현금 거래가 가능한 어떠한 형태의 재화 또는 정보라도 모두 거래가 이루어질 수 있다는 점으로 미루어 2008년에는 이 사이버 블랙마켓을 통해서 새로운 형태의 보안 위협이 등장할 수 있을 것으로 예측된다.

6.4 스파이웨어의 악성 코드화

국내에서 제작되는 스파이웨어 중 운영체제나 애플리케이션의 취약점을 직접 공격하거나 루트킷을 사용해

자신이 설치 또는 실행 중이라는 사실을 숨기는 프로그램은 많지 않았다. 그러나 앞으로는 스파이웨어를 통한 이익을 극대화하기 위해 취약점 공격, 보안 프로그램 무력화, 자기 은폐, 파일 감염 등 악성 코드에 사용되는 기법이 많이 사용될 것으로 예상된다.

6.5 애플리케이션 취약점 공격 증가

현재 마이크로소프트사의 운영체제나 애플리케이션 취약점을 노리는 공격이 가장 비중이 높지만 그 수는 점차 줄어드는 추세이다. 반면 PDF, 애플 맥 OS X, 액티브X, 멀티미디어 플레이어, 이미지 뷰어, 메신저 등 사용자들이 많이 사용하는 애플리케이션들에 대한 공격이 증가하고 있다. 이런 흐름은 2008년에도 이어질 것으로 예측된다. 이러한 흐름과 동일하게 2008년 5월에는 플래쉬(Flash) 파일인 SWF 파일 구조적 취약점을 이용한 공격도 발견되었다.

6.6 이동 저장장치 노린 악성 코드 기승

지난해에 이어 올해도 이동 저장 장치(USB 플래시 메모리, 이동식 하드디스크)를 통해 전파되는 악성 코드가 기승을 부릴 것으로 전망된다. 특히 보안 USB가 등장함에 따라 이를 뚫거나 중요 정보를 빼내려는 악성 코드가 등장할 가능성이 높다.

6.7 UCC와 SNS(Social Network Service) 등 웹2.0 서비스 통한 악성 코드 전파 가속화

UCC가 악성 코드 또는 스파이웨어를 배포하는 또 하나의 채널이 되고 있다. 동영상 플레이어의 일부인 양 설치를 유도하는 스파이웨어가 자주 발견되고 있으며 일반 동영상을 가장해 설치되는 스파이웨어도 적지 않은 실정이다. 이런 흐름은 2008년에도 지속될 것으로 보인다. 아울러 SNS(Social Network Service)가 주목받기 시작하자 이를 이용한 악성 코드가 기승을 부릴 것으로도 전망된다. 이미 2006년에 미국 마이스페이스(MySpace)에서 프로필을 보기만 하면 친구 리스트에 특정인이 추가되도록 한 악성 코드가 제작된 바 있다. 또한 1인 미디어인 블로그에 악성 코드를 내려 받게 유도하는 주소를 링크해놓는 일도 증가할 것으로 보인다.

한편, 향후 2~3년 후에 현실화할 이슈로는 VoIP를 겨냥한 DDoS 공격 및 도감청 본격화, 무선 인터넷 기기를 겨냥한 해킹 증가, 모바일 플랫폼인 안드로이드를 겨냥한 보안 위협 등장 등이 예측된다.

6.8 VoIP 겨냥한 DDoS 공격 및 도감청 본격화

2008년 1월VoIP(Voice over Internet Protocol) 번호 이동제의 시행으로 가입자가 증가할 것으로 예상된다. VoIP는 기존 공중전화망(Public Switched Telephone Network) 대신 인터넷으로 음성 통화 서비스를 제공하기 때문에 보안 측면에서 위험성이 높다. VoIP 서비스의 서버를 DDoS 공격해 서비스를 중단하거나 서버의 데이터를 위변조할 가능성이 있다. 또한 전송되는 데이터를 도감청할 수 있으며 스팸의 또 다른 채널로 악용할 가능성도 매우 크다.

6.9 무선 인터넷 기기 겨냥한 해킹 증가

현재 출시되는 대부분의 휴대용 컴퓨터와 모바일 기기는 물론 PSP, 휴대용 게임기에는 무선 인터넷에 접속할 수 있는 기능이 포함 되어 있다. 그러나 이들의 접속을 허용하는 AP(Access Point)가 보안 설정을 하지 않은 경우가 많으며, 보안 설정을 했어도 WEP(Wired Equivalent Privacy) 등과 같은 암호화는 쉽게 암호 키를 알아낼 수 있다. 이런 네트워크에 접속하면 해당 네트워크에 접속한 컴퓨터의 각종 자료를 열람할 수 있을 뿐 아니라 ARP 스푸핑(ARP Spoofing) 또한 가능하다. 따라서 무선 인터넷 사용이 대중화함에 따라 보안 위협은 더욱 증가할 것으로 예상된다. 이미 2008년 5월 국내 모 은행에 대한 해킹 시도가 무선 인터넷에 대한 스니핑으로 알려졌다.

6.10 모바일 플랫폼 안드로이드 겨냥 보안 위협 등장

구글을 비롯해 약 30여 개 업체가 연합해 만든 오픈 모바일 플랫폼인 안드로이드의 소프트웨어 개발 키트가 공개됐다. 이 플랫폼을 이용할 경우 모바일 기기를 제작할 때 제조 원가 절감을 비롯해 여러 이점이 있어 많은 업체들이 이를 적용할 것으로 예상된다. 아직 이 플랫폼을 적용한 제품이 출시되지는 않았지만, 안드로이드는 거의 모든 기능을 API(Application Programming Interface)로 제공하고 있어 현재로선 악용될 소지가 매우 높다.

Ⅶ. 결 론

본 논문에서는 최근 국내에서 유행하고 있고 피해가 발생하고 있는 악성 코드의 동향과 스파이웨어 동향 그리고 이 악성 코드와 스파이웨어에서 사용하는 운영체제 또는 애플리케이션에 존재하는 취약점들에는 어떠한 것들이 있는지 시큐리티 동향에서 살펴보았다. 이와 함께 극동아시아를 포함한 전 세계의 악성 코드 동향을 살펴봄으로서 한국에서 발생하고 있는 악성 코드 피해 사고와는 어떻게 다른지도 다루어 보았다. 이러한 동향들을 미루어 보아 향후의 악성 코드는 국지적인 공격이 더욱 거세질 전망으로 보이며 특히나 사이버 블랙마켓을 통해서 어떠한 사이버 재화라도 모두 금전 거래가 가능해지고 이러한 금전적 이익을 위해 대가성 공격도 증가 할 것으로 예측하였다. 그리고 미래 전망에 포함되어 있는 궁극적인 악성 코드의 미래 형태는 금전 획득을 위해 다양한 최신 기술의 습득으로 발전 될 것 이라고 보는 것이 정확한 표현으로 볼 수가 있다.

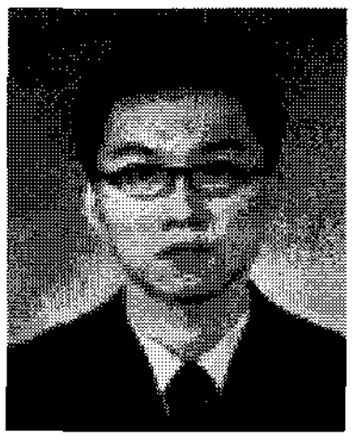
〈著者紹介〉

조 시 행 (SiHaeng Cho)

1984년 2월 : 한양대학교 건축공학과 졸업
1984년~1986년 : 동아건설 전산실 근무
1986년~1991년 : 쌍용정보통신 연구소 근무
1992년~1995년 : 한컴퓨터주식회사 & 한글과컴퓨터 근무
1996년~현재 : 안철수연구소 ASEC (시큐리티대응센터) 팀장
AVAR(Association of anti Virus Asia Researchers) Director
WildList Reporter
<관심분야> Information Security, Anti-Virus Tech.

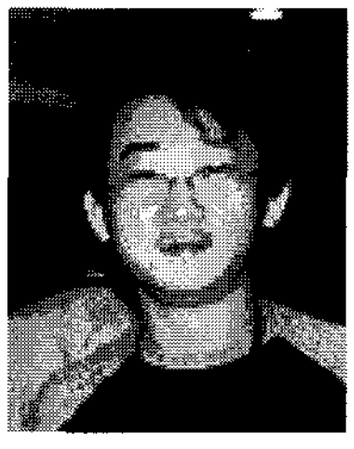
차 민 석 (Minseok Cha)

2004년 2월 : 울산대학교 전자계산학과 졸업
1997년 8월~현재 : 안철수연구소 ASEC(시큐리티대응센터) 선임 연구원
<관심 분야> Malicious Code Analysis, Malicious Code Chronicle, Heuristic Detection



정 진 성 (Jinsung Jung)

1996년 2월 : 혜전전문대 비서행정과 졸업
1999년 5월~현재 : 안철수연구소 ASEC(시큐리티대응센터) 선임 연구원
<관심분야> Malicious Code Analysis, Runtime Packer, Generic Unpacking



장 영 준 (Youngjun, Chang)

2003년 2월 : 동국대학교 중어중문학과 졸업
2002년 7월~현재 : 안철수연구소 ASEC(시큐리티대응센터) 주임 연구원
<관심분야> Information Security, Risk Management, Malicious Code Analysis Early Warning