ASEC Report 9월

® ASEC Report

2007. 10

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 악성코드와 시큐리티의 종합된 정보를 매월 요약하여 리포트 형태로 제공하고 있다.

I. ASEC 월간 통계

(1) 9월 악성코드 통계

순위		악성코드명	건수	%
1	-	Win-Trojan/Xema.variant	95	40.9%
2	-	Win32/Virut	60	25.9%
3	-	Win32/IRCBot.worm.variant	21	9.1%
4	new	VBS/Autorun	11	4.7%
5	new	VBS/Solow	11	4.7%
6	new	Win-Trojan/Eldo.10240	11	4.7%
7	new	HTML/Agent	8	3.4%
8	↑2	TextImage/Autorun	7	3.0%
9	new	Win-Trojan/Virut.45056	5	2.2%
10	new	JS/Exploit	3	1.3%
합계			232	100.0%

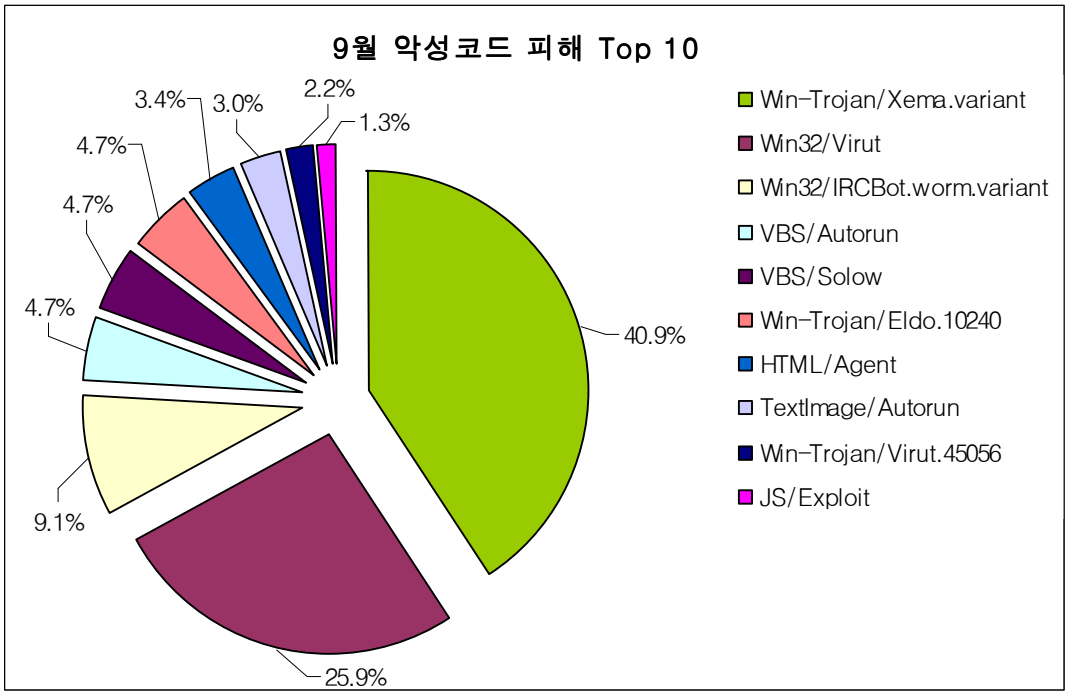
[표 1-1] 2007년 9월 악성코드 피해 Top 10

월 악성코드 피해 동향

2007년 9월 악성코드 Top10에는 전월과 동일하게 Win-Trojan/Xema.variant가 1위를 차지하였다. 또한, Win32/Virut, Win32/IRCBot.worm.variant도 나란히 2~3위를 유지하였다. 새로이 6위에 Win-Trojan/Eldo.10240와 9위에 Win-Trojan/Virut.45056가 Top10에 진입하였으며, 전월과 동일하게 온라인 게임 계정을 탈취하는 악성코드 류에 대한 피해가 많았으나 다수의 변종이 접수되어 Top10에는 진입하지 못하였다.

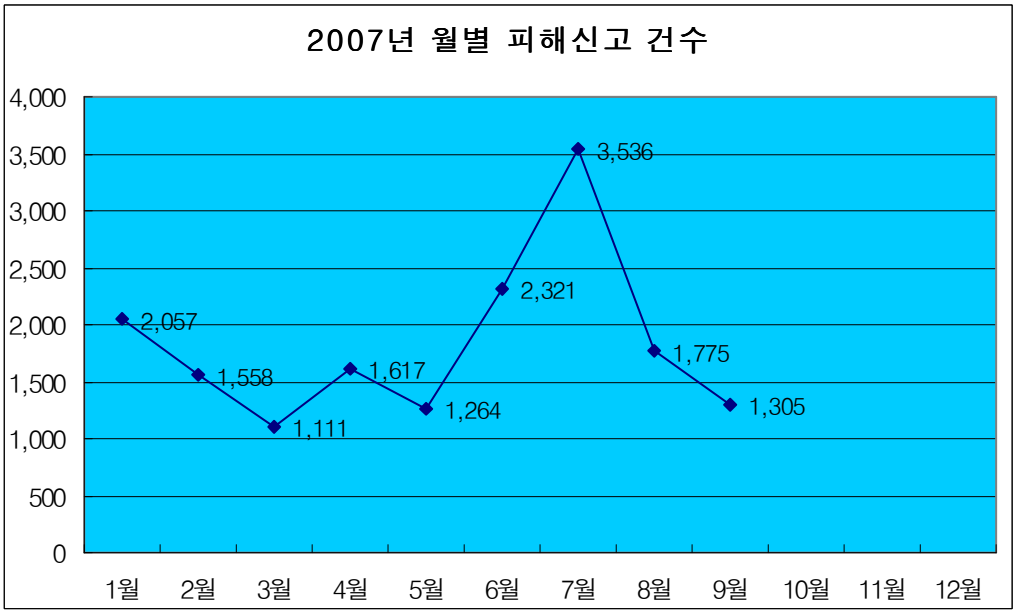
9월의 경우 스크립트 관련 악성코드가 무려 5건이나 Top10에 진입하였다. 그 중 USB메모리등을 통해 전파되는 VBS/Autorun, VBS/Solow가 기승을 부렸으며, 그에 따라 생성되는 TextImage/Autorun 또한 Top10에 진입된 것을 알 수 있다.

9월의 악성코드 피해 Top 10을 도표로 나타내면 [그림 1-1]과 같다.



[그림 1-1] 2007년 9월 악성코드 피해 Top 10

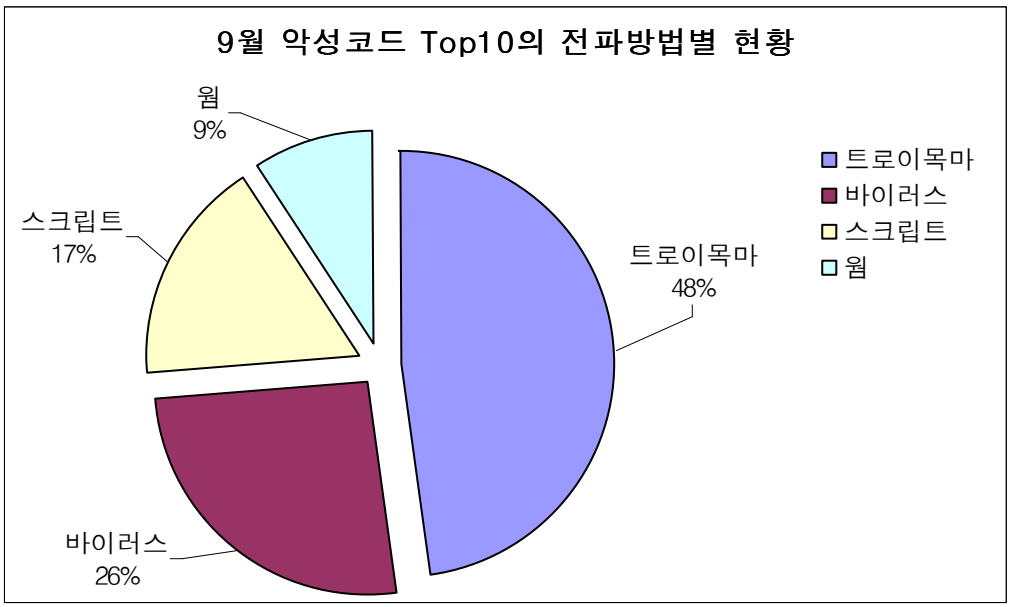
[그림 1-2]에서와 같이 1월부터 월별 피해신고 건수는 꾸준히 감소세를 보이다가 6, 7월에는 확산력이 강한 아이알씨봇(IRCBOT)의 증가와 함께 새로운 악성코드로 인해 전월보다 1000건 이상 증가하였다. 그러나, 8, 9월에는 연초와 유사한 수치를 보이며 피해건수가 감소되었다. 이는 인터넷 사이트, 게시판으로 주로 전파되는 트로이목마가 다소 감소되었으며, 휴가철을 맞이하여 컴퓨터 사용빈도가 낮은 것도 하나의 영향으로 보인다.



[그림 1-2] 2007년 월별 피해신고건수

9월 악성코드 Top 10 전파방법 별 현황

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

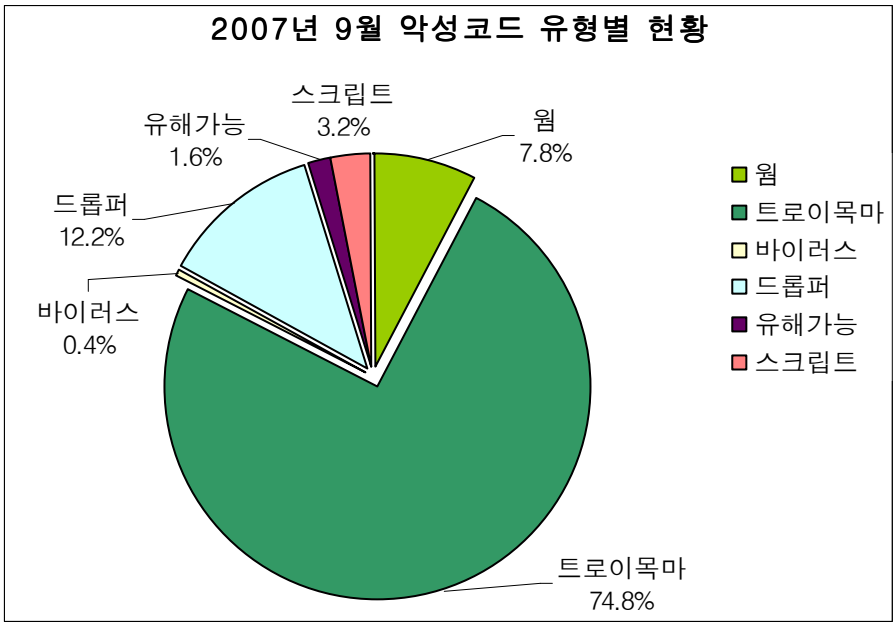


[그림 1-3] 2007년 9월 악성코드 Top 10의 전파방법별 현황

9월에도 변함없이 트로이 목마류가 가장 많은 피해를 발생시켰으나 전월(53%)에 비해 다소 감소하였다. 바이러스는 Virut의 기승으로 전월(21%) 대비 26%로 증가하였고, 스크립트는 전월(2%) 대비 무려 17%를 점유하며 상승되었다. 반면, 웜(Worm)은 전월(17%)대비 감소하였으나 꾸준히 Top10에 등록되어 위력을 과시했다.

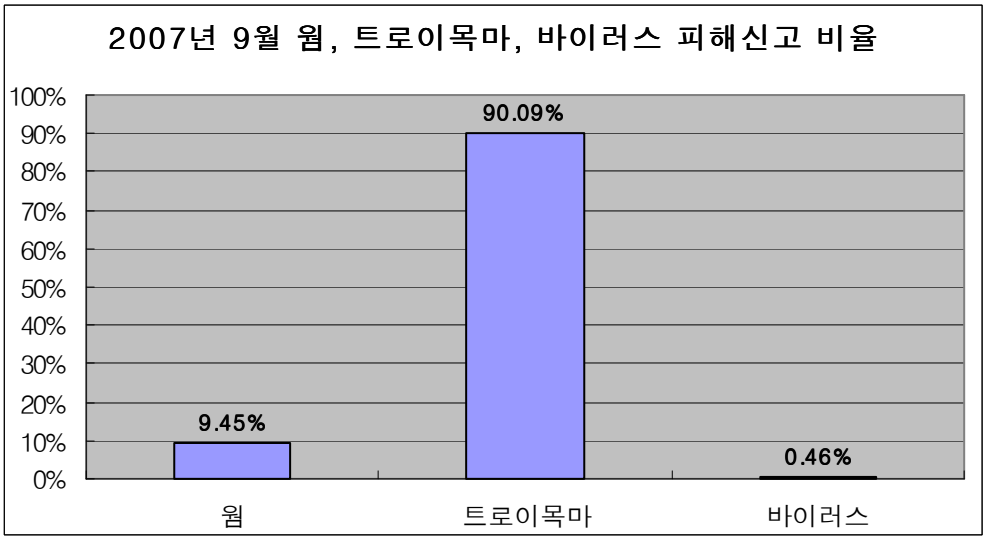
피해신고 된 악성코드 유형 현황

2007년 9월에 피해신고 된 악성코드의 유형별 현황은 [그림 1-4]와 같다.



[그림 1-4] 2007년 9월 피해 신고된 악성코드 유형별 현황

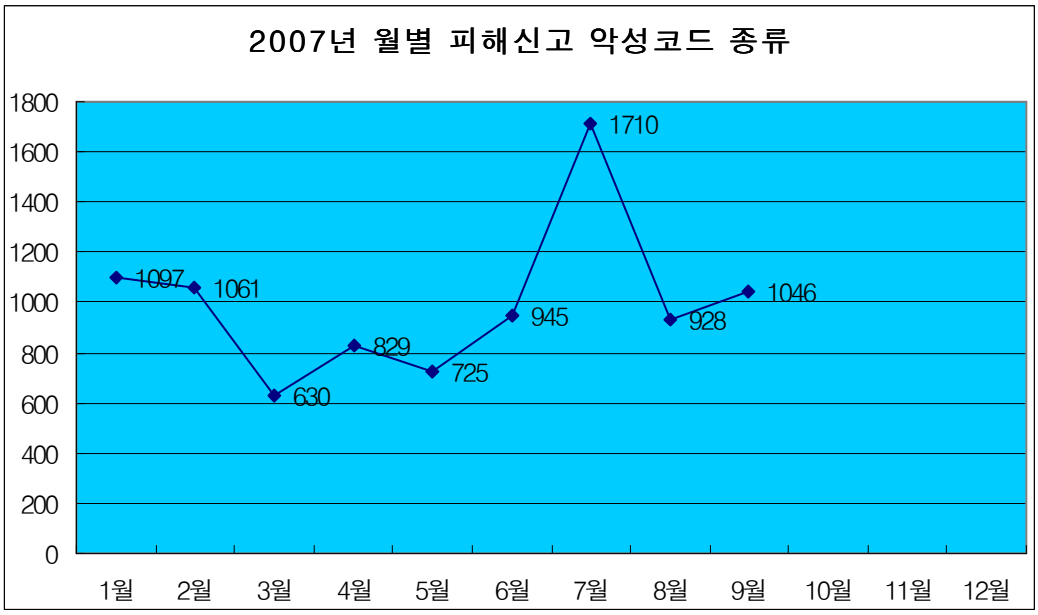
전체 피해 신고에서의 악성코드 유형을 확인해보면, 트로이목마가 74.8%로 가장 많았으며 2위는 드롭퍼(12.2%), 웜(7.8%)는 3위를 차지하였다. 그 외 스크립트 3.2%, 뒤를 이어 유해가능 1.6%, 바이러스가 0.4%였다. 바이러스의 경우 피해 건수에 대한 유형별 현황으로 보았을 때는 미미하나 Top10에 2위로 등극할 만큼 전체 피해통계 측면에서 보면 피해가 많았다. 트로이목마의 경우 여전히 74.8%를 차지해 다양한 악성코드들이 새로이 나타나고 있음을 단적을 보여주고 있다. 이중 주요 악성코드 유형인 트로이목마, 바이러스, 웜에 대한 피해신고 비율을 따져보면 [그림 1-5]와 같다.



[그림 1-5] 2007년 9월 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 2007년 8월에 급격한 감소세를 보인 이후 9월에 다시 증가 추세를 보이고 있다.



[그림 1-6] 2007년 월별 피해신고 악성코드 종류 개수

국내 신종(변형) 악성코드 발견 피해 통계

9월 한달 동안 접수된 신종 (변형) 악성코드의 건수 및 유형은 [표 1-2], [그림 1-7]과 같다.

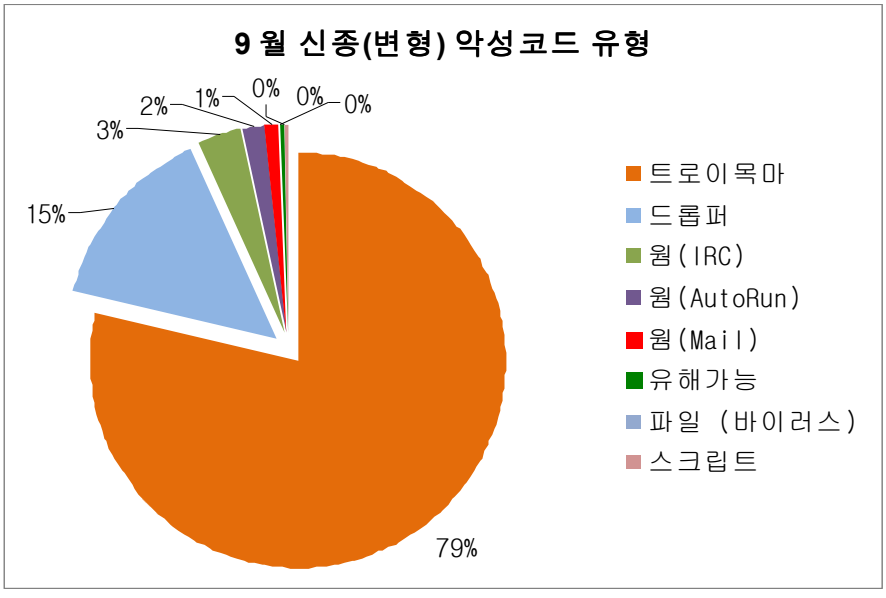
	웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
7 월	28	300	71	4	3	0	0	0	16	0	422
8 월	54	327	72	1	6	0	0	0	10	1	471
9 월	32	418	78	1	1	0	0	0	1	1	531

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

전월 대비 전체 악성코드가 13% 가량 증가하였다. 증가된 원인은 온라인 게임 계정을 탈취하는 악성코드류가 전월 대비 132% 가량 증가 하였기 때문에 그렇다. 최근 3개월간 해당 악성코드의 발견 수는 하락 하고 있었으나 이번 달 들어 갑자기 증가 하였다. 웜의 발생 비율은 전월 대비 줄었는데 그 이유는 대부분 악성 IRCBot 웜에 의한다. 앞의 피해신고 top 10에서 IRCBot 변형이 3위에 올랐으나, 웜 자체의 발생 건수가 줄은 것은 악성 IRCBot의 피해가 적은 건수에도 불구하고 심각하다는 것을 의미한다.

이외에 실행파일을 감염 시키는 바이러스도 전월 대비 1건 밖에 보고 되지 않았으며 유해가능 프로그램도 역시 그렇다. 전체적으로 악성코드는 전월 보다 줄었지만 온라인 게임의 사용자 계정을 훔쳐내는 악성코드류가 폭발적으로 증가 하였기 때문에 전체 악성코드 비율이 전월 대비 소폭 상승 하였다.

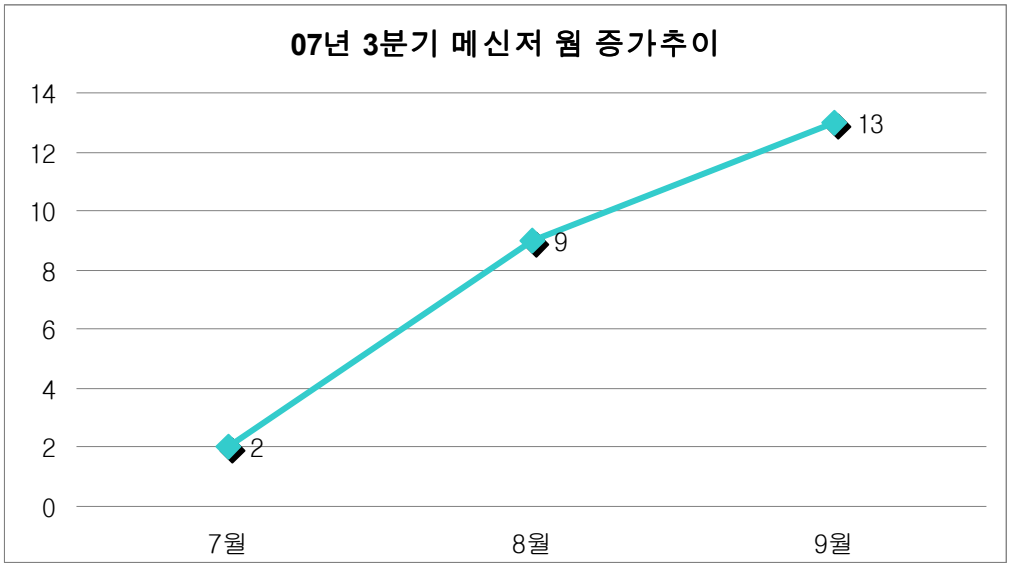
다음은 이번 달 악성코드 유형을 상세히 분류 하였다.



[그림 1-7] 2007년 9월 신종 및 변형 악성코드 유형

통계에서는 제외 되었지만 (통계는 국내 접수 샘플기준으로 작성) MSN 을 전파 수단으로 사용하는 웜도 4 개가 발견 되었다. 신종은 아니며 기존에 있었던 변형으로 특이하다면 기존의 메신저 웜이 자신을 전파할 때 사용하는 메시지가 영문이나 독어, 이탈리어등 아메리카 또는 유럽지역내 언어 였다. 그러나 9월에 발견된 MSN 메신저 웜 변형중 하나는 메신저에 출력하는 메시지를 중국어 병음을 영어로 표기한 것이 발견 되었다. 악성코드 자체로는 특이 할 만한 것은 없으나 이것은 처음 발견된 사례라 하겠다.

다음은 최근들어 증가추세인 메신저 관련 웜의 증가추이를 그래프로 나타내 보았다. 해당 악성코드들은 MSN과 Skype 를 전파 수단으로 사용하는 악성코드이다.

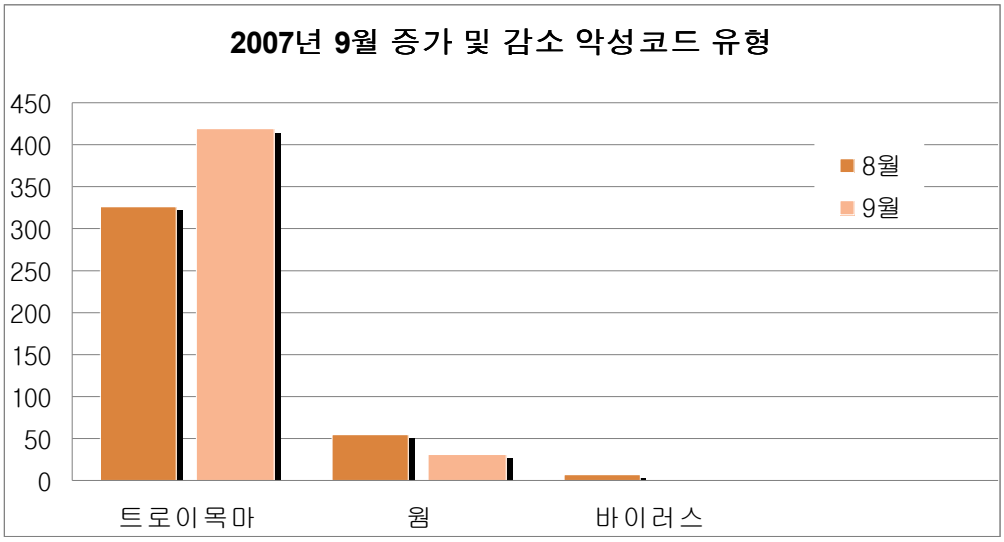


[그림 1-8] 2007년 3분기 메신저 웜 증가 현황

특히 이번달은 Skype로 자신을 전파 하는 악성코드인 Win32/Skipi 변형도 다수 발견되어 전월 대비 하여 상승하였다.

이번 달은 Win32/Klest.D라는 바이러스가 보고 되었는데 후위형 바이러스이고 원본 파일에 섹션 하나를 추가하며 특정 호스트로부터 파일을 다운로드 하는 작은 쉘코드를 하나 포함하고 있다.

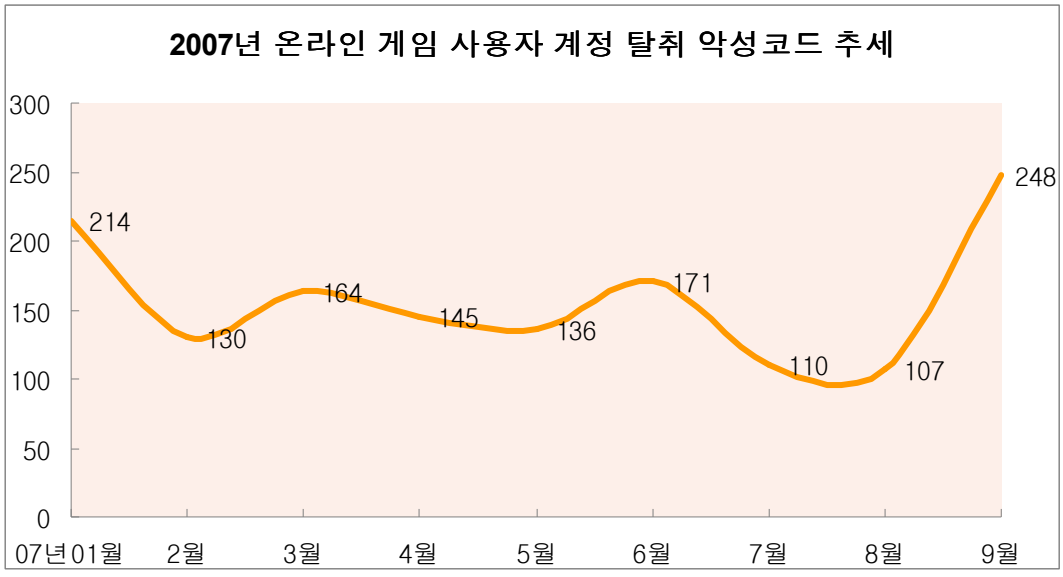
다음은 9월에 증가 및 감소한 주요 악성코드 유형에 대한 현황이다.



[그림 1-9] 2007년 9월 감소 및 증가 악성코드 유형

위에서 언급한 바와 같이 전체적으로는 악성코드 수는 줄었으나 트로이목마류의 증가가 눈에 띈다. 유해가능 프로그램 수도 줄었는데 대부분 V3에 포함되는 유해 가능 프로그램들은 리모트 어드민 프로그램류 또는 버추몬드라고 알려진 스파이웨어이다.

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



[그림 1-10] 온라인 게임 사용자 계정 탈취 트로이목마 현황[1]

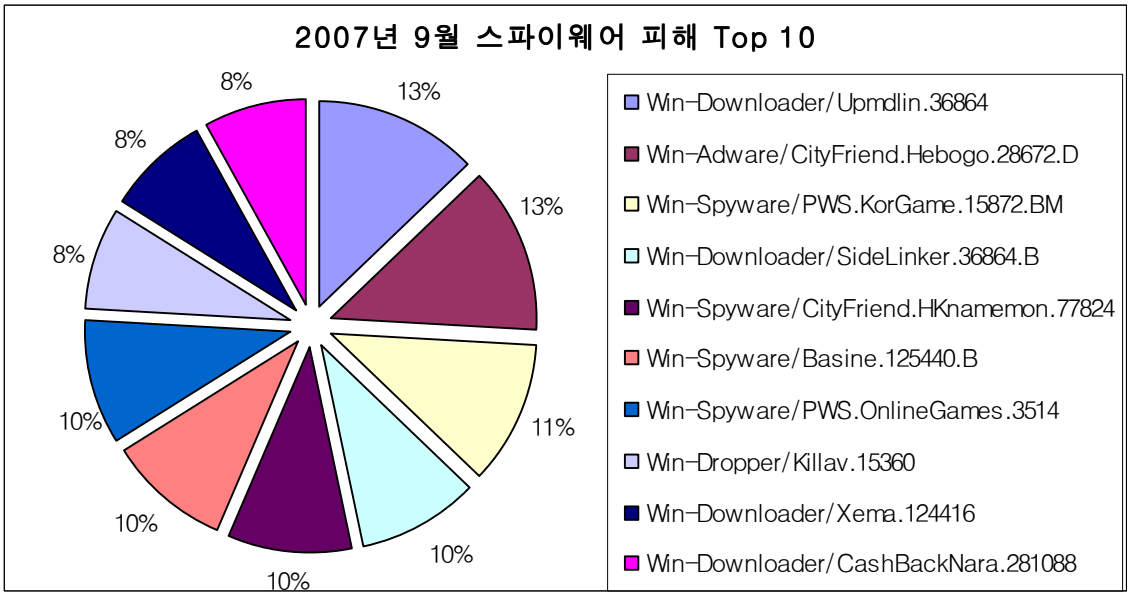
해당 악성코드들은 전월 대비 132 % 상승 하였다. 여러 가지 가능성이 있지만, 우선 국내 온라인 게임들을 타켓으로 하는 진단명을 갖는 Win-Trojan/KorGameHack의 수가 전월보다 무려 300% 넘게 증가하였다. 보통 이런 경우 과거에는 국내에 보안에 취약한 웹 사이트가 해킹을 당한 수도 많을 것으로 추정해 볼 수도 있으나, 최근에는 하나 이상의 다운로더 증상을 갖는 악성코드가 대량으로 다른 악성 파일을 다운로드하고 이러한 증상을 반복한다. 근래들어 온라인 게임 계정을 탈취하는 악성코드를 비롯하여 중국산 악성코드들은 한대의 시스템에 다른 변형들이 대량 감염 되는 특징이 있다. 올해 중국산 악성코드의 특징 중 하나는 이러한 대량감염이 특징이 된다 하겠다.

(2) 9월 스파이웨어 통계

9월 스파이웨어 피해 현황

순위		스파이웨어 명	건수	비율
1	New	Win-Downloader/Upmdlin.36864	8	13%
2	New	Win-Adware/CityFriend.Hebogo.28672.D	8	13%
3	New	Win-Spyware/PWS.KorGame.15872.BM	7	11%
4	New	Win-Downloader/SideLinker.36864.B	6	10%
5	New	Win-Spyware/CityFriend.HKnamemon.77824	6	10%
6	New	Win-Spyware/Basine.125440.B	6	10%
7	New	Win-Spyware/PWS.OnlineGames.3514	6	10%
8	New	Win-Dropper/Killav.15360	5	8%
9	New	Win-Downloader/Xema.124416	5	8%
10	New	Win-Downloader/CashBackNara.281088	5	8%
합계			62	100%

[표 1-3] 2007년 9월 스파이웨어 피해 Top 10



[그림 1-11] 2007년 9월 스파이웨어 피해 Top 10

2007년 9월 스파이웨어 피해 통계의 상위는 대부분이 국내 애드웨어가 차지하고 있다. 2007년에는 특히 국내에서 제작 배포되는 애드웨어가 많은 피해를 입히고 있으며, 영어권 국가에서 제작 배포되는 스파이웨어는 피해 순위 상위권에서 발견하기 힘들다. 피해 순위 상위권이 대부분 국내 애드웨어인 중에서 중국에서 제작된 온라인게임 계정 유출 스파이웨어

(Win-Spyware/PWS.KorGame, Win-Spyware/OnlineGames)가 피해 통계 Top10 에 포함되어 있다. 이들 온라인 게임 계정 유출 스파이웨어는 9월에 다수의 신종 및 변형이 발견되었으며, 이들 변형을 포함한 전체 피해 건수는 약 140건에 달하고 있으며, 여전히 큰 위협으로 존재하고 있다. 2007년 9월 스파이웨어 피해 통계의 공동 1위와 5위를 차지한 애드웨어 씨티프렌드(Win-Adware/CityFriend.Hebogo.28672.D)는 꾸준한 피해를 입히고 있는 애드웨어이다. 애드웨어 씨티프렌드는 팝업 광고를 노출하며, 제거 방법을 제공하지 않는데다 랜덤한 파일 이름을 사용하여 설치하기 때문에 수동제거가 어려운 특징이 있다.

2007년 9월 유형별 스파이웨어 피해 현황은 [표 1-4]와 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
7월	261	183	55	232	10	20	3	1	0	765
8월	197	105	43	156	12	6	0	0	0	519
9월	291	119	35	132	8	7	0	0	0	592

[표 1-4] 2007년 9월 유형별 스파이웨어 피해 건수

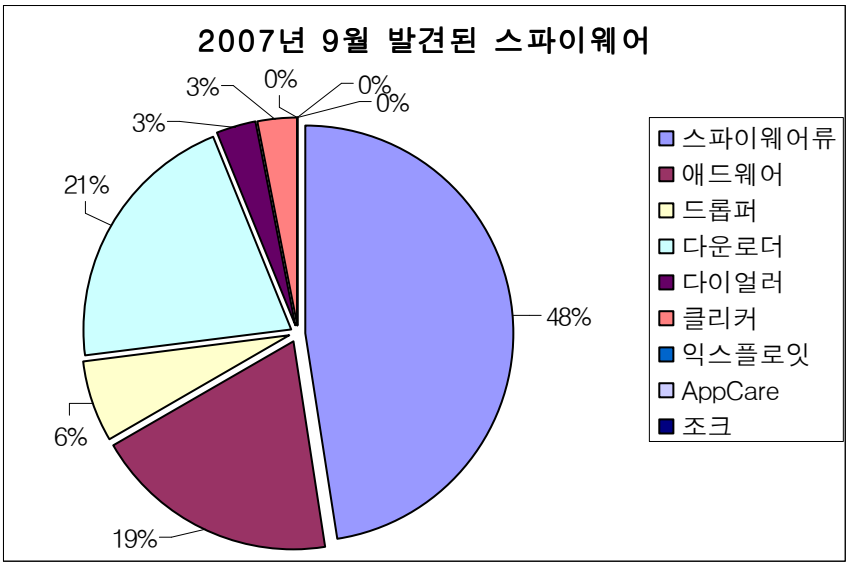
2007년 9월 스파이웨어 피해 신고 건수는 592건으로 지난 8월의 519건 보다 다소 증가한 가운데 중국에서 제작된 온라인게임 계정 유출 스파이웨어 증가의 원인으로 스파이웨어류의 피해가 100건 가까이 증가하였다. 이들 스파이웨어는 중국발 해킹이 시작된 지난 2005년부터 꾸준한 피해를 입히고 있으며, 현재에도 해킹으로 변조된 크고 작은 웹사이트를 통해 사용자의 시스템에 감염되고 있다. 보안 취약점을 이용하여 손 쉽고 빠르게 감염되며, 지금 현재에도 수 많은 변형이 만들어 지고 있기 때문에 이들 온라인게임 계정 스파이웨어의 예방이나 근절이 어려운 것이 사실이다. 또한 실행 중에도 눈에 띄는 동작이 나타나지 않기 때문에 감염된 시스템에서 찾아내는 것 또한 쉽지 않다. 이러한 특징으로 당분간 온라인게임 계정 유출 스파이웨어의 피해는 지속될 것으로 예상된다.

9월 스파이웨어 발견 현황

9월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 1-5], [그림 1-12]와 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
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

[표 1-5] 2007년 9월 유형별 신종(변형) 스파이웨어 발견 현황

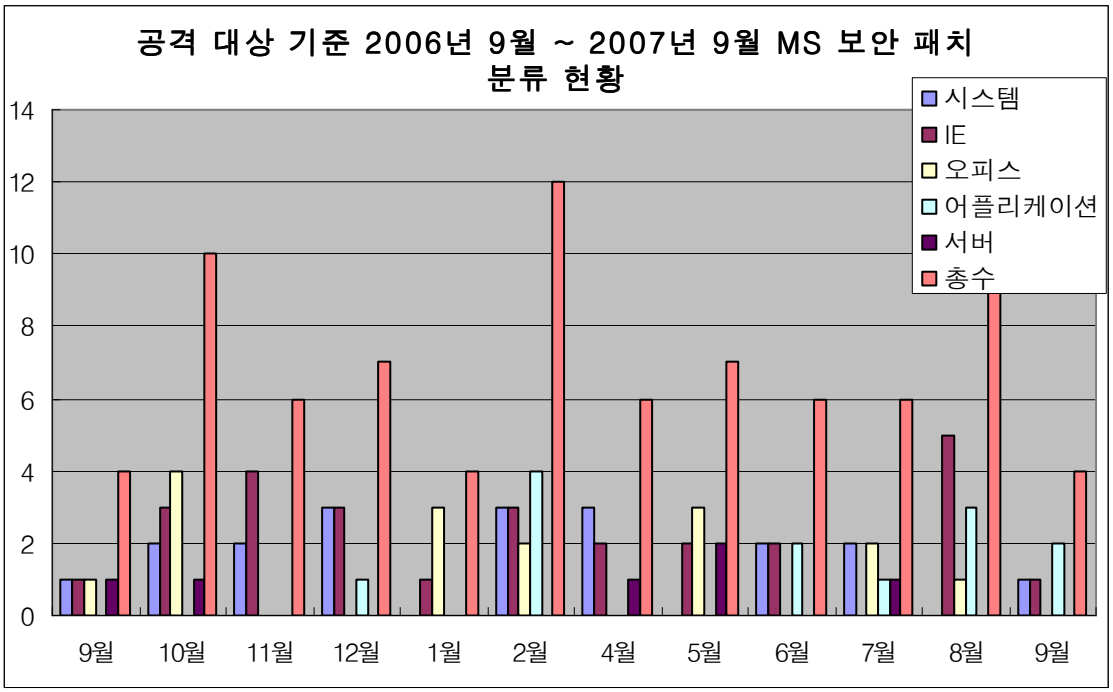


[그림 1-12] 2007년 9월 발견된 스파이웨어 프로그램 비율

. 스파이웨어 피해 통계에서도 언급한 중국에서 제작 배포되는 온라인게임 계정 유출 스파이웨어의 영향으로 스파이웨어류의 신종 및 변형 발견 건수가 8월에 비해 약 40% 증가한 91건을 기록하고 있는 것이 가장 큰 특징이다.

(3) 9월 시큐리티 통계

2007년 9월에는 마이크로소프트사에서 총 4개의 보안 업데이트를 발표하고, 발표된 업데이트는 긴급(Critical) 1개, 중요 3개로, 8월의 총 9건에 비해서, 줄어들었다. 이 중에서 인터넷 익스플로러 공격에 사용될 수 있는 MS07-051 에 대한 패치가 포함되었으며, Visual Studio 관련 패치인 MS07-052, 윈도우에서 유닉스 서비스를 동작시킬 때 필요한 Unix용 윈도우 서비스에 대한 패치 MS07-053 이 포함된 것이 특징이라고 할 수 있다.

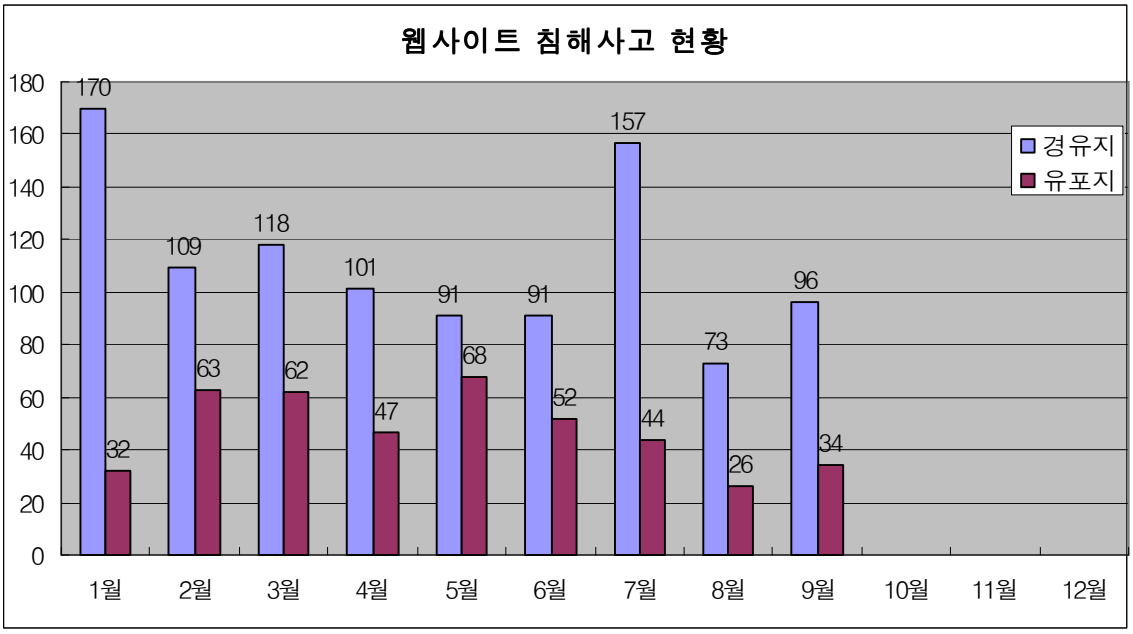


[그림 1-13] 2006년 9월 ~ 2007년 9월 공격대상 기준 MS 보안 패치 현황

[그림 1-13]을 보면, 전반적으로 2007년에 들어와서, 어플리케이션 취약점들(IE, 오피스, 기타 어플리케이션) 취약점들이 증가 추세에 있는데, 9월달에는 지난달에 비하여, IE를 공격할 수 있는 취약점과 MS Messenger 에 해당한 패치가 발표되어, 이러한 어플리케이션 취약점들에 대한 패치가 꾸준히 발생하는 것을 알 수 있다.

특이사항으로는 9월 달에 OpenOffice 에서 TIFF 관련 취약점이 발견되었는데, Microsoft Office의 취약점 증가 추세뿐만 아니라, OpenOffice 또한 취약점 수가 점차 증가하고 있다. 이러한 오피스 관련 취약점은 반드시 오피스 홈페이지에서 보안 업데이트를 적용해야만, 클라이언트 시스템의 보안성을 강화할 수 있다. 보다 자세한 사항은 3사분기 이슈/트렌드에서 알아 본다.

2007년 7월 웹 침해사고 현황



[그림 1-14] 웹사이트 침해사고 현황

2007년 9월의 웹 사이트 침해지/배포지 수는 96/34로 2007년 8월과 비교하여 증가하였다. 이는 다른 달과 비교하여 큰 차이가 없는 수치이며 결과적으로 2007년 8월 현황에서 예측하였던 수치와 비슷하다.

취약점별 현황을 살펴보면, MS07-017 취약점을 이용한 공격코드의 배포가 20.5%로 이전에 비하여 크게 줄어들었다. 이와 같은 상황은 AV제품들이 조작된 Animated Cursor 파일들을 잘 진단하였기 때문인 것으로 판단할 수 있으나 단순히 일시적인 상황으로 다음달에는 예전과 같은 수치를 회복할 가능성도 있기 때문에 2007년 10월에 가서야 명확히 분석될 수 있을 것으로 보인다.

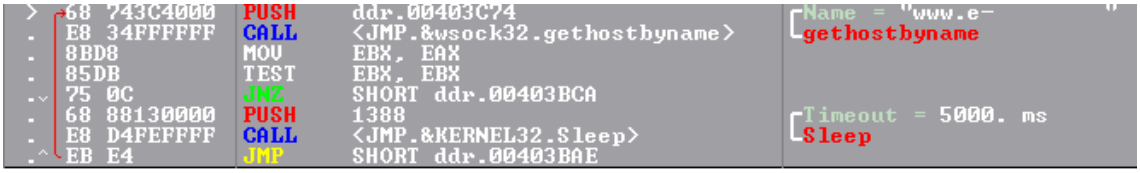
II. ASEC Monthly Trend & Issue

(1) 악성코드 – Win-Trojan/Eldo

9월은 비교적 조용한 한 달 있었다. 물론 DDoS 공격으로 잘못 알려져 버린 Eldo 트로이목마가 언론에도 보도가 되면서 세간의 관심을 끌기도 하였다. 그리고 이 트로이목마와 관련이 깊은 Win32/Virut 바이러스의 변형도 출현하여 분석가들을 고민에 빠트리기도 하였다. 이번 달에 이슈가 될 악성코드에 대하여 정리해 보았다.

► Win-Trojan/Eldo 트로이목마

먼저 이 트로이목마의 출처는 명확하지 않지만 잘 알려진 Win32/Virut 바이러스에 의해서 다운로드 되었을 가능성이 높다. 이러한 가능성은 Virut 바이러스가 특정 IRC 서버에 접속하여 파일을 다운로드 하고 실행 할 수 있는 증상이 있으며, 이러한 전례가 있었기 때문이다. Eldo 라고 명명된 이 악성코드는 분산 서비스 공격(DDoS) 기능이 있는 것처럼 알려졌으나 실제로는 그렇지 않고, 해당 악성코드에 의해서 의도적이지 않게 발생한 지속적인 연결요청 SYN 패킷으로 인하여 문제가 되었다. 이 트로이목마는 실행하면 특정 사이트로 HTTP Request 패킷을 생성하게 된다. 그러나 정상적으로 접속 되지 못한다면 5초간 대기하였다가 다시 HTTP Request 패킷을 생성하는 다른 스레드를 생성하게 된다. 코드상으로 다음과 같다.



[그림 2-1] Win-Trojan/Eldo 코드 일부분

해당 트로이목마는 이 과정에서 해당 웹 사이트로 접속이 되지 않자 지속적으로 HTTP Request 패킷을 생성하는 스레드를 생성하게 되는 무한 루프를 만들게 된다. 이러한 문제로 인해 과도한 네트워크 트래픽을 생성하게 되어 분산 서비스 거부 공격과 유사한 형태를 만들게 된다. 즉, 악성코드 제작자가 의도 하지 않았다 하더라도 결과적으로는 이것은 마치 DDoS 와 유사한 모습을 갖게 되었다. 또한 이것은 접속하려는 사이트의 서비스 거부 공격뿐만 아니라 해당 트로이목마가 대량으로 감염된 네트워크 환경에서도 제대로 네트워크를 이용할 수 없는 상황을 만들어내기도 하였다.

► 중국어 병음기호가 있는 메신저 웜

Win32/ShadoBot.worm 변형으로 알려진 MSN 메신저 웜은 올해 발견된 메신저 웜중 단연코 발견 순위가 앞선다. 메신저 특성상 실시간으로 메시지 확인이 가능하기 때문에 메신저 웜은 다양한 언어의 메시지를 포함하는 경우가 많다. ShadoBot의 경우도 프랑스, 이탈리아어, 에스파냐어, 영어등 포함하고 있다. 이번 달에 발견된 변형의 경우 다음과 같이 중국어 병음이 영문으로 표시된 것이 첫 발견 되었다.

```
ASCII "KAN BA LI XI ER DUN JIN JIANYU HOU SHI DUO ME QIAOCUI :<."
ASCII "NI HE WO !!! .... QING KAN :D."
ASCII "KAN WO DE ZHAOPIAN :D."
ASCII "JIESHOU WO DE ZHAO PIAN :> !!."
ASCII "YI ZHANG WO GEN WO PENGYOU ZUI HAO DE ZHAOPIAN :s !!."
ASCII "ZHE SHI WO DE LUOZHAO :o QING BU YAO FA GEI BIEREN !!."
```

[그림 2-2] Win32/ShadoBot 웜 변형 이 메신저로 전송되는 메시지 일부분

이렇게 다양한 메시지를 가지고 있는 이유는 감염된 시스템의 윈도우 언어에 따라 보내는 메시지도 달라지기 때문이다. 영문으로 된 스팸메일이 비 영어권에서 잘 읽혀지지 않듯이 사용자 자신의 언어가 아닌 경우라면 메일이든 메신저의 메시지인 경우도 확인 하지 않기 때문이다. 이러한 다양한 메시지도 일종의 사회공학기법으로 해석 될 수 있다.

► 또 다른 메신저 웜의 전파 경로 – Skype

인터넷 전화로 대표되며 VoIP에서 선도적인 Skype는 VoIP를 이용한 통화 이외에도 P2P 기반의 메신저 기능을 갖고 있다. Skype 역시 개발 관련 SDK 가 공개가 되어 악성코드 제작자가 이를 노리고 악성코드 제작에 악용하고 있다. 이번달 무려 9개의 변형이 거의 동시에 보고가 되었다. V3는 Win32/Skipi.worm 진단명으로 변형들을 진단 하고 있다.

Hex dump																ASCII
69	6C	29	00	3A	29	00	00	72	65	61	6C	6C	79	20	66	il).:)..really f
75	6E	6E	79	00	00	00	00	6E	6F	77	20	75	20	70	6F	unny....now u po
70	75	6C	72	00	00	00	00	68	61	68	61	20	6C	6F	6C	pulr....haha lol
00	00	00	00	6C	6F	6F	6B	20	77	68	61	74	20	63	72	....look what cr
61	7A	79	20	70	68	6F	74	6F	20	54	69	66	66	61	6E	azy photo Tiffan
79	20	73	65	6E	74	20	74	6F	20	6D	65	2C	6C	6F	6F	y sent to me,loo
6B	73	20	63	6F	6F	6C	00	49	20	75	73	65	64	20	70	ks cool.I used p
68	6F	74	6F	73	68	6F	70	20	61	6E	64	20	65	64	69	hotoshop and edi
74	65	64	20	69	74	00	00	77	68	65	72	65	20	49	20	ted it..where I
70	75	74	20	75	72	20	70	68	6F	74	6F	20	3A	44	00	put ur photo :D.
79	6F	75	72	20	70	68	6F	74	6F	73	20	6C	6F	6F	6B	your photos look
73	20	72	65	61	6C	79	20	6E	69	63	65	00	00	00	00	s realy nice....
6C	6F	6F	6B	00	00	00	00	68	6F	77	20	61	72	65	20	look....how are
75	20	3F	20	3A	29	00	00	68	65	79	00	4D	45	53	53	u ? :)..hey.MESS
41	47	45	20	25	73	20	25	73	00	00	00	65	63	68	6F	AGE %s %s...echo
31	32	33	00	2C	20	00	00	53	45	54	20	55	53	45	52	123., ..SET USER
53	54	41	54	55	53	20	44	4E	44	00	00	55	53	45	52	STATUS DND..USER
53	20	00	00	6C	76	00	00	72	75	00	00	6C	74	00	00	S ..lv..ru..lt..
55	49	5F	4C	41	4E	47	55	41	47	45	20	00	00	00	00	UI_LANGUAGE ....
4F	4E	4C	49	4E	45	53	54	41	54	55	53	00	00	00	00	ONLINESTATUS....
53	45	41	52	43	48	20	46	52	49	45	4E	44	53	00	00	SEARCH FRIENDS..
47	45	54	20	55	49	5F	4C	41	4E	47	55	41	47	45	00	GET UI_LANGUAGE.
53	6B	79	75	69	6A	68	2D	41	50	49	2D	43	72	2D	00	Skyuijh-API-Cr-.
53	6B	79	70	65	00	00	00	53	6B	79	70	65	43	6F	6E	Skype...SkypeCon
74	72	6F	6C	41	50	49	44	69	73	63	6F	76	65	72	00	trolAPIDiscover.
53	6B	79	70	65	43	6F	6E	74	72	6F	6C	41	50	49	41	SkypeControlAPIA

[그림 2-3] Skype 악성코드가 이용하는 메시지 및 Skype API 일부

Skype 관련 웜은 다른 MSN 메신저 웜과 달리 이전에도 소개된 Win32/Stration.worm 변형의 일부가 자신의 복사본이나 다른 변형을 유포하는 수단으로 곧잘 이용 된다.

► Win32/Virut 바이러스 변형 등장

작년에 이어서 올해도 Win32/Virut 의 피해와 이슈는 단연 독보적이다. Virut 바이러스는 안철수연구소기준으로 4개의 변형이 발견 보고 되었다. 이번 달에 발견된 변형 역시 Win32/Virut.C, D형에서 크게 벗어나지 않는다. 따라서 타사에서는 20개 이상 발견 되었다고 보도 되지만 이것은 Virut.B, C 또는 D형에서 크게 벗어나지 않는다. 이는 각 안티 바이러스 업체 기준에 따라 이것을 모두 다른 변형으로 보는지 같은 변형으로 보는지의 차이일 뿐이다. 이번에 나온 Virut 바이러스 변형은 때마침 Win-Trojan/Eldo 트로이목마와 밀접한 연관이 있는 것으로 알려져 Virut 바이러스가 더 큰 이슈를 불러왔다.

이번 달 ASEC 칼럼에서 9월에 발견된 Win32/Virut,C, D 형에 관하여 상세히 소개하고 있으니 참고하기 바란다.

(2) 스파이웨어 – 교묘해진 스파이웨어의 동의 과정

누군가 내 집의 초인종을 누르며 “잠깐 들어가도 될까요?” 하고 묻고는 주인이 미처 대답을 하기도 전에, 혹은 “누구세요?”라고 묻기만 했는데 집으로 들어온다면? 과연 이것은 무단침입이 성립 되는 것일까? 아닌 것일까? 하지만 그 결과가 무엇이 되었든 그 사람은 초대 받지 않은 손님. 즉, 불청객이라고 할 수 있다.

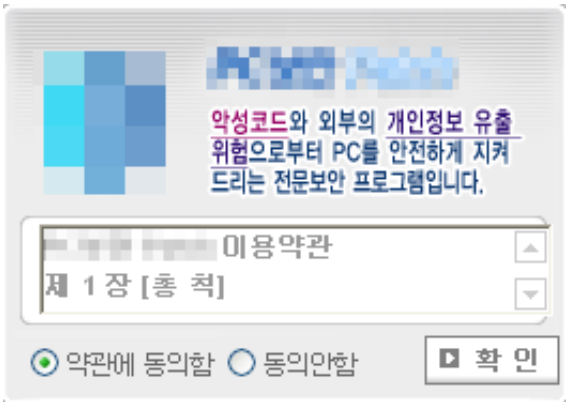
최근 내 컴퓨터 속으로 이러한 불청객과 같은 스파이웨어들이 속속 들이 모이고 있다. 첩보전을 방불케 하는 그들의 잠입 방법은 나날이 교묘해져 과거에는 사용자에게 묻지도 않고 설치되어 불법이라는 이미지를 강하게 풍겼다면, 최근의 프로그램들은 사용자의 동의를 얻는 ‘모양새’ 만 갖추는 것으로 그 방법이 바뀌었다.

사용자에게 유용한 프로그램이라 하더라도 사용자의 동의 없이 설치 되는 것은 PC 사용자의 기본적인 권리를 침해하는 것이다. 사용자의 동의를 얻는 과정 없이 설치되는 것은 당연히 스파이웨어 행위이기 때문에 스파이웨어로 분류되는 것이 마땅하다. 그리고 안티-스파이웨어 프로그램들은 그러한 프로그램을 진단/삭제한다. 이러한 연유로 국내의 많은 스파이웨어 제작업체들은 스파이웨어로 분류되어 삭제되거나 법적인 처벌을 받지 않도록 하기 위해 프로그램 설치 전 사용자의 동의를 얻는 과정을 포함시키는 것으로 그 설치 방법을 많이 변경하였다.

그런데 사용자의 적절한 동의를 얻어 설치하는 방법은 그렇게 하지 않는 방법과 비교하여 설치율이 크게 떨어질뿐더러 수익의 감소로 직결된다. 대부분이 광고를 띄우는 애드웨어이거나 그다지 필요 없는 프로그램들이기에, 사용자들이 그런 사실을 알고도 설치하는 경우는 많지 않기 때문이다. 이에 국내 스파이웨어 제작업체들은 안티-스파이웨어 업체로부터의 진단은 피하고, 설치율을 높이기 위하여 아래에서 설명하는 것들과 같은 행태를 보이게 되었다.

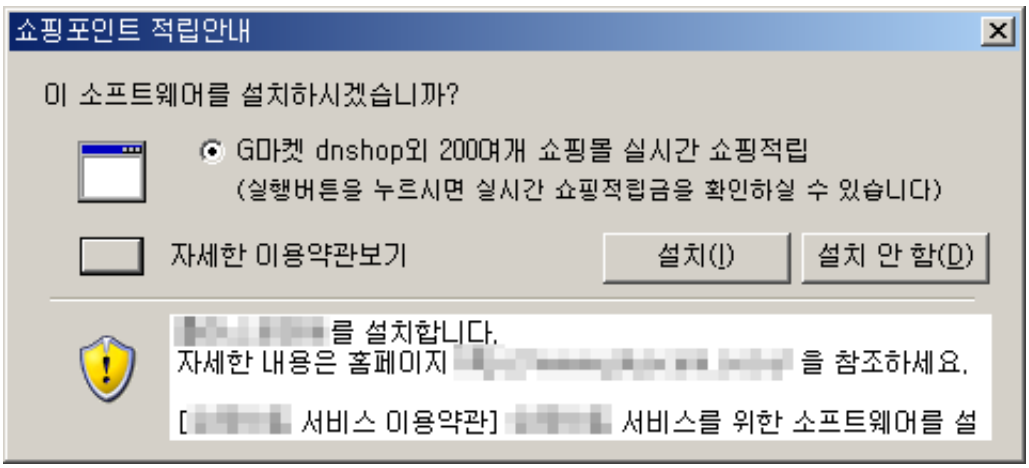
[그림 2-4] 이용 약관과 취소 버튼이 없는 설치 동의창

[그림 2-4]는 창의 버튼이 '설치'와 '확인' 버튼 밖에 존재하지 않는다. 아무리 찾아보아도 '취소' 버튼이나 '닫기(X)' 버튼은 보이지 않는다. 반드시 표시해 할 이용약관 역시 보이지 않는다. 대부분의 프로그램에서 '설치' 버튼 옆에 '취소' 버튼이 존재하는데 이 창에서는 '확인' 버튼이 있다. 그런데 이 창에서의 '확인' 버튼은 '설치' 버튼과 동일한 동작을 하는 버튼이다. 아마도 많은 사용자들이 설치를 취소하기 위해 '확인' 버튼을 누를 것이다. 하지만 이 프로그램은 사용자의 의도와는 다르게 동작한다. 결국 어떠한 방법으로든 사용자들은 이 프로그램을 설치할 수 밖에 없게 된다.



[그림 1-4] 확인하기 힘든 이용약관

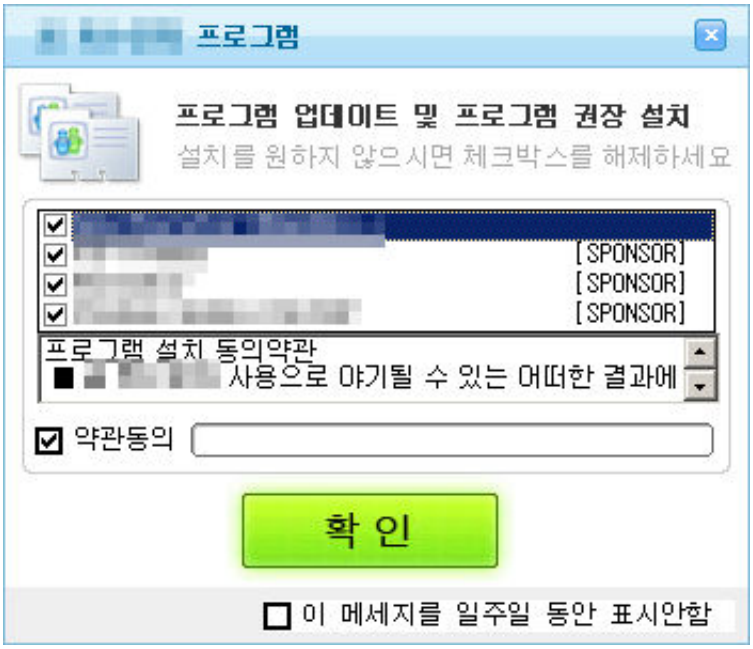
[[그림 1-4]는 이용약관을 거의 알아보기 힘들도록 작게 표시하고 이용약관에는 사용자에게 불리한 사항이 기록되어있다. 그나마 이 것은 양호한 편이다. 아래의 [그림 2-5]는 아예 스크롤 바가 존재하지 않아 처음 몇 줄 이외의 이용약관은 읽을 수 조차 없다.

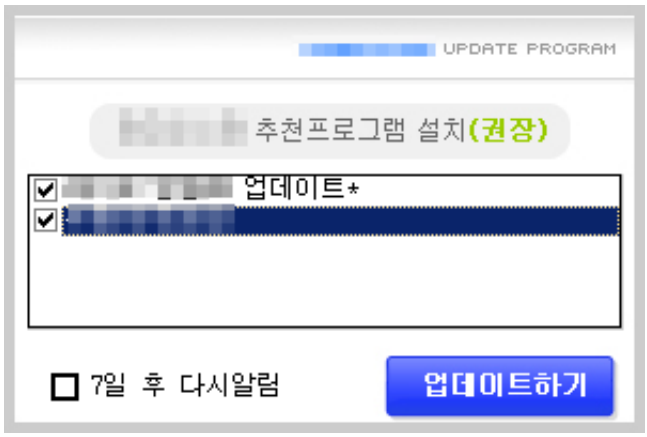


[그림 2-5] 읽을 수 없는 이용약관

[그림 2-5]의 창에서 '자세한 이용약관보기' 버튼을 누르면 이용약관이 표시되는 것이 아니라 해당 프로그램의 홈페이지로만 이동한다. 약관을 보려면 홈페이지의 약관이 있는 곳으로 찾아 들어가야만 한다.

지금까지는 집주인의 적절한 허락 없이 무단으로 들어온 것이었다. 이제부터 소개할 것은 집주인 허락 없이 들어온 것도 부족하여 다른 나쁜 친구들까지 불러들이는 경우이다. 많은 스파이웨어들이 사용자의 PC에 설치된 이후, 업데이트를 명목으로 다른 스파이웨어를 설치하려고 한다. 이 또한 사용자 동의 절차 없이 설치할 경우 스파이웨어로 분류되기에 스파이웨어 제작 업체들은 사용자의 동의를 구하는 정말 최소한의 노력만을 하고 있다.





[그림 2-6]. 적절한 동의 없이 번들 프로그램 설치

[그림 2-6]은 스파이웨어가 다른 스파이웨어를 다운로드하고 설치하기 위하여 업데이트를 한다는 식으로 사용자에게 알리고 프로그램의 설치를 유도하는 창이다. 이용약관이 아예 없거나 있더라도 너무 작아 읽기조차 힘들며 설치되는 각각의 프로그램에 대한 설명이 누락되어 있어 사용자는 무엇을 하는 프로그램인지 알 수 없고, 그냥 업데이트가 되는 것이려니 하고 생각하여 '확인' 버튼을 눌러버리는 경우가 허다하다.

지금까지 언급한 위와 같은 프로그램들의 동의를 받는 과정이 과연 사용자의 동의를 받아 설치되는 것이라고 볼 수 있을까? 당연히 그럴 수 없다. 프로그램이 설치되기 전, 사용자가 설치되는 프로그램이 자신의 PC에서 어떤 동작을 하는지 명확히 알 수 있도록 프로그램은 가능한 많은 정보를 제공해주어야 한다. 그러나 위와 같은 프로그램들은 전혀 그러하지 못하기 때문이다.

사실 위 프로그램들 중 대부분은 직접적으로 사용자의 PC에 보안상 위협을 주거나 개인 정보를 빼내거나 하는 것은 많지 않다. 대다수가 광고를 노출하거나 불필요하게 사용자의 PC에서 약간의 자원을 사용하는 것들이라, 설치되는 절차에서의 문제 이외에는 여느 프로그램과 다름 없는 프로그램으로 사용자에게 큰 피해는 주지 않는다. 그러나 사용자의 적절한 동의 없이 설치된다면 그것은 사용자의 기본적인 PC사용 권리를 침해하는 것이고 분명 잘못된 것이다.

그렇다면 이러한 프로그램들을 스파이웨어로 분류하고 법적으로 처벌하거나 안티-스파이웨어 프로그램에서 진단할 수 있을까? 일부는 그렇게 할 수 있겠지만 불행히도 전부는 그럴 수가 없다. 국내에서는 아직 프로그램이 설치될 때, 사용자 동의를 받는 과정에 대해 법적으로 적절하고 상세한 기준이 정의되어 있지 않기에 모두 스파이웨어라고 하기에는 무리가 있다. 때문에 사용자들은 부적절한 방법을 이용하여 설치되는 프로그램으로부터 입은 피해에 대해 어디 한군데 마땅히 하소연할 곳이 없는 안타까운 실정이다.

따라서 스파이웨어와 같은 원하지 않는 프로그램이 자신의 PC에 설치되지 않도록 유의하는 것이 가장 좋은 방법일 것이다. 만약 PC에 어떤 프로그램을 설치해야 한다면 불편을 없애기 위해 아래의 세가지 사항은 꼭 확인해보고 설치하도록 하자.

1. 설치 전, 이용약관을 명확히 표시하는지 확인한다.
2. 이용약관에 불합리한 조항은 없는지 확인한다.
3. 설치하려는 프로그램이 정확히 어떤 동작을 하는지 확인한다.

그리고 한가지 더 덧붙이자면 '다음' 버튼을 연속하여 눌러 설치를 곧바로 진행하는 일은 없도록 하자. 유명한 프로그램도 설치될 때, 애드웨어를 설치하는 경우가 간혹 있기 때문에 어떠한 것들이 설치되는지 확인하는 것이 중요하다.

한 번의 신중한 클릭. 당신의 컴퓨터를 보다 더 청결하게 만드는 왕도가 아닐까 하고 생각한다.

(3) 시큐리티 - 데이터 복원 이슈

마이크로소프트 보안 패치

2007년 9월에 마이크로소프트사는 [표 2-1]과 같이 총 4개의 보안 패치를 발표하였다. 발표된 보안 패치는 임의의 코드 실행이 가능한 취약점에 적용되는 것으로 해당 소프트웨어를 사용하고 있는 사용자는 반드시 해당 패치를 설치하여 만약에 있을 보안 위협을 사전에 방어해야 한다.

위험등급	취약점	PoC
긴급	Microsoft Agent의 취약점으로 인한 원격 코드 실행 문제점(MS07-051)	유
중요	Visual Studio용 Crystal Reports의 취약점으로 인한 원격 코드 실행 문제점 (MS07-052)	유
중요	UNIX용 Windows 서비스 취약점으로 인한 권한 상승 문제점(MS07-053)	무
중요	MSN Messenger 및 Windows Live Messenger의 취약점으로 인한 원격 코드 실행 문제점 (MS07-053)	유

[표 2-1] MS 9월 보안패치 요약

기존 패치와 비슷하게 클라이언트 어플리케이션에 집중적으로 보안상 문제점에 대한 패치가 발표되었다. 임의의 코드 실행이 가능한 취약점이 다수 존재하여 주의가 요구된다. 앞으로도 공격자가 불특정 다수의 사용자들을 공격대상으로 할 수 있다는 점에서 계속 클라이언트를 겨냥한 공격들이 늘어날 것으로 전망된다.

MS07-051 Microsoft Agent의 취약점으로 인한 원격 코드 실행 문제점(938827)

Microsoft Agent이 사용하는 agentdpv.dll은 특수하게 조작된 특정 URL의 길이를 올바르게 확인하지 않아 버퍼 오버플로우 취약점이 존재한다. agentdpv.dll은 Internet Explorer에서도 사용 가능한 ActiveX 컨트롤로 사용자가 관리자 권한으로 로그인되어 있는 경우 이 취약점을 악용한 공격자는 프로그램 설치, 보기, 변경, 데이터 삭제 등과 같은 권한을 얻게 되어 시스템을 완전히 제어할 수 있게 된다. 하지만, 이 취약점을 이용한 공격이 성공하기 위해서는 사용자 개입이 필요하게 된다.

Microsoft Windows 2000 제품권에 포함된 Microsoft Agent (CLSID:D45FD32B-5C6E-11D1-9EC1-00C04FD7081F)는 대화형 애니메이션 캐릭터를 사용하여 사용자가 컴퓨터를 보다 쉽게 사용하고 익힐 수 있는 방법을 제공하는 구성요소이다. agentdpv.dll이 제공하는

Characters 컬렉션의 Load함수가 URL을 처리하는 과정중 특수하게 조작된 URL이 입력되면 버퍼오버플로우가 발생하게 된다.

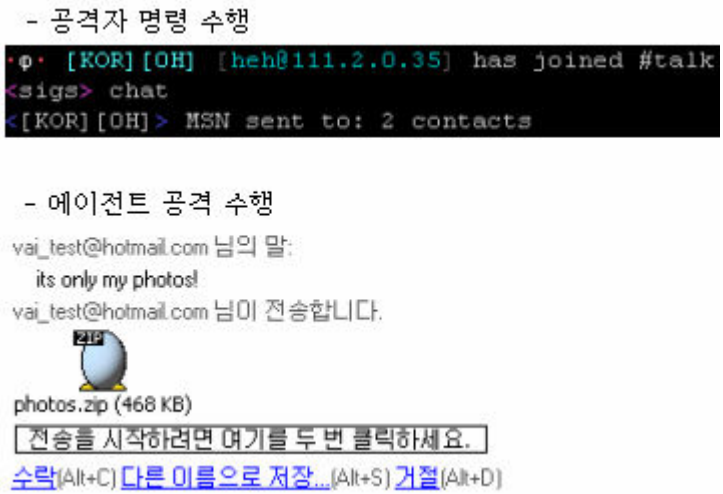
이 취약점은 원격에서 코드를 실행할 수 있는 취약점이 존재하는 것으로 관리자 권한으로 로그인되어 있는 경우, 공격자는 시스템을 제어할 수 있는 모든 권한을 얻을 수 있게 된다. 단, 일반적으로 이러한 공격에는 악의적인 공격자가 조작된 Agent ActvieX가 포함된 html 문서를 특정 웹사이트에 올려둔 후, 사용자가 조작된 홈페이지를 방문하는 사용자 개입으로 이루어진다. 이 취약점과 관련하여 보고된 것은 다음과 같다. - Microsoft Agent URL Stack Overflow Vulnerability (CVE-2007-3040)

MSN Messenger 및 Windows Live Messenger의 취약점으로 인한 원격 코드 실행 문제점 (942099)

보안취약점 공격 타겟의 중심 이동에 대해 다시 언급할 필요가 있다. 그동안 ASEC Report를 통해 OS에서 어플리케이션 레벨로 보안취약점 악용 사례가 현저히 증가하고 있음을 경고해 왔다.

메신저는 강력한 기업 내 주요 통신수단의 하나로 자리잡은 지 오래되었고, 공격자의 주요 공격 수단으로 활용되어 온 것이 사실이다. 메신저의 주요 기능이 악의적인 목적에도 그대로 활용되고 있고, 공격자가 봇넷을 구성하여 감염된 PC를 통해 메신저를 손쉽게 제어하고 있다.

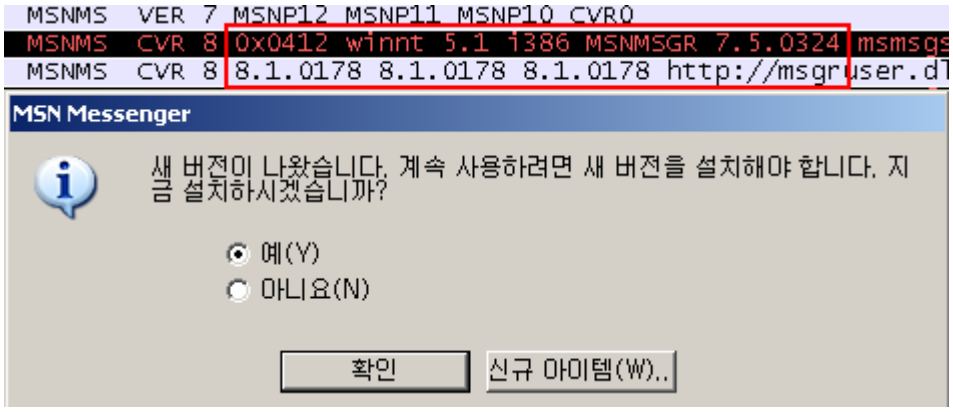
- 대화문자 전송: 악성코드 URL 전파, URL 클릭 유도
- 파일 전송: 악성코드 파일 전파 (zip형태)
- 화상 전화: 화상전화를 처리하는 구성요소의 취약성 공격을 통한 원격코드 실행



[그림 2-7] 봇넷에 의해 제어되어 MSN 메신저로 전파되는 악성코드

이번 MS07-054 MSN 메신저 및 라이브 메신저의 취약성은 웹캠을 이용하는 화상 전화 이용시 발생되는 패킷 조작으로 인한 원격코드 실행이 가능한 점이 특징이다. 공격자는 화상 전화 채팅 초대를 통해 공격코드를 삽입하는 방식으로 취약점을 이용, 공격하게 된다. 공격받는 사람은 화상 전화 채팅 요청을 수락하면 버퍼 오버플로우가 발생하게 되며, 이 때문에 프로그램이 종료되면서 공격자의 실행 코드가 실행된다.

최근 발표된 MSN 메신저을 비롯하여 Yahoo 메신저 취약성이 공개된 적 있으나, 아직까지 해당 취약점에 의한 악용사례는 보고된 바 없다. 또한 다행인 것이, MSN 메신저의 경우 보안취약한 버젼을 사용하는 이용자가 MSN 서비스에 접속하는 경우, 반드시 보안업데이트 된 새로운 버젼으로 업데이트하도록 유도하는 등의 방안을 채택하고 있어 발빠르게 취약점의 악용 사례를 방지하고 있다는 점이다. 다른 어플리케이션 제품 벤더들도 보안취약성을 갖는 제품이 인터넷 상에서 서비스되지 않도록 하는 강력한 보안 업데이트 방식을 채택해야 한다.



[그림 2-8] MSN 메시저 버전 업데이트

[그림 2-8]과 같이 필자가 웹캠 공격에 취약한 MSN Messenger 7.5버전으로 MSN 서비스 접속을 시도하자 취약점이 패치된 새로운 버전으로 업그레이드를 요구하고 있다. 이 취약점과 관련하여 보고된 것은 다음과 같다. – MSN Messenger Webcam or Video Chat Session Remote Code Execution Vulnerability (CVE-2007-2931)

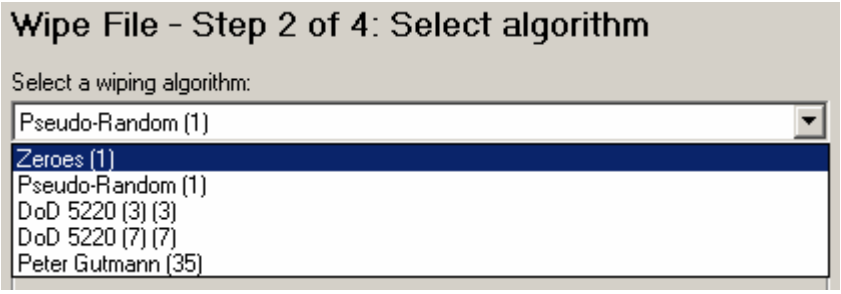
삭제된 데이터의 복원 가능성

이 글을 접하고 있는 독자에게 먼저 묻고자 한다. 자신의 소중한 데이터를 자신도 모르게 삭제한 경험이 있는가? 만약 있다면, 어떠한 방법을 이용하여 삭제된 데이터를 복원하였는가? 복원 프로그램을 구하거나 데이터 복구업체에 직접 하드디스크를 가지고 들고 뛰어본 경험들이 있을 것이다. 어쩌면 우리는 이미 삭제된 데이터의 복원 가능성에 대해서, 또는 실수로 삭제된 데이터의 복구의 중요성에 대해서 알고 있다는 사실을 잊고 있었을지도 모른다.

삭제된 기업 및 개인의 중요 정보가 하드 디스크로부터 복원되어 그대로 유출될 수 있다는 것이 사회적 이슈와 더불어 다시금 언론을 통해 세상에 공개되었다. 사건과 사고는 수없이 발생하고, 디지털포렌식 과정에서 수집된 휴대폰 통화기록, 네비게이션 위치 정보, 이메일 내용, 하드디스크 내의 중요 파일 등의 개인정보들이 용의자를 검거하는 데 결정적인 단서가 되기도 하고, 때로는 기업 및 개인정보의 유출 가능성에 대한 우려를 낳기도 한다.

이에 따라, 파일의 완전삭제 방법에 대한 이용자의 관심이 날로 커지고 있다. 이용자의 선택을 기반한 데이터 파일의 완전삭제기능에 대한 편의성을 충분히 제공할 수 있도록 한다. 하드디스크 내 파일을 완전 삭제하는 방법에는 크게 다음과 같이 구분된다.

- 방법1: 멀티미디어 파일과 같은 대용량 파일로 하드디스크 채움 (덮어쓰기)
- 방법2: 공개/사용 데이터 복구 방지 프로그램 이용 (Zeros / Pseudo-Random / DoD 5220 / P. Gutmann 방식)
- 방법3: 하드웨어의 물리적 파괴 (재생 의도 없을 경우)



[그림 2-9] ObjectWipe에 채용된 파일완전삭제 알고리즘

또한, 기사용된 PC를 폐기하는 경우 기업 및 개인 정보가 유출되지 못하도록 하드디스크 폐기 절차 등에 대한 보안정책을 수립, 적용할 필요가 있다.

- 개인 PC 사용의 경우, 외부에서 원격 접속하여 파일 시스템에 원격 접근하는 일을 사전에 방어하도록 한다.
- 게임방 혹은 타사 방문 등 외부의 공동PC를 이용하는 경우 되도록 기업 및 개인의 중요 파일을 저장하여 조작하는 행위를 금하도록 하고, 부득이하게 외부 PC에서의 작업이 진행되는 경우 데이터 복구 방지 프로그램의 파일 완전 삭제 기능을 작업한 중요파일을 복원할 수 없도록 조치한다.
- 개인 PC를 반납하거나 폐기하는 경우, PC 내 하드디스크의 파일을 복원할 수 없도록 데이터 복구 방지 프로그램을 이용하거나, 재사용할 수 없도록 파괴한다.

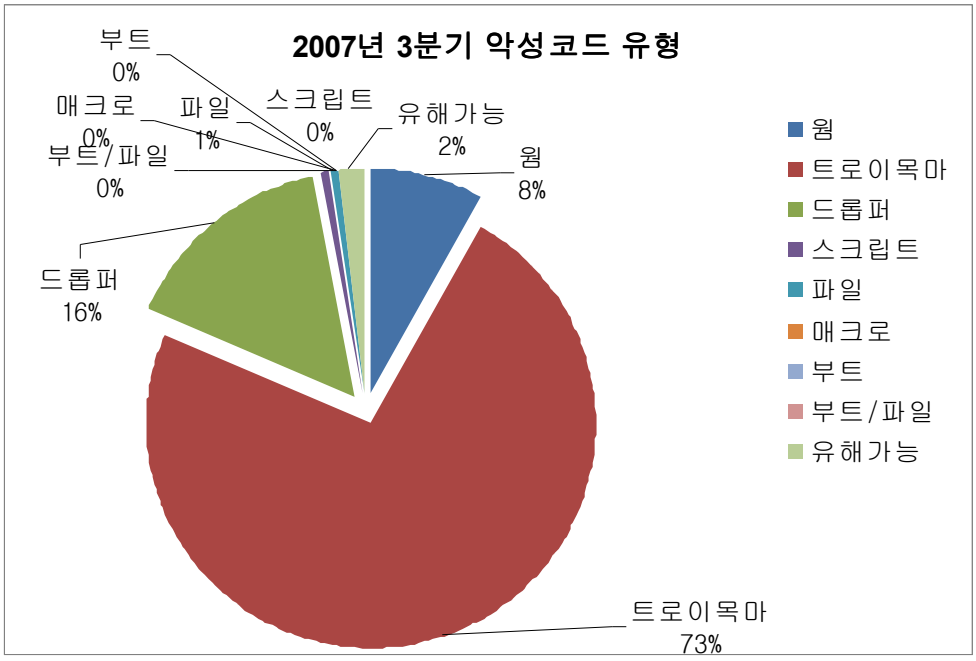
[참고] 완벽하게 파일을 지우는 방법

- http://kr.ahnlab.com/securityinfo/infoView.ahn?seq=10687&category=15

III. 2007년 3/4분기 동향

(1) 2007년 3/4분기 악성코드 동향

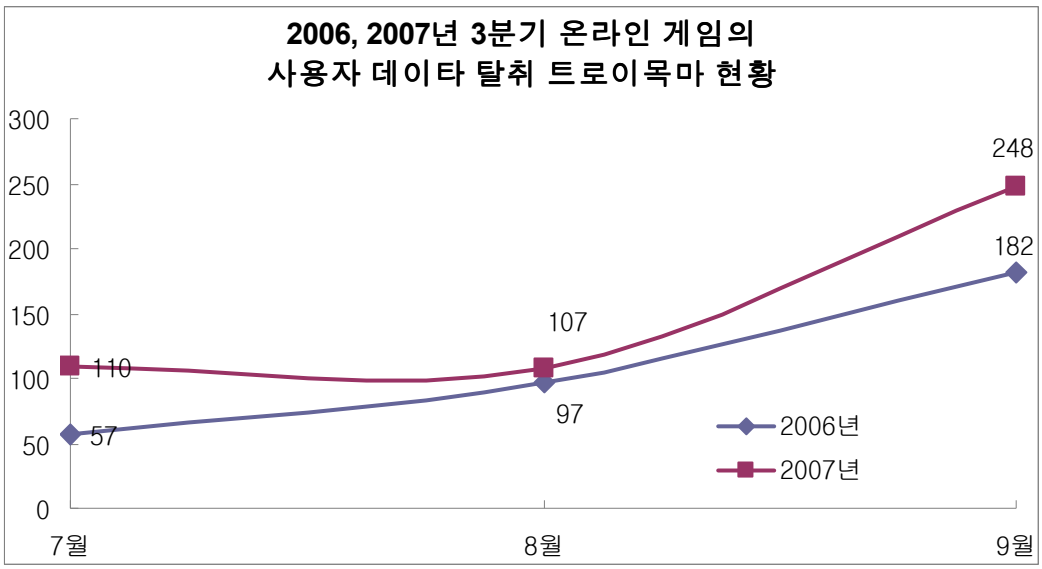
3분기 신종 및 변형에 대한 악성코드 동향은 전반적으로 상반기 악성코드 유형을 그대로 따르고 있다. 세계를 뒤흔드는 가공할만한 악성코드나 취약점은 보고 되지 않고 있으며, 대신 은밀하게 자신의 목적을 수행하는 악성코드의 수는 여전히 증가하고 있는 추세이며 일반 사용자들은 대부분이 이에 대하여 무방비로 노출 되어 있는 경우가 많았다. 다음은 3분기 악성코드 유형이다.



[그림 3-1] 2007년 3분기 악성코드 유형

트로이목마의 유형이 압도적으로 많으며 지난 상반기의 경우 전체 악성코드에 대한 트로이목마의 비율은 70%였고 단순 비교하기는 어렵지만 3분기에는 73% 로 소폭 상승하였다.

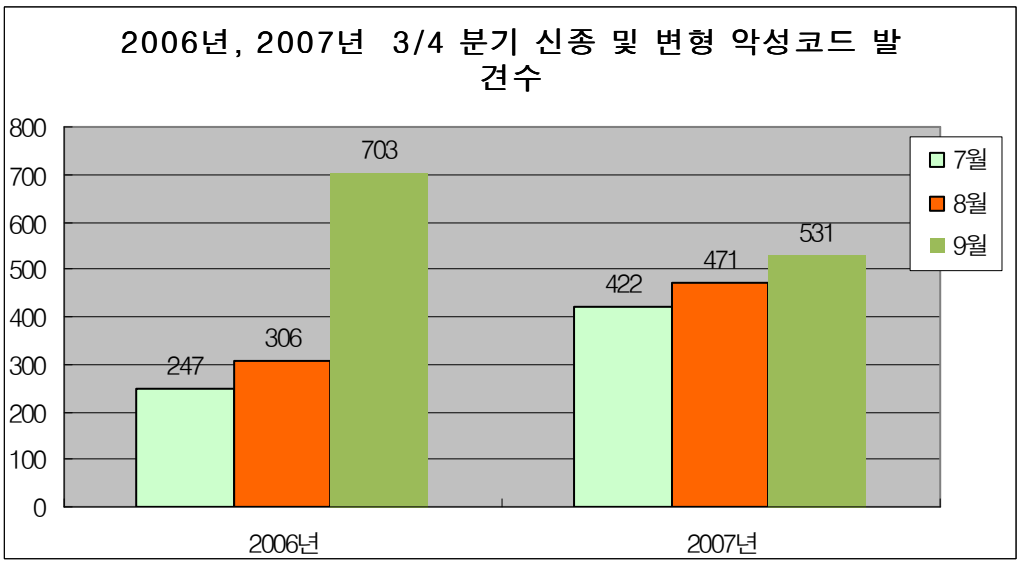
이중에서 가장 큰 비중을 차지하는 온라인 게임의 사용자 계정을 탈취하는 트로이목마의 3분기 추세는 다음과 같다. 작년 동기와 더불어 상승추세에 있다.



[그림 3-2] 2006, 2007년 3분기 온라인 게임의 사용자 데이터 탈취 트로이목마 발견 수

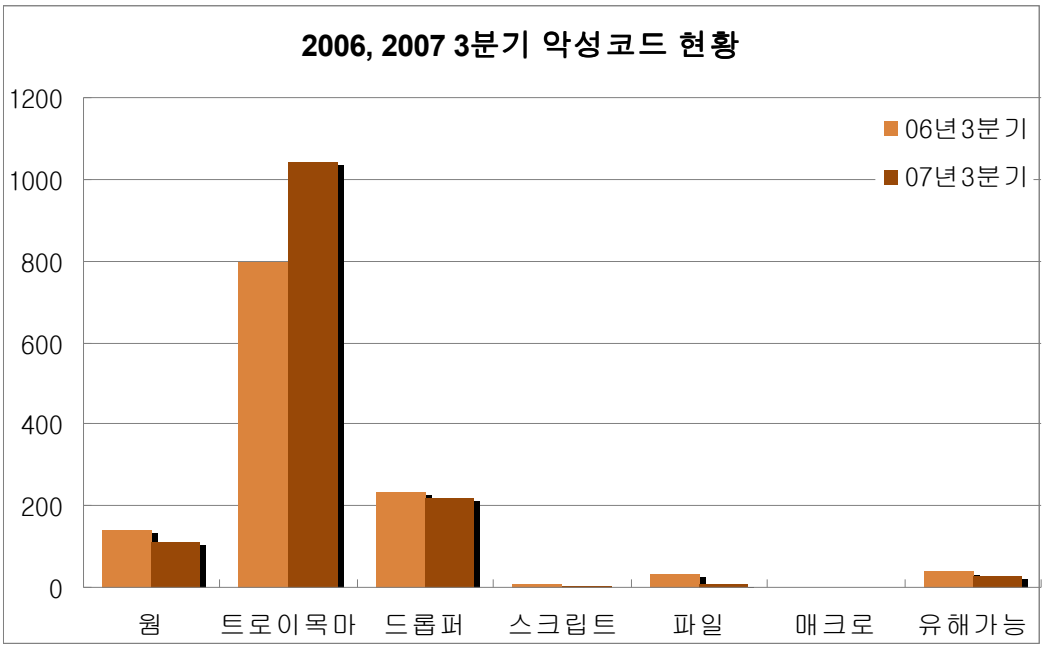
특히 9월달에 발견된 악성코드 수는 올해 가장 많이 보고된 수이기도 하다. 또한 상반기와 더불어 3분기 역시 국내보다는 중국내 온라인 게임을 타켓으로 하는 악성코드의 수가 더 많았다.

다음은 작년 동기와 비교한 악성코드 발견 수이다. 참고로 작년 9월에는 인터넷 익스플로러 관련 취약점을 이용한 악성코드 급증 및 Win32/Viking 바이러스 증가로 인하여 매우 높은 발견 수를 보이고 있다. 그러나 9월을 제외한다면 올해 3분기가 전체적으로 작년 동기 대비 하여 13% 가량 올해 상승 하였다.



[그림 3-3] 2006, 2007년 3분기 신종 및 변형 악성코드 발견수

트로이목마의 비율은 작년 동기보다 높으나 바이러스 유형은 작년 동기에 비하여 낮다. 작년에는 중국산 바이러스인 Win32/Viking, 그리고 Win32/Dellboy 변형 바이러스의 폭발적인 증가로 인하여 바이러스 비율이 높다.



[그림 3-4] 2006, 2007년 3분기 악성코드 현황

그러나 올해 들어 이 두 바이러스중 Dellboy 제작자가 검거가 되고 V3를 비롯한 안티 바이러스 엔진에서 Generic 하게 진단 되는 등 진단방법이 강화 되었기 때문에 이 바이러스에 대한 변형의 수는 작년 동기 대비하여 변형이 일부만 발견, 보고 되고 있다.

다음은 3분기에 이슈가 되었던 악성코드를 정리해보았다.

► 자기 보호 기능이 있는 Win-Trojan/Runtime 트로이목마

메일을 통해서 광범위하게 확산된 이 트로이목마는 국내외적으로 피해 사례가 많이 보고 되었다. 메일 제목과 본문에 매우 자극적이고, 당시에 대중적인 소재를 사용하여 많은 사용자들이 첨부된 파일의 실행하도록 유도 하였다. 메일에 첨부된 파일은 드롭퍼 또는 다운로더로 진단되며 변형이 매우 많다.

V3에서는 Win-Trojan/Agent.20992.CK 또는 Dropper/Agent.20992.XXX(XXX 는 임의의 알파벳)로 진단되고 있으며, 실행 후 특정 호스트로부터 파일을 다운로드하며 자신의 파일과 프로세스를 은폐하고 Covert Channel (은닉 채널)을 이용하여 스팸메일을 발송한다. 따라서

감염되어도 사용자는 감염여부를 알기 어렵고, 자기보호기능이 뛰어나 일반적인 방법으로 치료가 매우 어려우며 자신을 제거하려하면 다시 복구하려는 자기보호기능이있다.

► MSN 메신저 웜의 기승

올해 MSN 메신저를 비롯한 메신저로 전파되는 악성코드가 부쩍 증가 하였다. Win32/ShadoBot.worm, Win32/MSN.worm, Win32/MSGBot.worm 등으로 명명된 악성코드는 모두 MSN 을 이용하여 자신을 전파시키는 웜이다. Win32/Stration.worm.Gen 의 일부 변형은 자신의 변형을 Skype 또는 다른 메신저로 전파하기도 한다.

2005년도 비슷하게 Win32/Kevir.worm, Win32/Bropia.worm 등으로 인한 피해가 급증하였는데, 그 당시의 MSN 웜과 최근 발견되는 MSN 웜과의 차이는 BotNet의 직접적인 이용 여부에 있다. 즉, 2005년에 극성을 부린 MSN 웜은 악성 IRCBot 웜을 다운로드 또는 내부에 별도의 실행파일을 포함하고 이를 실행하는 것이 주목적이였다면, 최근에 발견되는 MSN 웜의 특징은 BotNet 직접 접속하고 IRCBot 기능과 자신을 전파시키기 위한 수단으로 윈도우 OS 취약점이 아닌 MSN 메신저를 노렸다는데 있다. 또한 MSN 으로 자신을 전파 하려는 증상은 BotNet 에 접속 후 접속 한 채널의 공격자가 명령을 내려야만 동작하므로 메신저를 이용한 전파 증상이 재현 될 수도 있고 재현 되지 않을 수도 있다.

► Win32/Virut 과 DDoS 공격의 가능성?

국내에서 Win-Trojan/Eldo.10240 라는 트로이목마에 의해서 해당 트로이목마가 감염된 네트워크 환경에서는 트래픽이 과도하게 발생하는 이상 현상이 발생했다. 먼저 이 트로이목마가 어떤 경로로 국내에 다수의 시스템들에 감염 되었는지 명확하지 않다. 이 트로이목마가 발견된 시스템에서 Win32/Virut 바이러스가 발견되어 Win32/Virut에 의하여 DDoS 공격이 발생한 것으로 언론을 통하여 발표가 되었지만 단정할 수는 없다.

이전의 Virut 바이러스 변형이 VT100.exe 란 파일명을 갖는 은폐형 악성코드를 다운로드 하여 실행한 전력이 있기 때문에 가능성은 있다. Virut 은 특정 IRC 서버에 접속하여 명령을 받을 수 있는데 특정파일을 다운로드 & 실행 할 수 있는 명령을 가지고 있다. 따라서 Virut 바이러스 또는 변형이 Win-Trojan/Eldo.10240 을 다운로드 하여 실행 한 후 트로이목마가 특정 웹 사이트 접속을 하는데 이때 접속이 실패 되면 지속적인 접속요청을 하는데, 이 때 대량의 SYN 패킷이 발생하여 마치 DDoS 공격으로 보일 수도 있었을 것으로 추정된다.

► Win32/Zhelatin.worm 의 기승

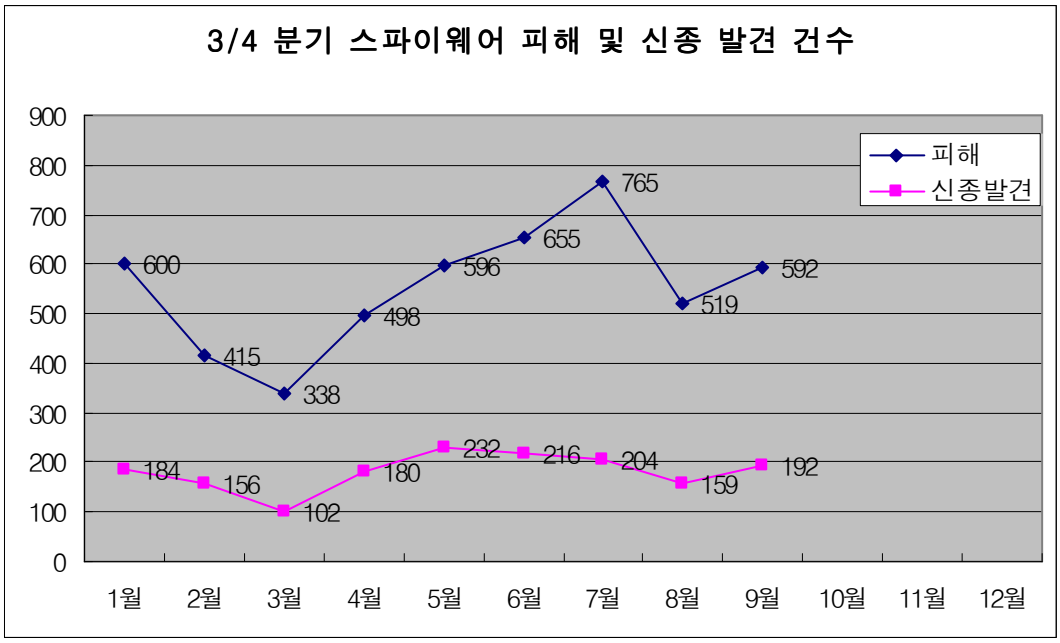
Win32/Zhelatin.worm 은 잘 알려진 악성코드로 감염된 시스템의 안티 바이러스 및 보안 프

로그램을 무력화 시키며 메일 주소를 수집하여 자신의 변형 및 스팸 메일을 발송한다. 또한 감염된 다른 시스템들과 암호화된 내용으로 오버넷이라고 알려진 일종의 파일 공유 관련 프로토콜을 이용하여 P2P 네트워크를 구성한다. 이는 감염된 시스템들만 사용되도록 private network 를 구성한 후 악의적인 사용자 또는 감염된 시스템들로부터 정보를 획득하여 특정 파일을 다운로드 및 실행 할 수 있도록 해둔다.

안티 바이러스로부터 진단을 회피하기 위해 암호화된 자신의 코드를 풀어 낼 때 바이너리에 하드코딩된 키값이 아닌 랜덤한 쓰레기 API 의 호출 한 후 리턴되는 인자값을 복호화 키로 사용하는 동적인 방법으로 키값을 구해서 자신을 복호화한다. 이와 같이 동적인 키값을 사용하는 이유는 진단 또는 분석을 방해하도록 가상머신이나 에뮬레이터에서 자신이 실행 되지 않도록 하기 위해서이다.

끝으로 3분기 악성코드 동향을 정리해보면 상반기와 마찬가지로 은밀하게 동작하면서 스팸 메일 발송과 자신의 Botnet 을 구성하는 악성코드들이 문제가 되고 있다. 또한 중국산 악성코드의 경우 한 개의 다운로더가 대량감염 시도하는 마치 인해전술과 같은 현상도 하나의 트렌드로 잡아가고 있다. 그리고 메신저를 전파 수단으로 사용하는 악성코드의 증가도 관심을 가지고 주의를 기울일 필요가 있다.

(2) 2007년 3/4분기 스파이웨어 동향



[그림 3-5] 2007년 3/4분기 스파이웨어 피해 및 신종발견 건수

[그림 3-5]는 2007년 3/4분기 스파이웨어 피해 및 신종발견 건수를 나타내는 그래프이다. 1월부터 9월까지 월 평균 약 550건의 스파이웨어 피해 신고가 접수 되었으며, 7월에 최고 수치인 765건을 기록하고 있다. 분기별로는 3/4 분기 피해 신고 건수가 1868건으로 최고 수치를 기록하고 있다. 신종 및 변형 스파이웨어는 월평균 약 180건이 보고되었으며, 피해신고, 신종 및 변형 발견 건수 모두 3월에 가장 낮은 수치를 보이다가 점차 증가하여 8월에는 다소 감소한 모습을 보이고 있다. 3/4 분기에는 국내에서 제작 배포되는 허위 안티-스파이웨어와 애드웨어가 특히 많은 피해를 입혔으며, 중국발 해킹으로 시작되는 온라인게임 계정 유출 스파이웨어의 경우 1월부터 현재까지 꾸준한 피해를 입히고 있다.

3/4분기 스파이웨어의 특징은 다음과 같이 요약할 수 있다.

► 국내 스파이웨어 설치 방법의 변화

2007년 상반기 국내 제작 애드웨어 및 허위 안티-스파이웨어의 수가 증가하였다. 국내에서 제작되는 애드웨어 또는 허위 안티-스파이웨어는 배포 방법으로 불특정 웹 사이트에서 ActiveX 컨트롤 설치에 대부분 의존하였으나 하반기에 들어서면서 다운로더를 이용하는 번들 소프트웨어 설치로 배포 방법이 변화하고 있다. 이미 설치된 애드웨어는 별도의 다운로더를 이용하여 여러 다른 애드웨어의 설치 파일을 사용자 동의 없이 다운로드하고 실행할 수 있다. 따라서 실수로 설치한 단 한 개의 애드웨어에 의해 여러 개의 애드웨어 또는 허위 안티-스파이웨어가 설치될 수 있다. 정상적인 동의를 받고 설치되는 프로그램이라 하더라도

프로그램 사용 약관에 “다른 소프트웨어의 설치 광고 전달을 할 수 있다.”는 문구가 포함된 것도 있어 용도가 불분명한 프로그램을 설치할 때는 각별한 주의가 필요하다.

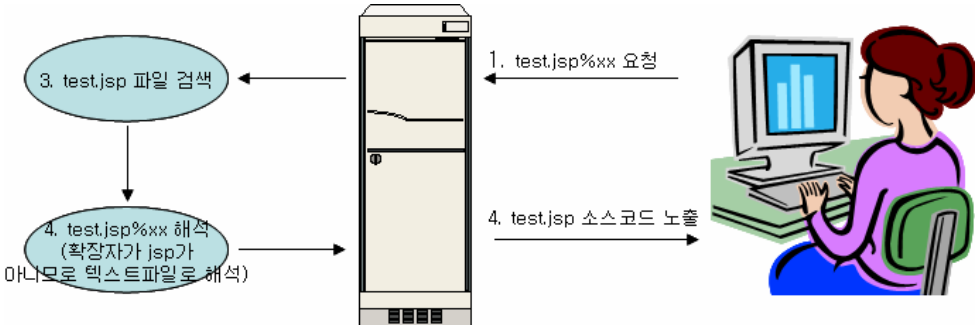
► 바이러스에 감염된 스파이웨어

악성코드 중에서도 바이러스는 시스템 무결성을 해치고 오류를 일으키거나 예기치 않은 동작을 유발하기 때문에 매우 위험하다. 이들 바이러스는 웜, 트로이 목마와 같은 다른 악성코드에 의해 또는 바이러스에 감염된 파일 실행에 의해 감염되는 것이 일반적이지만, 바이러스에 감염된 스파이웨어에 의해 확산되기도 한다. 2007년 8월에는 허위 안티-스파이웨어 프로그램이 바이럿 바이러스(Win32/Virut) 바이러스에 감염된 채로 배포되기도 하였다. 스파이웨어는 그 자체로 사용자 권리를 침해하고 광고와 같이 사용자가 원하지 않는 동작을 하기도 하지만 보안을 크게 위협하지는 않으나 바이러스에 감염된 채로 배포되는 경우 보안에 치명적인 위협으로 존재할 수 있다.

(3) 2007년 3/4분기 시큐리티 동향

티맥스 미들웨어 제우스의 디렉토리 및 소스코드 노출 취약점

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



[그림 3-6] 제우스(JEUS) 취약점

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

플래시 플레이어 취약점

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

```
0000000: 464c 5601 0500 0000 0900 0000 0012 0000  FLV.............
0000010: 7c00 0000 0000 0000 0200 0366 6f6f 0cff  |..........foo..
0000020: ffff ff[illegible]                       ...[illegible]
```

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

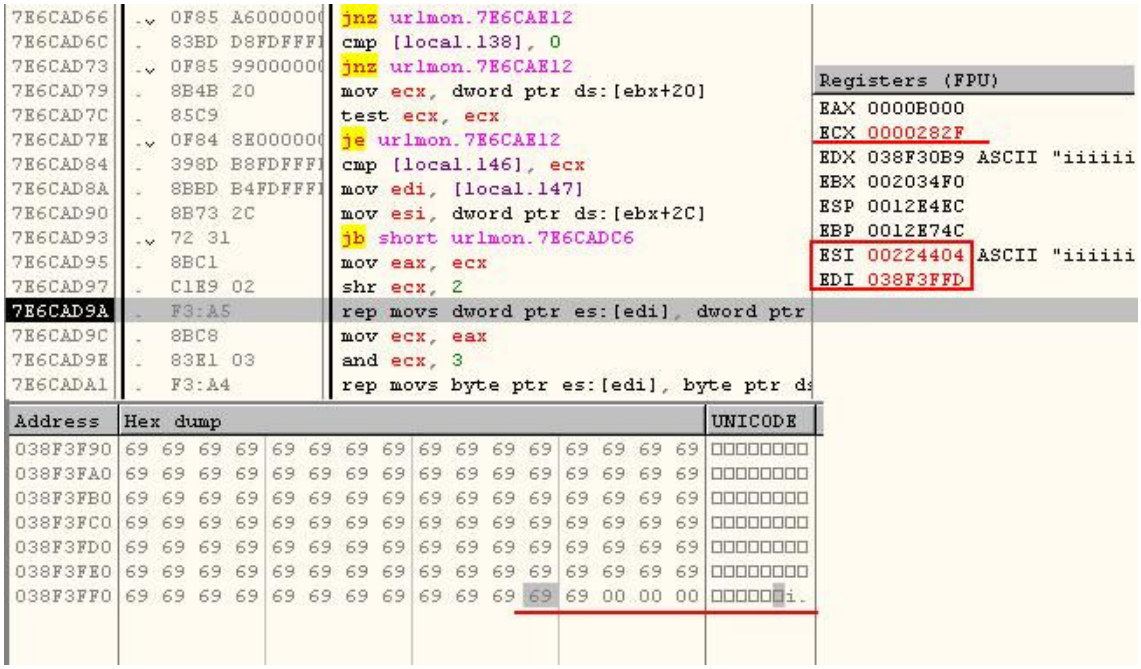
Ms07-042 Microsoft XML Core Services의 취약점으로 인한 원격 코드 실행 문제점

Microsoft XML Core Services(MSXML)는 JScript, Visual Basic Scripting Edition(VBScript), Microsoft Visual Studio 6.0을 사용하여 XML 1.0 표준을 준수하는 다른 응용 프로그램과 상호 운용성을 제공하는 XML 기반 응용 프로그램을 개발할 수 있도록 제공해 준다. 이러한 XML Core Services의 보안 취약점을 통해 공격자는 Internet Explorer(IE)를 통해 특수하게 조작된 웹사이트를 만들어 불특정 사용자를 공격할 수 있다. 공격자는 이로 인해 로그인 된 사용자의 모든 권한을 획득 할 수 있다.

var JScript
= new ActiveXObject("Microsoft.XMLDOM"); = new ActiveXObject("msxml2.DOMDocument"); = new ActiveXObject("Msxml2.DOMDocument.3.0");
VBScript
set xmlDoc = CreateObject("Msxml2.DOMDocument.3.0")
CLSID
<object classid="clsid:f6d90f11-9c73-11d3-b32e-00c04f990bb4" id="xmlDoc"></object>

MS07-050 벡터 표시 언어의 취약점으로 인한 원격 코드 실행 문제점

Microsoft Windows에 구현된 VML(벡터 표시 언어)에 원격 코드 실행 취약점이 존재한다. VML(벡터 표시 언어)은 업무용 사용자 및 그래픽 디자인 전문가의 요구를 모두 만족하도록 웹에서 고화질 벡터 그래픽을 교환, 편집, 배포하는 XML 기반 형식이다. 이 취약점은 압축된 HTTP response 데이터를 받을 때 VML(vgx.dll)을 처리하는 과정에서 integer underflow를 일으키게 된다. 공격자는 특수하게 조작된 웹 페이지나 HTML 전자 메일을 구성하여 이러한 취약점을 악용할 수 있다.



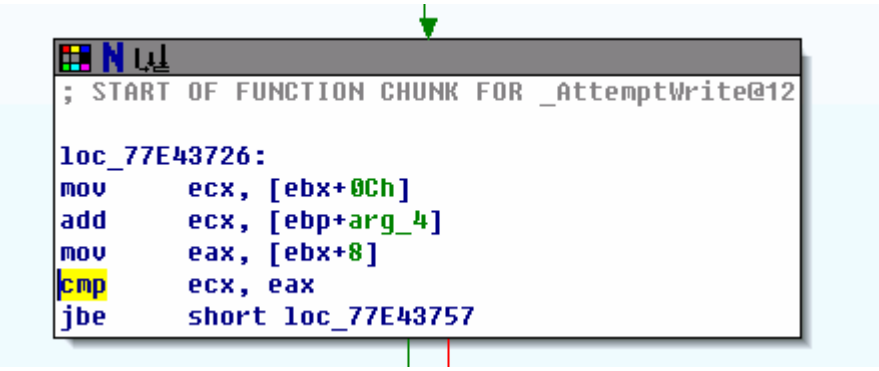
MS07-046 GDI의 취약점으로 인한 원격 코드 실행 문제점

그래픽 렌더링 엔진 GDI32.DLL 에서 특수하게 조작된 이미지를 처리하는 방식에 원격 코드 실행 취약점이 존재한다. 그리고, 이 취약점을 악용한 공격자는 프로그램의 설치, 보기, 변경, 데이터 삭제등과 같은 권한을 얻게 되어 시스템을 완전히 제어할 수 있다. 공격자는 특수하게 조작된 WMF을 파일을 전자 메일에 첨부하여 발송하거나 웹을 통하여 배포한 후 사용자가 해당 파일을 열게 되면 원격 코드가 실행되는등의 비정상적인 동작을 유발할 수 있다.

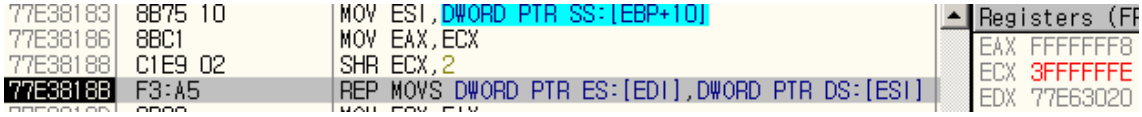
```
typedef struct _WindowsMetaHeader
{
  WORD  FileType;       /*Type of metafile (0=memory, 1=disk) */
  WORD  HeaderSize;     /* Size of header in WORDS (always 9) */
  WORD  Version;        /* Version of Microsoft Windows used */
  DWORD FileSize;       /* Total size of the metafile in WORDs */
  WORD  NumOfObjects;   /* Number of objects in the file  */
  DWORD MaxRecordSize;  /* The size of largest record in WORDs */
  WORD  NumOfParams;    /* Not Used (always 0) */
} WMFHEAD;

typedef struct _StandardMetaRecord
{
    DWORD Size;           /* Total size of the record in WORDs */
    WORD  Function;       /* Function number (defined in WINGDI.H) */
    WORD  Parameters[];   /* Parameter values passed to function  */
} WMFRECORD;
```

[그림 3-7] Windows Meta File 파일 포맷



[그림 3-8] Integer Overflow(정수 오버플로우) 발생 코드



마이크로소프트 오피스 취약점의 꾸준한 증가

일반적으로 MS 오피스의 취약점은 특정 오브젝트의 특정 필드에서 Overflow 버그가 발생하거나, 오피스 공통 라이브러리에서 취약점이 발견되는 경우도 존재한다. 2007년 3사분기 발표된 MS 오피스 취약점은 아래와 같다.

- 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)

MS 오피스 취약점은 2006년 상반기부터 본격적으로 나타나기 시작하였다. MS 사의 보안 패치 중에 2006년과 2007년 9월까지 MS 오피스 공격에 이용될 수 있는 취약점은 총 25건이다. 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.

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 제로 데이(Zero-Day) 공격에도 자주 사용이 되고 있기 때문에, 주의가 필요하다. 9월에 MS 오피스 2003의 서비스팩 3가 발표 소식이 있었는데, 이번 2003 SP3 에서 주요 변경사항은 보안이 보다 강화되었다. 주요 특징은 아래와 같다.

- 비스타에서의 호환문제
- 오피스 2007과의 호환문제
- 확장된 보안 – MOICE (Microsoft Office Isolated Conversion Environment), File Block

오피스 2003 사용자들은 SP3를 사용하는 것이 악성코드나 취약점등으로부터 예전보다 좋은 방법으로 방어할 수가 있으니, 반드시 이용하도록 하자.

오픈오피스 취약점

2007년 9월에 OpenOffice TIFF 취약점인 발표되었는데, TIFF 에서는 Image File Directory를 포함하고 있는데, Image File Directory의 Data Count 에서 정수 연산을 잘 못하여, Integer Overflow가 발생하는 취약점이다. 오픈오피스는 MS오피스 보다 아직 사용자수가 많지 않지만, 오픈오피스의 사용자수가 점차 늘어나고 있는 추세이다. 이에 오픈오피스 관련 취약점에 대해서 살펴보도록 하자.

1. 오픈오피스 취약점이란 무엇인가?
오픈 오피스(http://www.openoffice.org) 프로그램은 선 마이크로시스템즈에서 개발한 스타 오피스(StarOffice)에 기반을 하고 있으며, 대다수 사용자가 이용하는 응용 프로그램으로 스프레드 시트 프로그램인 Calc, 문서 작성/편집 프로그램인 Writer, 멀티미디어 프리젠테이션 관련 프로그램인 Impress, 데이터 베이스 관련 프로그램인 Base, GUI 로 구성된 수학 프로그램인 Math등으로 구성되어있다.

오픈 오피스 취약점은 이러한 오피스 프로그램 및 오피스 라이브러리에 버그(Bug)가 존재하는 것을 말한다. 사용자가 악의적으로 조작된 오피스 관련 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. 오픈 오피스 프로그램의 사용은 점차 늘어나는 추세이며, Platform Independent 하기 때문에, 리눅스, 윈도우, 솔라리스, 맥 OS X등에서 동작함으로 위험의 심각도가 있다고 볼 수 있다.

2. 오픈 오피스 취약점 동향 및 피해사례

오픈 오피스 취약점은 2006년 상반기부터 점차 나타나기 시작하였다. 해당 취약점들은 오픈 오피스에서 사용되는 매크로부터 시작하여 이미지 및 문서를 parse 하는데 필요한 관련 라이브러리 등의 버그등((libcurl, Macro, WMF, EMF, libwpd, RTF, TIFF)에 이르기까지 다양한 추세로 발견되고 있다. 이러한 취약점 유형은 마이크로소프트의 오피스 취약점 추세와 비

숫하게 볼 수 있다.

지난 5월 외국에서는 오픈오피스의 매크로 취약점을 이용한 SB/BadBunny-A 가 발견되었는데, SB/BadBunny-A 는 오픈오피스의 취약점을 이용한 최초의 악성코드라고 볼 수 있겠다. 그러나, 국내에는 SB/BadBunny-A에 의한 피해는 발견되지 않았다.

오픈 오피스의 사용이 증가할 수록 오픈 오피스의 취약점을 이용한 악성코드가 증가할 것으로 예상이 되는데, 취약점을 이용한 공격에는 조작된 파일을 특정/불특정 사용자에게 메일 또는 웹으로 전달하여 사용자가 해당 오피스 관련 파일(File) 읽는 경우 임의의 코드 또는 악성코드를 실행할 수 있게 된다. 오피스 파일 내부에 있는 악성코드는 주로 트루잔(Trojan) 및 다운로더(Downloader)등이 포함되어 있다. 오픈 오피스 프로그램의 취약점을 이용한 공격중에 매크로 취약점을 제외한 Overflow 취약점을 이용한 경우에는 OS에 의존적으로 작성되어야 하는 점이 있다. 또한 오피스 취약점을 이용한 공격은 주로 특정 목적을 가지고 수행되는 경우가 많으며, 개인 및 기업등의 민감한 정보를 노리는 것으로 파악되어 보다 주의가 필요하다.

3. 사용자가 유의해야할 점

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

은행 인터넷 뱅킹 문제점

지난 8월에 현 시대에 없어서는 안될 인터넷 뱅킹 보안 문제가 KBS 뉴스 방영 이후 수면위로 떠올랐다. 이 문제점은 게임 해킹 프로그램과 거의 유사하게 동작하며, 이 공격에 의한 피해는 인터넷 뱅킹을 이용하여 계좌이체를 할 경우 자신의 의도와는 다르게 공격자나 다른 계좌 이용자에게 금액을 이체 시킬 수 있다. 또한 보내고자 하는 이체 금액도 공격자 마음대로 조작이 가능한 것으로 타났다. 아직까지 이를 이용한 악성코드 등은 없으나 사용자의 각별한 주의가 요구된다.

이번 인터넷 뱅킹 보안 문제는 이용자가 인터넷 뱅킹을 통해 계좌 이체를 할 경우 입력한

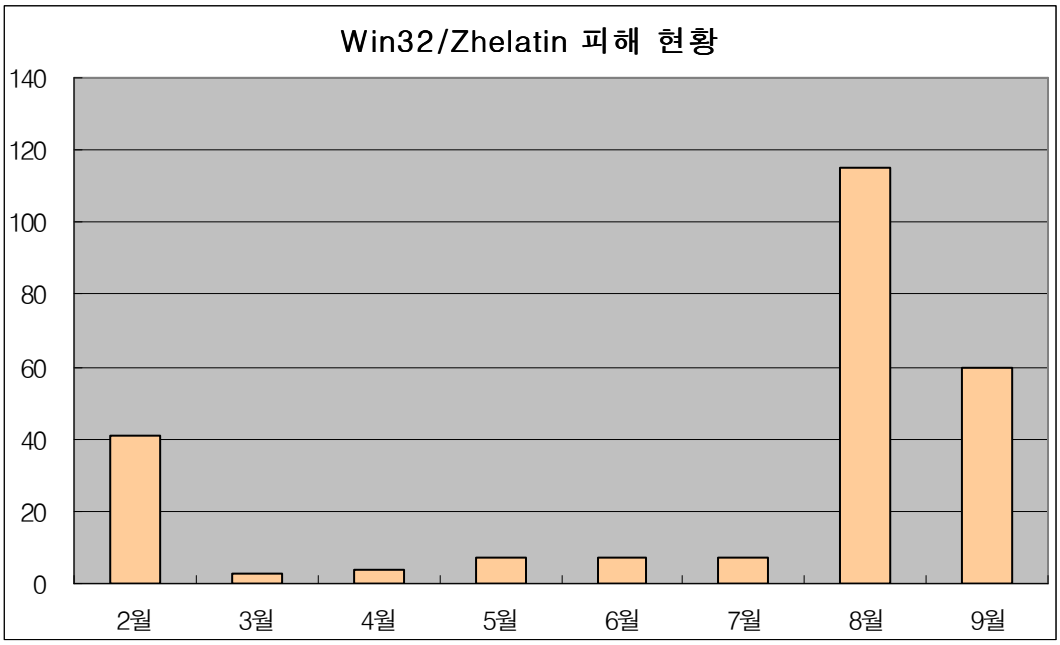
데이터는 메모리상에 남게 된다. 메모리상에 존재하는 데이터를 조작하여, 공격자 의도대로 자신의 계좌로 수정하거나 금액을 바꿀 수 있으며, 기타 보안 정보를 획득할 수 있다. 이를 처하기 위한 방법으로는 인터넷 뱅킹을 사용하였을 경우 꼭 다시 한번 이체결과등을 확인하는 습관을 기르며, 윈도우 보안 업데이트 및 백신을 설치하여 악의적으로 설치된 프로그램을 치료하고 자주 업데이트하는 것이 좋다.

(4) 2007년 3/4분기 일본 악성 코드 동향

2007년 3분기 일본의 악성코드 동향한 주요 이슈는 8월 한달 동안 급격하게 증가한 젤라틴 웜(Win32/Zhelatin.worm)의 메일 트래픽과 소로우 웜(VBS/Solow)의 감염으로 인한 피해가 점점 늘어나고 있는 점, 바이럿(Win32/Virut) 바이러스의 지속적인 피해가 발생하고 있는 점을 들 수 있다.

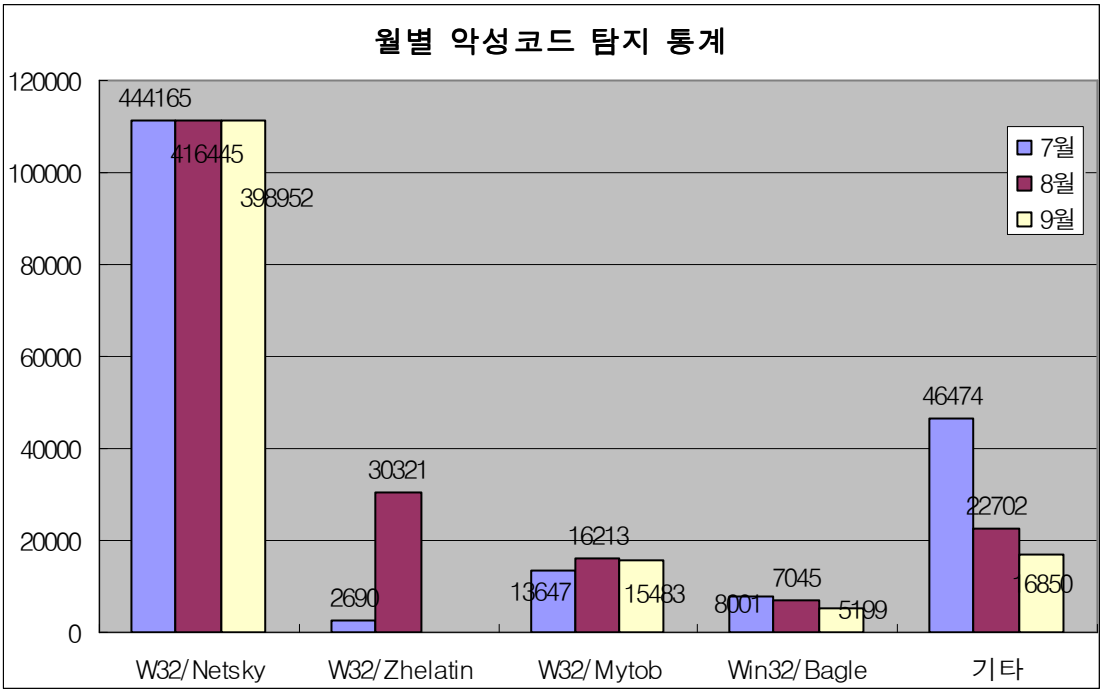
젤라틴 웜의 증가

IPA의 자료에 의하면 일본에서 젤라틴 웜은 2007년 2월 최초로 발견된 것으로 보고되고 있다. 젤라틴 웜은 이메일을 이용하여 전파되는 악성코드로써 감염이 된 시스템에 드로퍼를 설치하고 설치된 드로퍼가 다시 루트킷을 설치하는 형태로 감염을 유발하며 최초 발견된 이후 현재까지도 여러 형태의 변형이 지속적으로 발견되고 있다.



[그림 3-9] 젤라틴 웜 감염 피해 현황 <자료출처: 일본 IPA>

위의 [그림 3-9]는 IPA에서 집계한 젤라틴 웜의 월별 감염 피해 수치를 나타낸 것이다. 2007년 2월 최초 발생시에는 많은 피해가 보고된 후 3월 이후에는 피해량이 그리 많지 않은 상태였으나 8월이 되면서 급격히 증가한 것을 볼 수 있다.

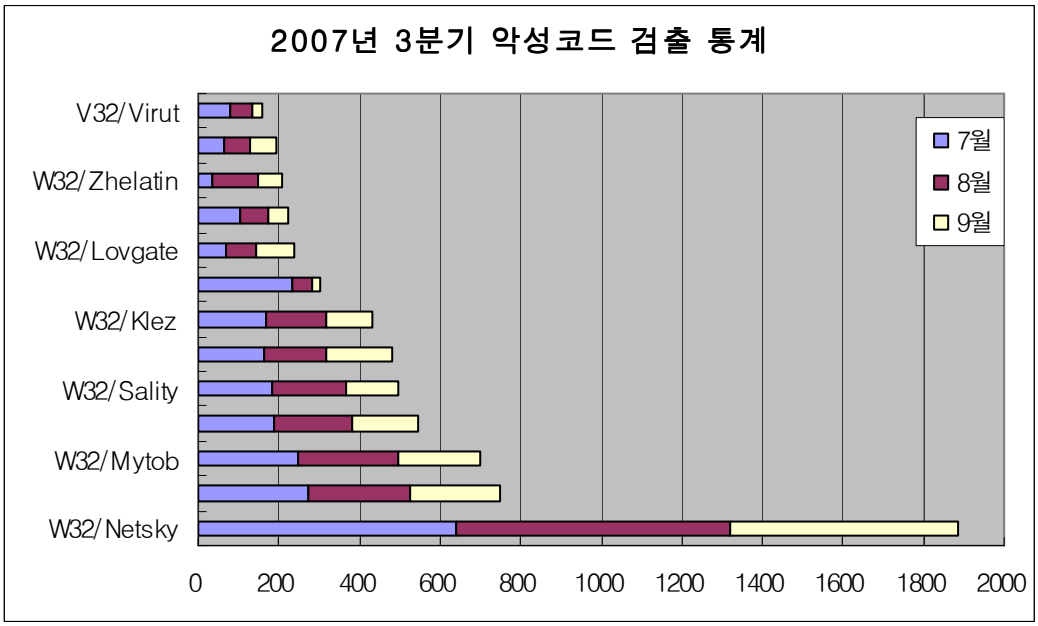


[그림 3-10] 월별 악성코드 탐지 통계 <자료출처: 일본 IPA>

[그림 3-10]은 인터넷 접점에서 관측된 악성코드들의 탐지 현황을 그래프로 나타낸 것이다. 8월 한 달 동안 젤라틴 웜의 탐지 횟수가 급격하게 증가하였으나 9월 들어 거의 탐지가 되지 않고 있는 것을 볼 수 있다. [그림 3-9]와 [그림 3-10]의 데이터로 미루어 보았을 때 당분간 젤라틴 웜으로 인한 피해가 늘어날 가능성은 낮아 보이나 많은 불특정 다수에게 쉽게 노출되고 전파력이 강한 메스메일러의 특성으로 미루어 볼 때 동일한 현상이 발생할 수 있는 가능성은 항상 존재하므로 주의가 필요하다.

악성코드 피해 동향

2007년 3분기 일본에서 가장 많은 피해가 발생한 악성코드는 이전과 동일하게 넷스카이 웜(Win32/Netsky.worm)이다. 베이글 웜(Win32/Bagle.worm)과 마이탑 웜(Win32/Mytob.worm) 또한 여전히 많은 피해를 주고 있다.

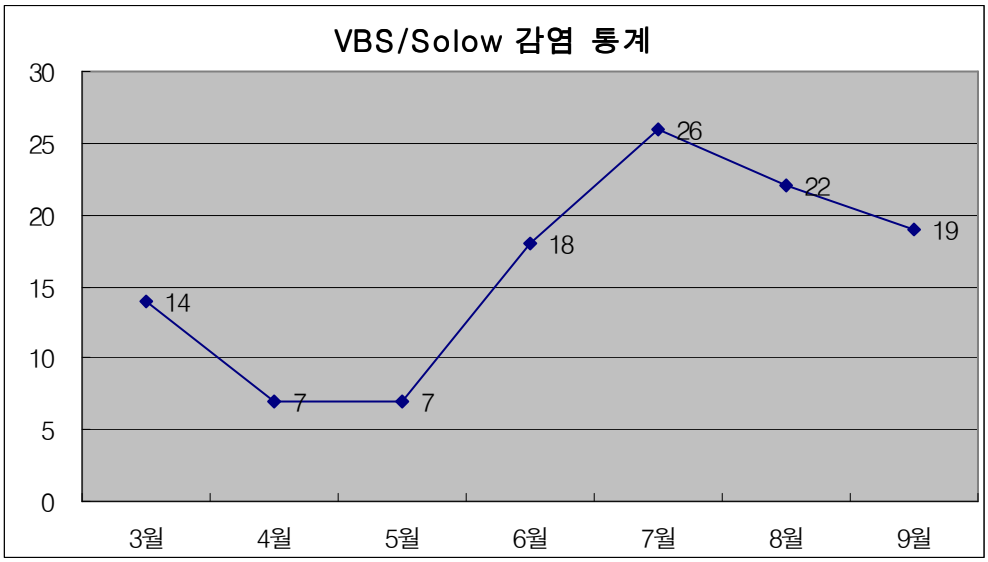


[그림 3-11] 2007년 3분기 악성코드 검출 통계 <자료출처: 일본 IPA>

[그림 3-11]은 월 별 악성코드 피해 통계를 그래프로 나타낸 것으로 넷스카이 웜 등 이메일에 의한 피해가 여전히 많은 것을 알 수 있다. 표에서 주목할 점은 스트레이션 웜(Win32/Stration.worm)의 감염 피해가 7월 이후로 급격하게 감소하고 있는 것이다. 피해가 감소하는 원인을 자세히 알 수는 없으나, 최근 변형이 발견되지 않고 있는 것으로 보아 이와 같은 상태가 앞으로도 지속될 것으로 보인다.

바이럿 바이러스의 피해가 전월에 이어 3분기에도 지속적으로 발생한 것 또한 주목할 만한 점이다. 주로 웹사이트 등에서 악성코드를 유포되고 인터넷 익스플로러의 취약점을 이용하여 감염되는 바이럿은 실행파일을 감염시키고 트로이목마를 설치하는 악성코드이다. 웹사이트를 방문하는 것만으로도 감염이 되고 배포지가 방문자가 많은 유명 웹사이트인 경우도 있으므로 사용자가 감염 여부를 쉽게 인지하기 어렵고, 특히 파일을 감염시키는 형태의 악성코드이므로 사용자에 의한 치료가 어렵기 때문에 감염 예방을 위해서는 백신 프로그램을 사용하는 것이 바람직하다.

위의 통계에는 나타나지 않았지만 소로우 웜(VBS/Solow)의 피해가 계속 발생하고 있는 것에 주목할만 하다. 최근 USB 드라이브를 감염시키고 루트 드라이브에 inf 파일을 생성하는 형태의 악성코드들이 많이 발견되고 있고 소로우 웜 또한 이러한 동작을 하는 악성코드이다. 아래의 [그림 3-12]는 소로우 웜의 감염 피해에 대한 통계이다. 2007년 3월 최초로 발견된 이후 지속적으로 감염 피해가 발생하고 있는 것을 알 수 있다.



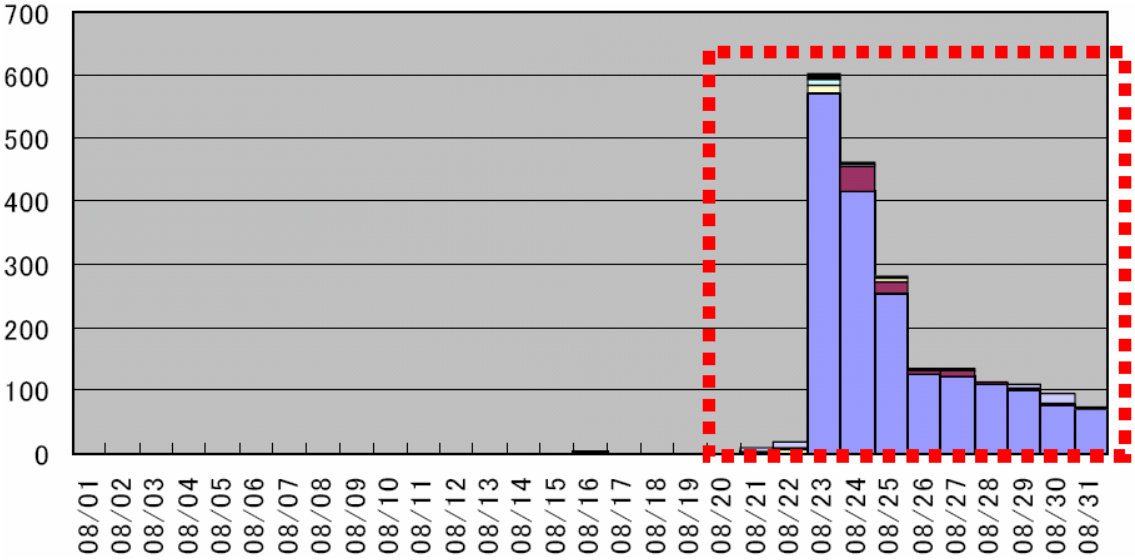
[그림 3-12] 소로우 웜 감염 통계

최근에는 소로우 웜 이외에도 여러 형태의 다운로더나 드롭퍼들에 의해 USB 메모리를 감염시키는 피해를 당하는 경우가 발생하고 있는데 9월에 들어 일본에서 발견되기 시작한 오토런(Win32/Autorun)과 같은 악성코드가 대표적인 예이다. USB 드라이브는 개인의 중요한 정보를 많이 저장하고 있는 매체이다. 따라서 신뢰할 수 없는 PC에서 함부로 사용하는 것은 중요한 정보의 유출이나 훼손이 발생할 수 있는 매우 위험한 행동이므로 사용자의 주의가 필요하다.

빈번하게 발생하는 제로데이 공격(Zero Day Attack)

제로데이 공격은 보안 취약점이 알려진 후 이에 대한 패치 등의 보완책이 아직 제공되지 않은 짧은 기간에 해당 취약점을 이용한 사이버 공격을 수행하는 것을 말한다. 공격의 형태는 여러 가지로 행해질 수 있는데 대표적인 예가 얼마 전에 발생한 MS의 Ani 취약점을 이용한 악성코드 유포이다. 이러한 추세는 일본에서도 크게 다르지 않아 취약점이 존재하는 특정 프로그램을 대상으로 하는 제로데이 공격이 빈번하게 발생하고 있다.

아래의 [그림 3-12]는 TCP 5168 포트에 대한 모니터링 결과를 보여주는 그래프이다 8월 23일부터 해당 포트를 이용한 트래픽이 급격하게 늘어나는 것을 알 수 있다.



[그림 3-12] TCP 5168 포트의 급격한 트래픽 증가

해당 포트는 트렌드마이크로사에서 제공하는 서버용 소프트웨어에서 사용하는 포트로써 8월 23일 해당 프로그램과 관련한 취약점이 발표된 상태였다.(JP Cert의 보안 권고문: http://www.jpcert.or.jp/at/2007/at070019.txt) 취약점이 공개된 당일 해당 포트를 이용한 트래픽이 비정상적으로 급증했다는 것은 해당 소프트웨어가 설치된 시스템을 찾기 위한 스캐닝이 빈번하게 발생했다는 것을 보여준다.

이러한 현상은 이미 과거에도 범용으로 사용되는 소프트웨어에 대한 취약점이 발표될 때면 빈번하게 발생해 왔었다. 현재까지 이러한 공격으로 인해 일본에서 크게 이슈가 될 만한 사건이 발생하지는 않고 있지만 이러한 시도가 증가하는 것은 보안의 측면에서 항상 잠재된 위험요소가 아닐 수 없다.

(5) 2007년 3/4분기 중국 악성코드 동향

중국의 최대 명절 중의 하나인 중추절(仲秋節)로 인한 연휴가 10월 초까지 중국에서 이어졌다. 보통 2주 정도의 연휴를 즐기는 중국인들은 월병(月餠)을 만들어 먹으며 가족들과 즐거운 시간을 보내는 것이 일반적이다. 이러한 모습은 한국에서 송편을 빚어 먹는 한국인들과도 참으로 유사한 풍습이라고 할 수 있다. 이렇듯 음력을 사용하는 비슷한 풍습과 문화가 많은 중국의 2007년 3분기 악성코드 동향을 알아보도록 하자.

► **악성코드 TOP 10**

순위 변화	순위	Rising
-	1	Trojan.PSW.Win32.OnLineGames
↑ 3	2	Hack.SuspiciousAni
New	3	Trojan.Win32.Agent
New	4	Trojan.PSW.Win32.XYOnline
New	5	Adware.Win32.Agent
↑ 1	6	Trojan.DL.JS.Agent
New	7	Trojan.DL.Win32.Agent
New	8	Trojan.PSW.Win32.QQPass
New	9	Trojan.DL.Agent
New	10	Trojan.PSW.Win32.RocOnline

[표 3-1] 2007년 3/4 분기 중국 라이징(Rising) 악성코드 TOP 10

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

이번 2007년 3분기의 라이징(Rising)의 악성코드 TOP 10을 나타낸 [표 3-1]을 본다면 3종의 악성코드를 제외하고는 모두 새롭게 순위에 포함된 악성코드 들이다. 1위에는 지난 2분기에 이어서도 Trojan.PSW.Win32.OnLineGames(V3 진단명 – Win-Trojan/OnlineGameHack)이 차지하고 있다. 이외에도 Trojan.PSW.Win32.XYOnline와 Trojan.PSW.Win32.RocOnline 역시 중국 또는 대만에서 제작된 온라인 게임 사용자 정보를 유출하는 트로이목마들이다. 이외에도 순위에는 포함이 되지 않았지만 Trojan.PSW.Win32.SunOnline과 Trojan.PSW.Win32.WoWar(V3 진단명 – Win-Trojan/WowHack) 등으로 미루어 2분기부터 이어진 온라인 게임 사용자의 정보를 유출하는 형태의 트로이목마는 3분기에도 지속적인 확산을 보이고 있는 것으로 분석된다.

이번 3분기에서의 특이한 점은 올해 들어서 처음으로 애드웨어가 라이징(Rising)의 악성코드 TOP 10에 포함되었다는 것이다. 해당 애드웨어는 5위를 기록한 Adware.Win32.Agent로서 7월 중순에 최초로 순위에 등장하였다. 그리고 8월 한달 동안 주간 악성코드 TOP 10에서 2

위를 차지할 정도로 많은 감염 활동을 보였으나 9월에 접어들면서는 급속한 감소형태를 보였다.

그 외에도 2종의 악성코드가 순위 상승을 기록하였다. Hack.SuspiciousAni(V3 진단명 - Win-Trojan/Exploit-ANI.suspicious)와 Trojan.DL.JS.Agent이 이번 3분기에 3단계와 1단계씩 각각 상승한 악성코드이다. 이 2종의 악성코드의 공통점들은 모두 윈도우 운영체제에서 사용되는 인터넷 익스플로러의 취약점을 이용하는 악성코드로 다른 악성코드를 다운로드 후 실행한다는 공통점을 가지고 있다. 이러한 형태의 악성코드의 순위가 상승한 점으로 미루어 취약한 웹 사이트가 중국 내에서 악성코드 전파에 큰 영향을 미치고 있는 것으로 볼 수 있다.

순위 변화	순위	JiangMin
-	1	Checker/Autorun
-	2	Exploit.ANIfile.b
New	3	Trojan/PSW.GamePass.xyh
New	4	TrojanDropper.Agent.ctm
New	5	TrojanDropper.Agent.ctl
New	6	Trojan/Agent.psm
New	7	Worm/Viking.auw
New	8	Trojan/Agent.rsx
New	9	TrojanDownloader.Agent.hmi
New	10	Trojan/PSW.OnLineGames.flv

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

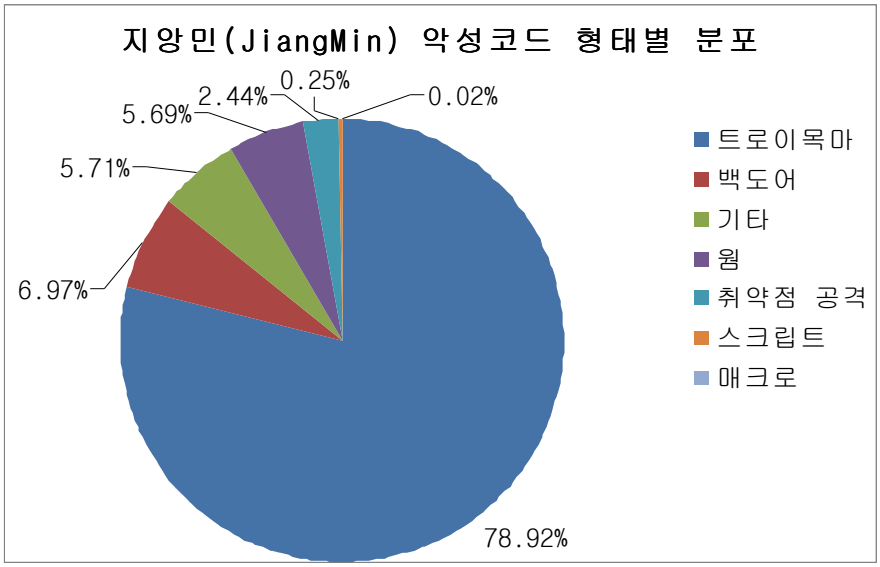
'-' - 순위변동 없음, 'New' - 순위에 새로 진입, '↑'- 순위 상승, '↓' - 순위 하락

지앙민(JiangMin)의 악성코드 TOP 10을 나타낸 [표 3-2]를 보면 지난 2분기와 동일하게 Checker/Autorun(V3 진단명 - TextImage/Autorun)와 Exploit.ANIfile.b(V3 진단명 - Win-Trojan/Exploit-ANI.suspicious)가 순위 변동 없이 1위와 2위를 지키고 있다. 그 외에는 모두 이번 3분기에 새로 순위에 기록된 악성코드들로 구성되어 있다. 그러나 2분기와 비교하여 악성코드의 명칭만 변경되었을 뿐 동일한 변형의 악성코드들로 구성되어 있는 것을 알 수가 있다. 이러한 큰 흐름은 라이징의 악성코드 TOP 10과 비교하여 커다란 차이점이 없는 것으로 보여진다.

라이징의 TOP 10과 지앙민의 TOP 10을 간추려 본다면 현재 중국 내에서는 취약한 웹 사이트와 USB 외장형 저장 장치가 악성코드 전파의 가장 큰 수단으로 이용되고 있는 것으로 분

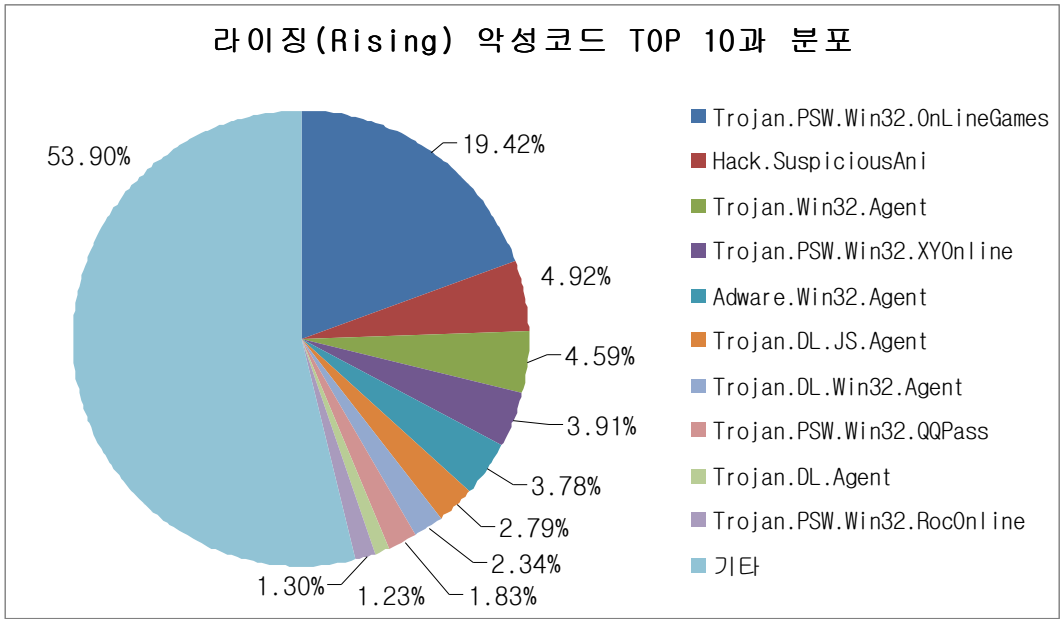
석이 가능하다. 그리고 이러한 악성코드들의 감염 형태는 결국 두 업체의 순위에 빠지지 않고 등장하고 있는 온라인 게임 사용자 트로이목마들을 사용자의 시스템에 감염시키기 위한 수단인 것으로 분석된다.

► **악성코드 TOP 10 분포**



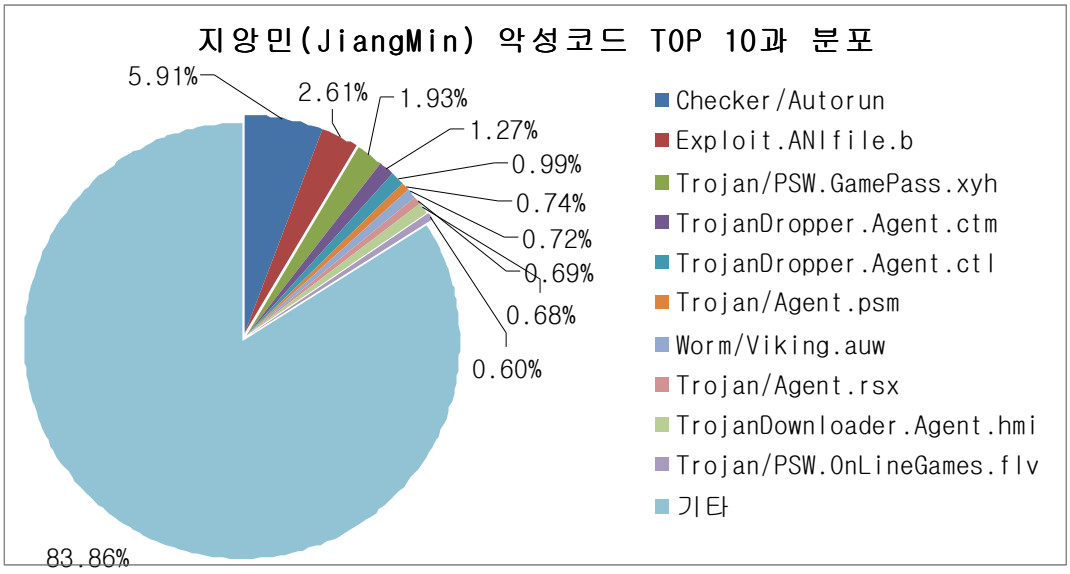
[그림 3-13] 2007년 3/4 분기 중국 지앙민(JiangMin) 악성코드 형태별 분포

3분기 지앙민의 악성코드 형태별 분포를 살펴보면 지날 달에 이어 트로이목마가 절대 다수를 차지하고 있는 것을 알 수 있다. 백도어 및 웜은 2분기 대비 소폭 상승하였다. 그러나 매크로와 스크립트 형태의 악성코드는 소폭 감소 형태를 보였으나 분포도 상에서 분포율이 워낙 미비하여 전체에 영향을 줄 정도는 아닌 것으로 보여진다.



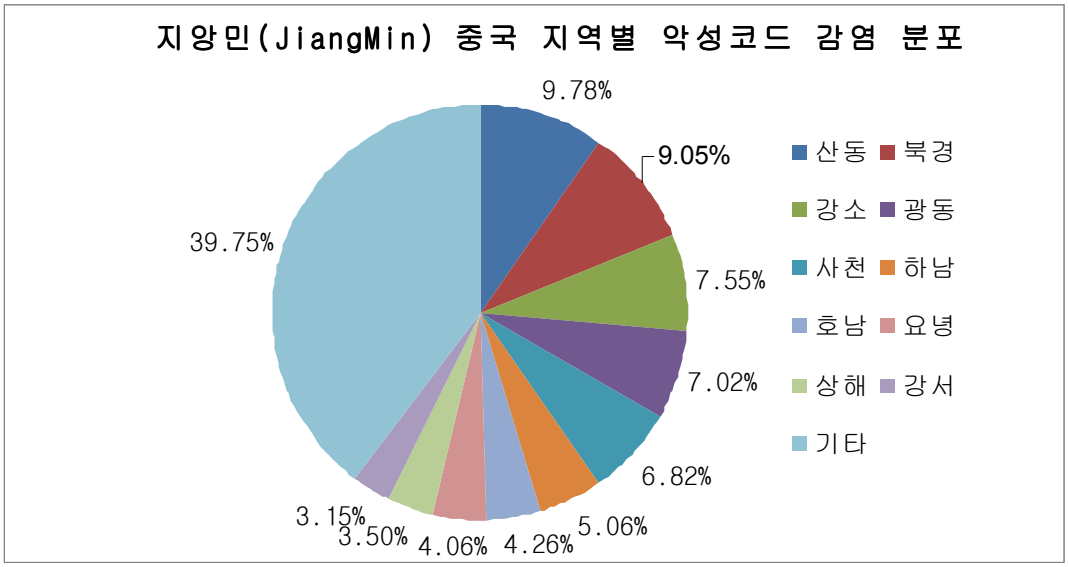
[그림 3-14] 2007년 3/4 분기 중국 라이징(Rising) 악성코드 TOP 10과 분포

3분기 라이징 악성코드 TOP 10의 분포를 나타낸 것이 [그림 3-14]와 같다. TOP 10에 포함된 악성코드는 전체의 46% 가량을 차지하고 있으며 순위에 포함되지 못한 악성코드가 전체의 53% 가량을 점유하고 있는 것으로 나타났다. 그러나 사용자 정보 탈취 형태의 악성코드를 두고 보았을 때 전체 악성코드 분포에서 지난 2분기의 경우 21% 가량을 차지하였으나 이번 3분기에서는 2배 가량 증가한 42% 가량 차지하고 있다. 이러한 사용자 정보 탈취 악성코드의 증가 추세는 현재 중국 악성코드 동향에서 가장 큰 문제점으로 볼 수 있으며 이에 대한 효과적인 대응책을 마련하는 것인 것이 시급한 것으로 분석된다.



[그림 3-15] 2007년 3/4 분기 중국 지앙민(JiangMin) 악성코드 TOP 10과 분포

지앙민의 경우에는 특히나 TOP 10에 포함되지 못한 악성코드들의 분포인 기타부분은 [그림 3-15]와 같이 전체의 83% 가량으로 상당히 크게 분포하고 있다. 이는 TOP 10 악성코드의 분포가 미약할 뿐만 아니라 실제 중국 네트워크 상에서는 상당히 다양한 악성코드들이 존재하고 있다는 것을 보여주고 있다 할 수 있다. 특히 Checker/Autorun의 경우에는 2분기 2.89%에서 이번 3분기에 5.91%로 증가하였다는 점은 중국 내에서 Auntorun.inf를 통한 자동 실행 기법을 사용하고 있는 다양한 형태의 악성코드들이 증가하고 있다는 것으로 해석할 수가 있다.



[그림 3-16] 2007년 3/4 분기 지앙민(JiangMin) 중국 지역별 악성코드 감염 분포

[그림 3-16]는 지앙민에서 집계한 지역별 악성코드 감염 분포이다. 이번 3분기에서는 산동지방이 9.78%를 차지하고 있으며 그 뒤를 이어 중국의 수도인 북경이 9.05%로 차지하고 있다. 이 분포 역시 중국 내륙 지방보다는 중국 동부 해안 지역의 인구 밀집도시에서 컴퓨터 사용률과 함께 악성코드 감염 사고가 많은 것으로 볼 수 있다.

► 중국어로 전파되는 MSN 메신저 웜

이번 3분기에는 한국 동향에서와 같이 중국 내에서도 유달리 MSN 메신저로 전파되는 웜의 활동이 많았었다. 중국의 경우에는 중국 업체에서 개발한 QQ 메신저라는 프로그램을 많이 사용함으로 MSN 메신저의 사용 비율은 그리 높지 않다고 볼 수 있다. 그리고 MSN 메신저로 전파되는 웜의 경우에는 MSN 사용자를 현혹하기 위한 수단으로 영어로 된 특정 문구를 전송하는 것이 일반적이라 중국 내에서는 많은 감염 피해를 유발하지는 않았다. 그러나 이번 8월에는 중국어 병음으로 된 문구를 전송하는 MSN 메신저 웜이 중국 내에서 발견되는 특이

사항이 있었다.

```
ZHE SHI WO DE LUOZHAO :o QING BU YAO FA GEI BIEREN !!.
YI ZHANG WO GEN WO PENGYOU ZUI HAO DE ZHAOPIAN :s !!.
JIESHOU WO DE ZHAO PIAN :> !!.
KAN WO DE ZHAOPIAN :D.
NI HE WO !!! ....
QING KAN :D.
kAN BA LI XI ER DUN JIN JIANYU HOU SHI DUO ME QIAOCUI :<.
```

[그림 3-17] MSN 웜에서 사용되는 중국어 문구]

[그림 3-17]은 중국 내에서 발견된 MSN 메신저 웜이 전송에 사용되는 중국어 병음 문구이다. 중국어 병음이란 한자인 중국어를 영어로 된 발음기호 형태로 표기하는 것을 말한다. 중국어 병음 문구 역시 사용자를 현혹하기 위한 의미를 포함하고 있지만 중국인 대부분이 영어에 친숙하지 않다는 것을 해당 악성코드 제작자가 의식한 것으로 보여진다.

► 악성코드 제작자와 보안 업체

지난 4월경 중국 내에서는 델보이(Win32/Dellboy) 바이러스와 다수의 악성코드를 제작한 혐의로 리 준(Li Jun)이 체포되는 사건이 있었다. 리 준은 해당 악성코드 제작혐의로 중국 법원으로부터 4년 형을 선고 받았으나 9월 중순 중국 일민 일보의 한 기사로 인해 보안 업계에서는 악성코드 제작자와 보안 업계와의 관계에 대해 심각한 우려를 나타내고 있다. 해당 기사에 따르면 리 준의 변호사는 그의 감형을 위해서 그의 높은 프로그래밍 실력으로 인해 중국 내 10여 곳이 넘는 많은 보안 업체들이 그를 직원으로 채용하기 위해 높은 연봉을 제안을 하였다고 이야기하였다.

안티 바이러스(Anti-Virus) 업계에서는 일반적으로 악성코드 제작자와 악성코드 수집가들을 채용하지 않는 관행이 있다. 이는 안티 바이러스 업계의 순수성과 신뢰성을 나타내기도 하지만 일반적으로 악성코드 제작을 할 수 있다고 하여 프로그래밍 실력이 높다고 평가할 수 없기 때문이다. 그리고 무엇보다도 고객의 시스템과 정보를 보호하는 보안 업체에 있어서 가장 중요하게 생각되는 점은 바로 도덕성이기 때문이다.

► 2008년 북경 올림픽을 이용한 악성코드

9월 말 중추절 연휴 기간인 중국에서는 특이한 제목의 이메일이 다수의 사람들에게 수신되었다. 해당 메일은 “2008년 북경 올림픽 참석자 명단”이라는 제목을 가지고 있었으며 본문에는 친절하게 연락처와 함께 첨부한 등록표라는 워드 파일을 작성해서 보내면 2008년 북경 올림픽을 참관할 수 있게 해준다라는 내용이 포함되어 있다. 그러나 해당 워드 파일은 마이크로소프트 오피스 제품의 취약점을 이용하여 악의적인 원격제어 형태의 트로이목마를 설치

하는 워드 파일이었다.

일반적으로 이메일로 전파되는 악성코드들의 경우에는 사회적인 기사거리 등을 이용하는 사회 공학 기법을 많이 사용하고 있다. 이번 취약한 워드 파일이 첨부된 2008년 북경 올림픽 관련 메일 역시 중국인들이 많은 관심을 가지고 있는 2008년 북경 올림픽을 이용하였다는 점에서 사회 공학 기법의 전형을 보여준 사례라고 할 수 있다.

(6) 2007년 3/4분기 세계 악성코드 동향

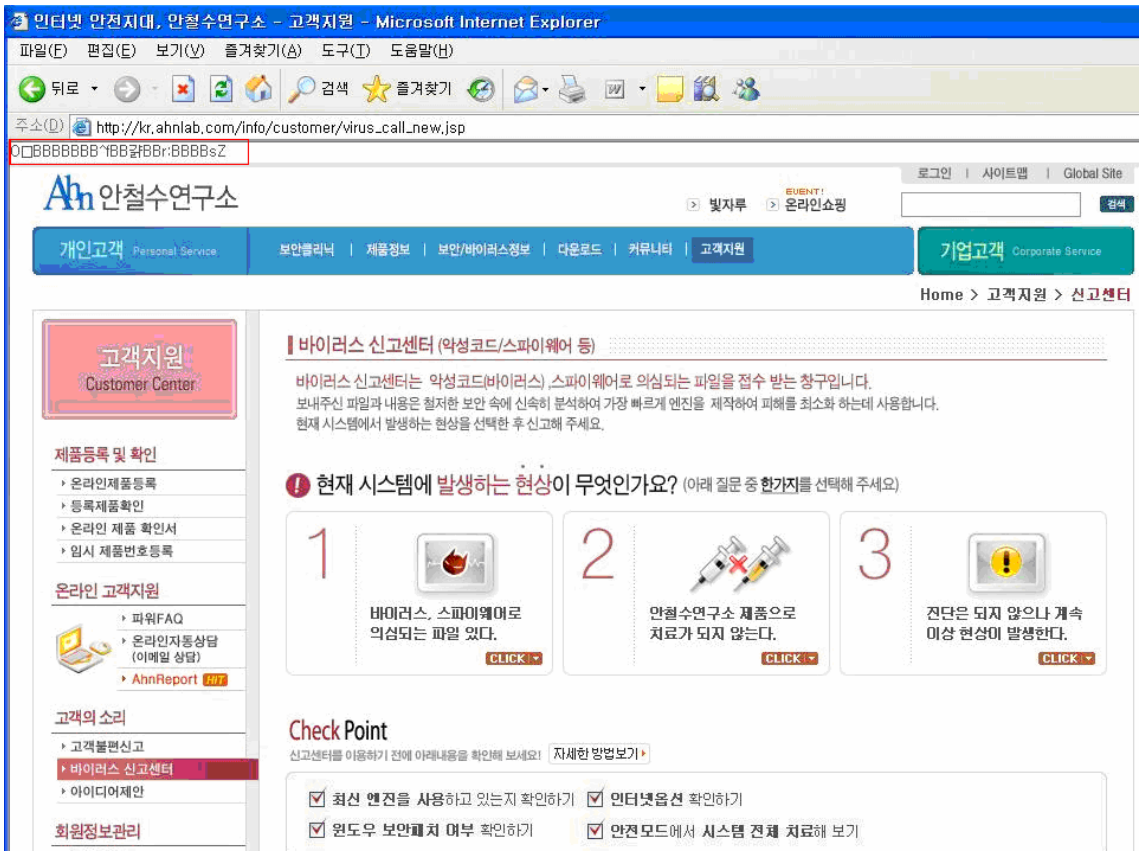
2007년 3/4 분기의 통계를 보면 과거부터 유행한 악성코드의 건재와 큰 변화 없는 순위이다.

독일의 아비라(Avira) 통계에 따르면 3/4분기 순위권의 악성코드는 여전히 넷스카이 웜, 마이톱 웜 등이었다. 영국 소포스의 통계도 넷스카이, 마이톱, 자피, 마이둠 등이 순위에 있다. 러시아 카스퍼스키 연구소의 순위도 크게 다르지 않았다. 이는 메일로 전파되는 악성코드가 상대적으로 집계가 편해 높은 순위를 차지하기 때문이다. 하지만, 캐스퍼스키 연구소의 온라인 스캐너(Online Scanner) 검사 결과를 보면 1위를 차지하고 있는 악성코드가 Trojan.Win32.Dialer.qn으로 1.65%뿐에 불과하며 순위권을 모두 합해도 나머지 악성코드가 80% 이상을 차지하고 있다. 이는 바이러스, 웜 보다 트로이목마의 수가 압도적으로 많으며 이들 트로이목마가 그 지역에서 사용되는 취약점을 공격하는 해킹된 웹사이트, 해당 지역 언어로 된 메일 등의 경로로 감염되기 때문에 지역화 영향이 큰 것으로 보인다. 또 하루에도 수천 개의 악성코드가 쏟아지지만 대부분 며칠 활동하고 사라지는 영향도 큰 것으로 보인다.

이외 3/4 분기 주요 사건은 다음과 같다.

ARP 스푸핑을 이용한 공격이 보고되었는데 국내에서는 2007년 초부터 국내에서 간간히 보고되었다가 여름에 집중되었다. 맥아피는 블로그에서는 2007년 10월 ARP 스푸핑에 대한 글을 올렸다. [1] 맥아피에서 늦게 발견했을 수 있지만 한국에서 발생하는 ARP 스푸핑은 대부분 중국에서 시작되었고 맥아피에서 보고된 내용도 중국에서 제작되었다면 상대적으로 가까운 대한민국에서 실험해보고 공격이 세계로 뻗어나갔을 가능성도 존재한다.

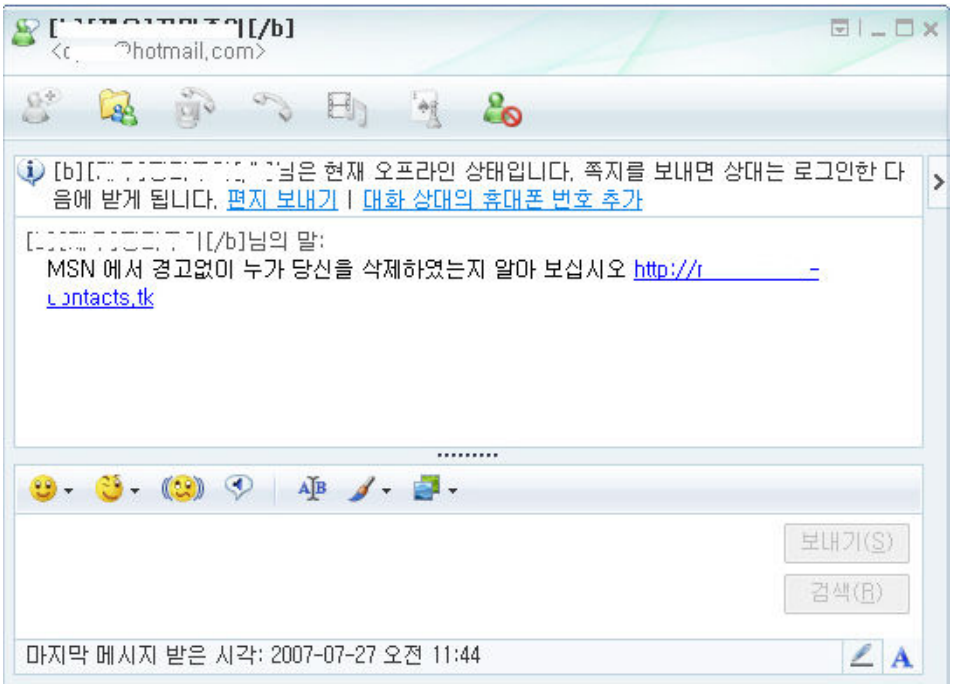
[1] http://www.avertlabs.com/research/blog/index.php/2007/10/04/arp-spoofing-is-your-web-hosting-service-protected/



[그림 3-18] ARP 스푸핑 공격을 받았을 때 출력될 수 있는 BBBBB 문자열

미국에서 여교사인 줄리에 아메로(Julie Amero)가 수업 시간에 아이들에게 포르노 사이트를 보여주는걸 방치했다고 2007년 3월 2일 유죄를 선고 받았다. 무려 40년 형을 선고 받았는데 포르노가 금지된 한국이지만 사실상 포르노가 방치되는 한국과 달리 미국이나 유럽은 유아 포르노 및 아이에게 성인물을 노출되는 건 큰 죄인 것으로 보인다. 하지만, 여교사는 애드웨어(스파이웨어)가 설치되어 발생한 일이라고 주장했고 실제 시스템에서 성인 광고를 띄우는 애드웨어가 발견되었다고 한다. 결국 이 사건은 여름에 무죄로 최종 판결 났다. 성인 광고를 노출하는 애드웨어가 어떤 영향을 끼칠 수 있는지 보여주는 사건이라고 할 수 있다.

2007년 7월 MSN 메신저를 통해 'MSN에서 경고없이 누가 당신을 삭제하였는지 알아보십시오'라는 내용과 함께 특정 주소를 클릭하는 내용이 보내졌다. 이미 5월에도 유사한 사건이 있었지만 영어가 아닌 다른 언어로도 보내진 점이 차이점이다.



[그림 3-19] MSN 메신저를 통한 특정 사이트 유도

해당 사이트로 접속해보면 구글 애드센스 광고가 있어 클릭 수익을 노린 것으로 보인다. 보다 높은 사이트 접속을 위해 여러 언어로 보낸 것으로 추정된다.

스팸 메일의 형태로 다양해 지는데 초기 스팸 메일은 단순한 텍스트였으나 이후 HTML 형식, 이미지에 이어 2007년에는 PDF 파일이나 DOC, XLS, RTF 같은 오피스 문서 포함된 스팸 메일이 유행한다.

IV. ASEC 컬럼

(1) Virut 바이러스 상세 분석

해마다 접수되는 악성코드의 통계를 보면 대부분이 인터넷 웜 또는 트로이목마가 대부분을 차지하며, 파일에 기생하는 바이러스는 그 수가 적어지는 것이 추세이다. 그도 그럴 것이 최근의 악성코드 특징은 개인의 능력과시가 아닌 돈과 연관되는 악성코드 작성이 대부분이기 때문이다. 그렇다면 Virut 바이러스가 인터넷 웜과 트로이목마를 제치고 국내뿐만 아니라 해외를 통하는 어떠한 특성과 방법들을 사용하여 많은 피해자를 만들고 있는지 자세히 살펴보도록 하자.

► Virut 바이러스의 발전

2006년 초 처음 등장한 Virut 바이러스는 당시까지의 후위형 파일바이러스와 비교하여 시스템의 공통 라이브러리 API를 후킹하여 다른 PE 파일을 감염시키는 것을 제외하고는 크게 다른 특징이 없었다. 이 후에 등장한 변형에서는 바이러스 본체를 암호화시키고 복호화 루틴을 매 감염 때마다 변경하는 다형성 알고리즘을 사용하였으나, 감염루틴의 버그로 인하여 크게 문제가 되지는 않은 것으로 보인다.

근래 발견된 바이러스 변형은 4가지의 다양한 형태의 감염방식과 중복감염문제, IRC 서버에 접속하여 DDoS 공격을 하는 등의 종합적인 악성코드 특성을 지니게 되었다.

► 바이러스의 전파

Virut 바이러스 자체는 시스템의 실행파일 만을 감염대상으로 하기 때문에 네트워크를 통한 감염은 이루어지지 않는다. 그러나 최근의 Virut 바이러스는 국내에만 수 십만 대의 시스템을 감염시킨 것으로 보이며, 해외의 감염보고에서도 높은 수치를 나타내고 있다. 많은 시스템들은 타 시스템에 의해서 감염이 되었다기 보다는 해킹된 웹사이트에 삽입된 Exploit Script 또는 Script에 추가된 IFrame 등의 원인에 의해서 감염된 파일을 특정 서버서부터 다운로드 되는 것으로 판단된다.

글을 작성중인 현재까지도 새로운 바이러스가 특정 사이트로부터 배포되고 있는 것으로 확인되었기에 사용자들은 항상 최신의 윈도우 취약점 업데이트와 바이러스 엔진 업데이트를 하여야 바이러스로부터 안전할 수 있겠다.

► Virut.C & D의 특성

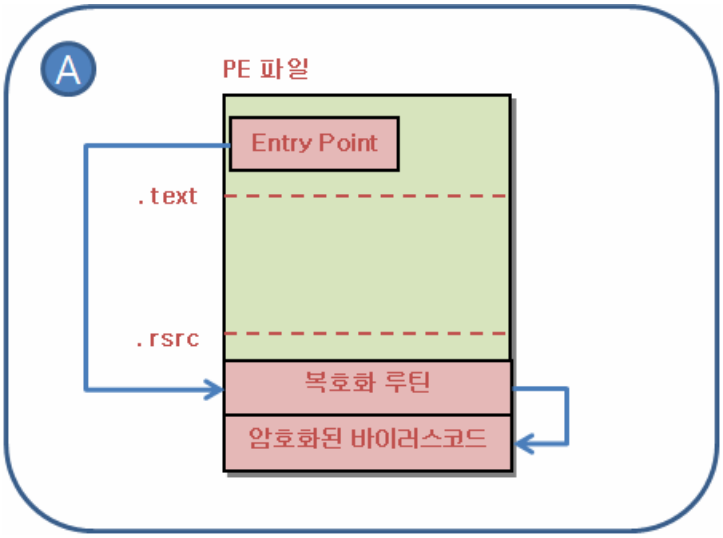
Win32/Virut.C, Win32/Virut.D로 명명된 근래의 바이러스의 특징들을 먼저 살펴보면 다음과 같은 것들을 찾아볼 수 있다.

첫째, 4가지의 다양한 감염방식 – 다형성, EPO(Entry-Point Obscuring), 암호화
둘째, PE 파일 감염 – 특정 확장자(.EXE, .SCR)
셋째, 실행된 모든 프로세스의 공통라이브러리(NTDLL.DLL)의 API 후킹을 이용한 파일감염

- ✓ ZwCreateFile
- ✓ ZwOpenFile
- ✓ ZwCreateProcess
- ✓ ZwCreateProcessEx

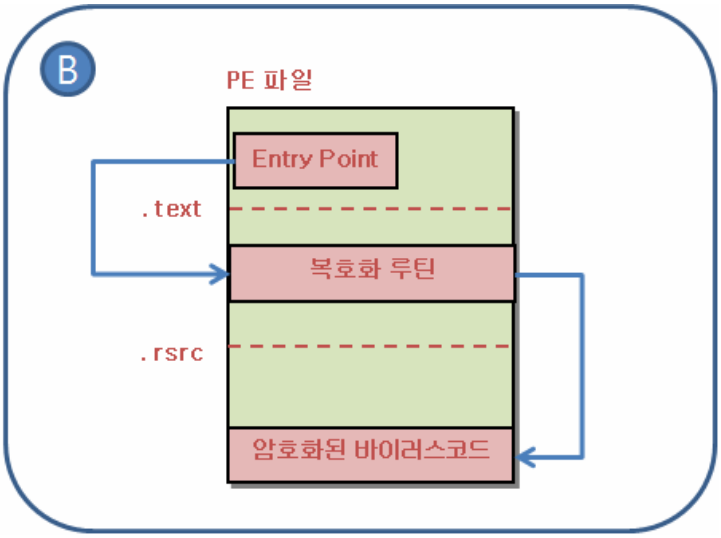
넷째, 시스템 프로세스인 Winlogon.exe에 RemoteThread 생성
다섯째, 외부연결 및 파일 다운로드
여섯째, 특정 IRC 서버접속 및 명령대기

► 감염방식



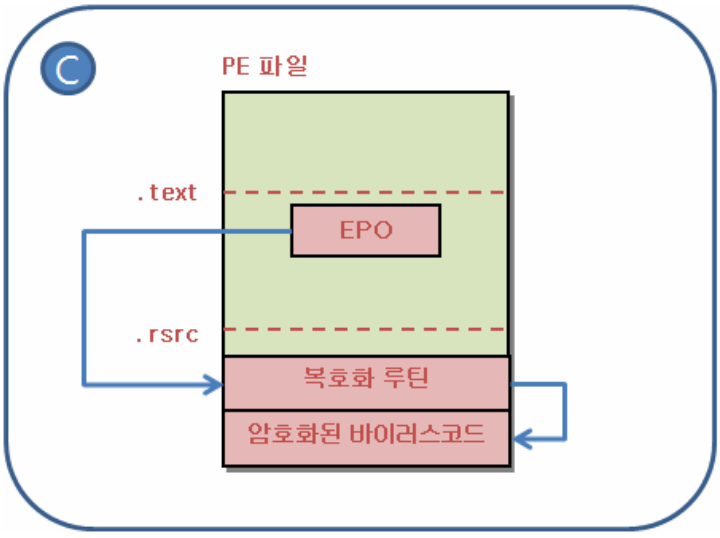
[그림 4-1] Virut A형의 감염 방식

위 그림과 같이 A 형인 감염방식은 일반적인 후위형 바이러스와 크게 다르지 않다. PE 파일의 시작점인 EntryPoint를 파일 후미에 추가된 바이러스 복호화 루틴의 시작지점으로 변경하여 바이러스가 먼저 동작하도록 만든다.



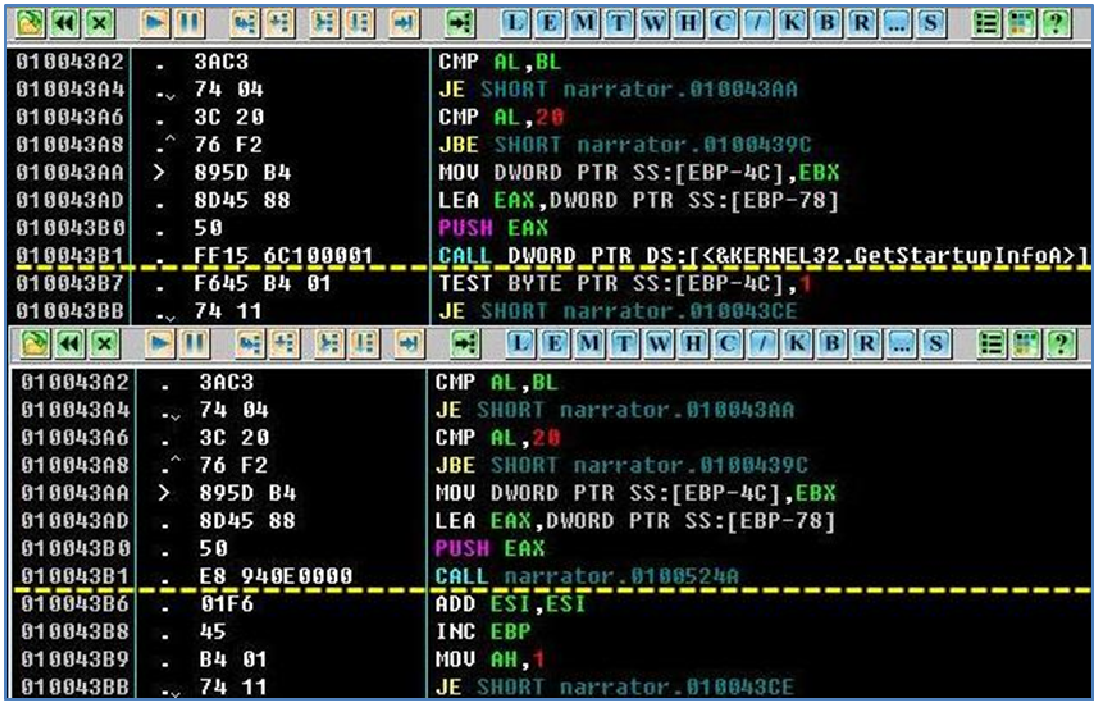
[그림 4-2] Virut B형의 감염 방식

B 형은 PE 파일의 시작점인 EntryPoint를 변경하지 않고 바이러스 복호화 루틴을 파일의 시작위치 특정코드 위에 덮어씌워 버렸다. 물론 본래의 코드는 파일후미의 암호화된 바이러스코드 뒷부분에 암호화하여 백업한다.



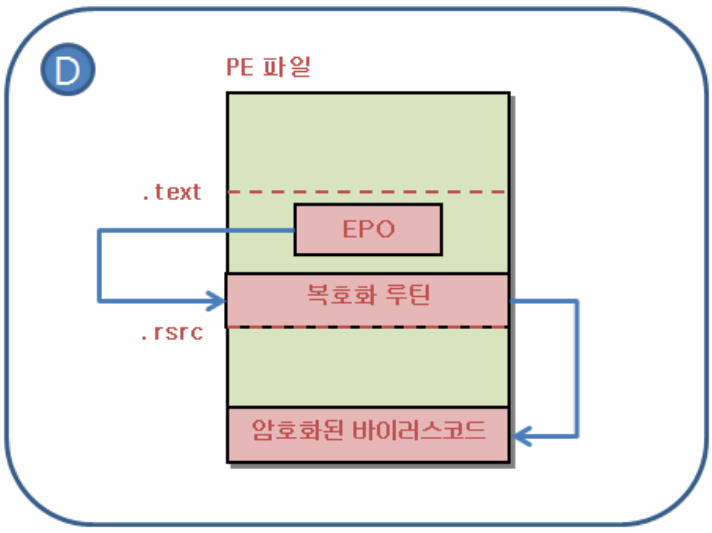
[그림 4-3] Virut C형의 감염 방식

C 형식은 EPO(Entry-Point Obscuring) 방식을 취하는데, 이는 정상적인 특정 CALL 함수호출(5 바이트)에 대해서 파일 후미에 추가된 바이러스 복호화 루틴의 시작점으로 함수호출 옵셋(Offset)을 변경하여 바이러스가 동작하도록 하는 방법이다.



[그림 4-4] EPO를 이용한 코드

[그림 4-4]을 보면, 상단의 밑줄코드가 감염 전의 호출이며 하단의 밑줄코드는 감염된 이후의 호출을 보여준다.



[그림 4-5] Virut D형의 감염 방식

D 형식은 이전의 C 형식과 같다. 다만 바이러스 복호화 루틴이 코드섹션 영역의 마지막 부분에 덧붙여 있다는 것이 다르다. 코드섹션 영역에 복호화 루틴이 추가되므로 인하여 코드섹션의 VirtualSize는 증가할 수 있다.

► 바이러스 복호화 루틴

Virut의 바이러스 복호화 루틴은 실제 바이러스 코드에 대한 복호화 알고리즘으로 이루어져 있다. 문제는 이 복호화 루틴이 다형성으로 구성되었기 때문에 감염된 파일마다 기계어 코드가 다르다는 점이다. 이러한 다형성 코드를 분석하기 위해서는 다양한 감염된 샘플들에 대해서 동일한 분석방법을 사용하여 공통된 코드나 알고리즘을 찾아내야 한다. 하나의 복호화 루틴을 예로 살펴보면 굵게 표시된 부분의 코드들이 복호화에 중요하게 이용되고 있는 부분임을 알 수 있을 것이다.

```
01006AE0 60              PUSHAD
01006AE1 55              PUSH EBP
01006AE2 8BEC            MOV EBP,ESP
01006AE4 E8 0C000000     CALL 01006AF5

// Exception Handler
01006AE9 F8              CLC                ; 01006B2D, 01006B4D 에서 Exception 발생시 호출
01006AEA F8              CLC
01006AEB E8 B4000000     CALL 01006BA4
01006AF0 E9 5E000000     JMP 01006B53             ; 01006B53 분기

01006AF5 67:64:FF36 0000 PUSH DWORD PTR FS:[0]
01006AFB 892D 546B0001   MOV DWORD PTR DS:[1006B54],EBP
01006B01 67:64:8926 0000 MOV DWORD PTR FS:[0],ESP ;  Exception Handler 등록 0x01006AE9
01006B07 31C0            XOR EAX,EAX
01006B09 68 00000080     PUSH 80000000
01006B0E 50              PUSH EAX
01006B0F 68 00000080     PUSH 80000000
01006B14 68 00000080     PUSH 80000000
01006B19 68 00000080     PUSH 80000000
01006B1E 68 01000000     PUSH 1
01006B23 68 00000080     PUSH 80000000
01006B28 50              PUSH EAX
01006B29 50              PUSH EAX
01006B2A 50              PUSH EAX
01006B2B 50              PUSH EAX
01006B2C 50              PUSH EAX                                        ; FileName => NULL
01006B2D FF15 CC100001   CALL DWORD PTR DS:[<&KERNEL32.LoadLibraryA>]  ; LoadLibraryA
01006B33 31D2            XOR EDX,EDX
01006B35 52              PUSH EDX
01006B36 68 00000080     PUSH 80000000
01006B3B 52              PUSH EDX
01006B3C 52              PUSH EDX
01006B3D 68 00000080     PUSH 80000000
01006B42 68 00020000     PUSH 200
01006B47 68 40000000     PUSH 40
01006B4C 52              PUSH EDX                                        ; FileName => NULL
01006B4D FF15 CC100001   CALL DWORD PTR DS:[<&KERNEL32.LoadLibraryA>]  ; LoadLibraryA
01006B53 BD A0FF0600     MOV EBP,6FFA0
01006B58 8B75 F8         MOV ESI,DWORD PTR SS:[EBP-8]
```

```
01006B5B 67:64:8936 0000    MOV DWORD PTR FS:[0],ESI
01006B61 F8                 CLC
01006B62 89C9               MOV ECX,ECX
01006B64 E8 00000000        CALL 01006B69
01006B69 59                 POP ECX                          ;  0x01006B69
01006B6A 81C1 973E0100      ADD ECX,13E97                    ;  복호화위치

01006B70 51                 PUSH ECX
01006B71 31D2               XOR EDX,EDX
01006B73 81CA D1290000      OR EDX,29D1                      ;  복호화크기
01006B79 87DB               XCHG EBX,EBX
01006B7B 87DB               XCHG EBX,EBX
01006B7D 90                 NOP
01006B7E 90                 NOP
01006B7F BE E8000000        MOV ESI,0E8                      ;  복호화키
01006B84 F5                 CMC
01006B85 F8                 CLC
01006B86 F8                 CLC
01006B87 F9                 STC
01006B88 8A01               MOV AL,BYTE PTR DS:[ECX]
01006B8A 66:31F0            XOR AX,SI                        ;  복호화연산
01006B8D 8601               XCHG BYTE PTR DS:[ECX],AL
01006B8F 83C1 01            ADD ECX,1
01006B92 83EA 01            SUB EDX,1
01006B95 F5                 CMC
01006B96 83FA 00            CMP EDX,0
01006B99 75 ED              JNZ SHORT 01006B88
01006B9B 59                 POP ECX
01006B9C C9                 LEAVE
01006B9D 894C24 18          MOV DWORD PTR SS:[ESP+18],ECX
01006BA1 61                 POPAD
01006BA2 FFE1               JMP ECX                          ;  복호화된 위치로 분기
```

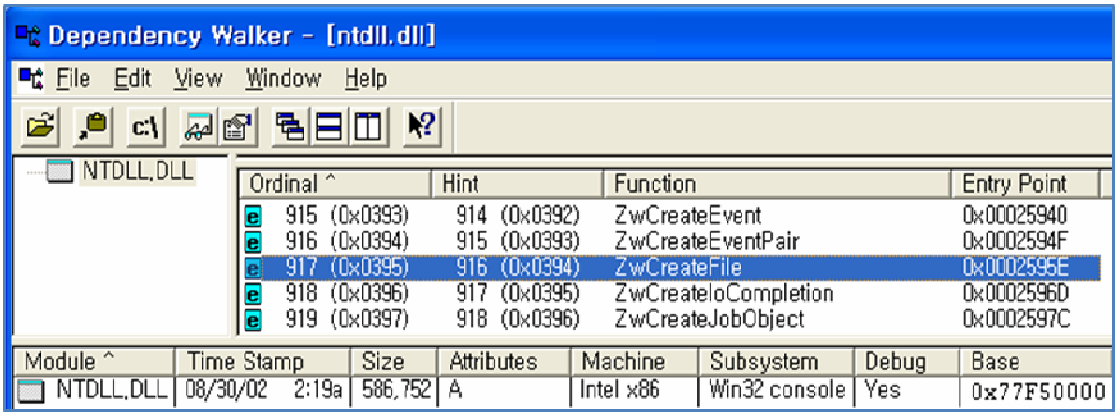
► 바이러스 코드

복호화된 바이러스 코드는 몇 가지의 흥미로운 방식으로 감염루틴을 생성하게 되는데 시간의 흐름에 따른 동작들을 살펴보면 다음처럼 작성될 수 있다.

1. 중복 감염루틴 설치를 피하기 위한 이벤트 객체 생성 (“Vx_4”)
2. 감염루틴을 모든 프로세스에 메모리매핑(MemoryMapping)하기 위한 오브젝트섹션(ObjectSection) 생성 (“\BaseNamedObject\VtSect”)
3. 실행된 모든 프로세스의 공통메모리 영역에 이미 생성한 오브젝트섹션을 매핑
4. 공통라이브러리인 NTDLL.DLL의 특정 Export 함수에 대한 후킹 (ZwCreateFile, ZwOpenFile, ZwCreateProcess, ZwCreateProcessEx)
5. 시스템 프로세스인 Winlogon.exe의 메모리영역에 매핑한 RemoteThread 실행

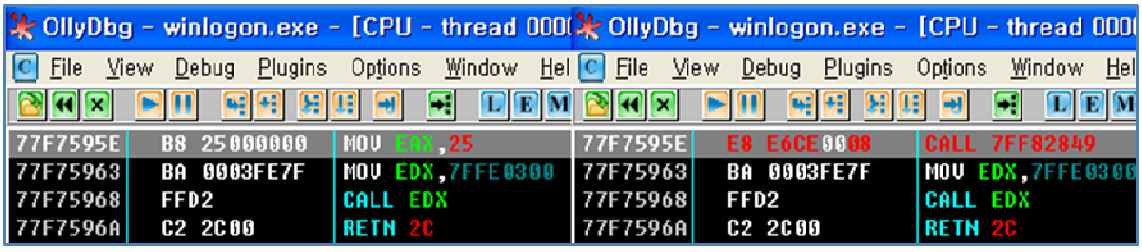
► NTDLL.DLL Export API 후킹

앞서 언급한 바와 같이 Virut 바이러스는 API 후킹(Hook)을 이용해서 다른 PE 파일들을 감염시킨다. [그림 4-6]은 Visual Studio의 유틸리티인 Depends를 이용하여 살펴본 NTDLL.DLL의 Export 함수이다. Virut 바이러스가 후킹(Hook)할 함수 ZwCreateFile의 EntryPoint는 0x0002595E이다. NTDLL.DLL의 Base 주소는 0x77F50000 이므로 실제 VirtualAddress는 0x77F7595E 일 것이다.



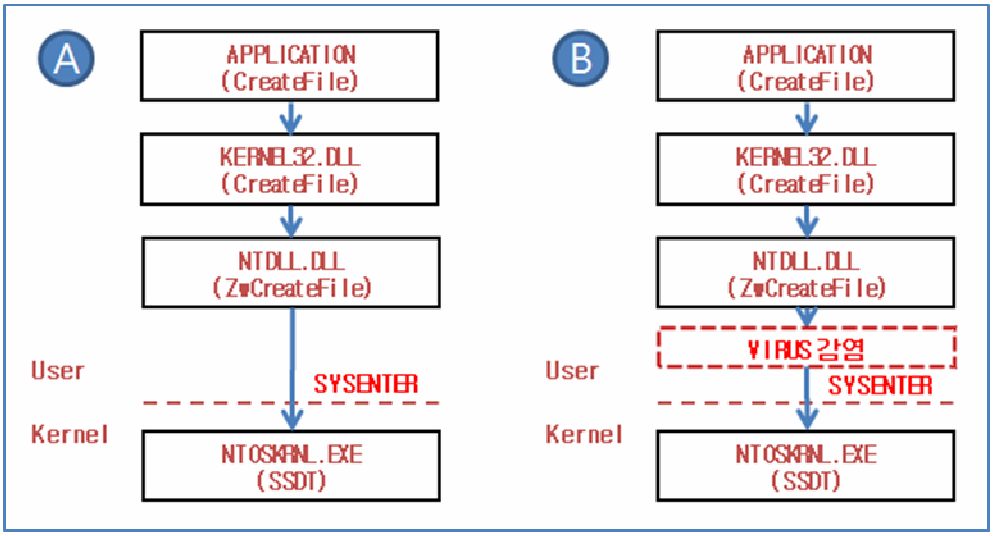
[그림 4-6] ntdll.dll의 export 함수

[그림 4-7]은 후킹되기 전과 후킹된 후의 어셈블리코드 상태에 대한 캡쳐 이미지이다. 왼쪽의 후킹 전 코드는 EAX 레지스터에 ZwCreateFile의 서비스 번호인 0x25번을 넣는 코드이며, 오른쪽의 후킹 후 코드는 바이러스의 특정함수를 호출하는 코드로 변경되어 있다.



[그림 4-7] 후킹 전후의 어셈블리 코드 상태 비교

이와 동일한 방법으로 나머지 ZwOpenFile, ZwCreateProcess, ZwCreateProcessEx Export 함수에 대한 5 바이트 메모리 패치(후킹)가 이루어진다. (NTDLL.DLL의 모든 Export 함수들은 시스템 서비스 함수를 호출하기 위한 시스템 서비스 번호(System Service Number)를 EAX 레지스터에, 스택에 존재하는 인자 값을 EDX 레지스터에 옮긴 다음, 커널 서비스 인터럽트를 발생시키는 INT 0x2E 혹은 SYSENTER를 발생시킨다.)



[그림 4-8] 바이러스 감염 위치

► Winlogon.exe의 바이러스 쓰레드

Virut이 생성한 오브젝트섹션("\BaseNamedObject\VtSect")에는 RemoteThread를 위한 코드와 후킹된 API 함수에 대한 감염코드가 존재한다. 오브젝트섹션은 메모리매핑을 통해 모든 실행된 프로세스의 메모리에 공유되며, 그 중에서 Winlogon.exe에 대해서만 매핑된 오브젝트의 Thread를 실행시킨다. RemoteThread의 순서화된 동작을 보면 다음과 같다.

1. 시스템 OS에 따른 WFP(Windows File Protection) 무력화 - 윈도우 자체 파일보호를 위한 WatcherThread(SFC.DLL or SFC_OS.DLL)를 중지시키는 방식을 통하여 시스템 파일도 감염대상으로 하고 있다.
2. 중복감염 방지에 대한 이벤트 객체를 통한 동기화 ("Vx_4")
3. 외부연결 파일다운로드 및 실행 - 분석 중에는 Win-Trojan/Agent.40960.HB 악성코드를 다운로드하여 실행하였으며, 다운로드된 악성코드는 중국 사이트 (alexa.XXXXXX.cn)로 연결 또 다른 악성코드를 다운로드하는 등의 연속적인 감염이 이루어지고 있었다.
4. IRC 채팅 서버로의 연결을 통한 명령대기
   - Ircd.XXXX.pl (NICK qsfzqiie, USER I, JOIN &virtu)
   - Proxim.ircXXXXXX.pl

   (접속 URL 주소는 악용방지를 위해 'X'로 일부 문자를 변경, 표기하였다.)

이상으로 Virut 바이러스에 대한 전반적인 사항에 대해서 살펴보았다. Virut의 특징인 API 후킹에 의한 감염 때문에 사용자가 수동으로 치료한다는 것은 거의 불가능하다. 대부분의 바이러스 백신업체에서 전용백신을 따로 만들어 배포하는 것도 이러한 특징 때문이기도 하다.

문제가 발생하기 전에 사전방역을 확실히 하는 것이 더 중요하다는 원리는 해당 바이러스에서도 마찬가지라고 할 수 있다.

(2) 실행 압축 파일 진단의 장단점

► 패커란

실행 압축 파일(ExePacker, 이하 패커)은 실행 파일에서 불필요한 부분을 제거하고 코드와 데이터를 압축해서 실제 파일 크기 보다 작게 만든 파일이다. 도스 시절 부족한 디스크 공간을 효율적으로 사용하기 위해 실행 파일의 크기를 줄이는 LZEXE, DIET, PKLITE 등이 알려져 있다. 윈도우 시대로 넘어오면서 디스크 공간 확보의 목적 뿐만 아니라 리버스 엔지니어링(Reverse Engineering)을 통하여 분석을 어렵게 하기 위한 목적으로도 이용된다.

패커는 악성코드에서 많이 이용되지만 자신을 보호할 필요가 있는 보안 프로그램이나 언더그라운드에서 제작되는 크랙 파일 등에도 사용된다. 패커는 크게 단순히 길이를 줄이기 위한 압축형(Compressor), 분석을 방지하기 위해 단순 암호화 방법을 사용하는 암호형(Cryptor), 여러 파일 설치형(Installer), 압축보다 안티 디버깅 기법(anti-debugging tricks)등 원래 코드 분석을 방해 목적이 강한 보호형(Protector) 등으로 나뉜다. 일반적으로 악성코드에서는 압축형, 암호형, 보호형이 사용되며 이들이 혼합되기도 한다.

► 악성코드에서 패커 이용

악성코드에서 이들 프로그램을 이용 하는 이유는 다음과 같다.

첫째, 악성코드 크기가 줄어듦: 악성코드는 비정상적인 활동을 하므로 자기복제, 전송 등의 시간을 줄이기 위해서 악성코드의 길이가 가급적 짧을 필요가 있다. 하지만, 최근 컴퓨터나 네트워크 성능이 좋아지면서 악성코드 크기에 대한 민감성은 많이 줄어들었다.

둘째, 안티 바이러스의 진단을 피할 수 있음: 패커 이용의 가장 큰 목적은 안티 바이러스의 진단을 피하는 것이다. 변형이 많을 경우 안티 바이러스 회사는 악성코드에서 발견되는 고유값이 아닌 유사 변형을 진단할 수 있는 기능을 추가한다. 악성코드 제작자 입장에서는 소스코드를 상당히 수정하지 않는 이상 제작하는 변형이 사용자들에게 퍼지기도 전에 사전에 진단 될 수 있다. 하지만, 패커를 통해 실행 파일을 수정하면 유사 변형에 대한 진단 기능이 있는 안티 바이러스 제품도 해당 실행 압축을 해제하지 못하면 진단 할 수 없다. 실제로 패커가 잘 알려지기 시작한 2004년은 유사 악성 IRC봇 변형이 대량으로 등장한 시기이다.

셋째, 분석을 어렵게 할 수 있음: 분석 방해 기능이 포함된 패커로 분석가의 분석을 지연해 결과적으로 악성코드의 생존 기간을 연장 시키려는 목적으로 이용된다. 최근 악성코드는 40%만 일주일간 활동하고 30일 동안 활동하는 악성코드 역시 15%에 불과하다. 따라서, 악성코드 제작자는 동일한 목적을 이용해 사용되지만 분석을 최대한 어렵게 하고 많은 변형을

동시에 배포해 생존 확률을 높일 필요가 있다.

► 패커를 둘러싼 보안업체와 악성코드 제작자들

기존에 진단되는 웜이나 트로이목마를 패커로 압축하면 전혀 다른 파일이 되어 해당 패커를 해제하지 못하는 안티 바이러스 제품은 진단 할 수 없었다. 이에 안티 바이러스 프로그램은 널리 사용되는 패커에 대한 압축 해제 기능을 조금씩 추가하기 시작한다. 하지만, 2004년 악성 IRC봇 소스가 공개되면서 같은 소스에서 접속 IRC 서버 주소만 조금씩 수정된 변형이 전 세계적으로 수없이 등장하기 시작했다. 소스코드 제작자는 안티 바이러스 제품에서 진단되지 않는 방법으로 패커의 사용을 알려주었고 패커의 사용이 악성코드 제작자들 사이에 일반화 되었다. 더 이상 언패킹 기능이 부가기능이 아닌 필수 기능이 되면서 안티 바이러스 제품에서도 알려진 패커의 해제 기능이 강화되었다.

2005년부터 악성코드 제작자들은 널리 알려져 있지 않은 패커를 이용하거나 기존에 나와있는 패커를 일부 수정해 자신만의 패커를 만들어 이용하기 시작했다. 또 흔히 PE 패치로 불리는 실행 코드를 일부 수정해 안티 바이러스 프로그램에서 패커 이용 사실을 알 수 없게 하는 방법도 증가했다. 개인적으로 제작된 패커와 PE 패치가 급증하면서 안티 바이러스 업계에서는 패커를 풀어서 내용을 보고 진단하는 방식보다 일반적이지 않은 패커를 사용하거나 다중 압축된 파일은 악성코드의 가능성이 매우 높으니 이들에 대한 진단 가능성에 대한 견해가 나타났고 2006년부터 더욱 많은 샘플 증가로 특정 패커를 진단하는 안티 바이러스 프로그램이 늘어나기 시작했다.

► 패커 진단의 이점

패커 자체를 진단 했을 때 장점은 알려지지 않은 악성코드 진단이다. 물론 이는 정확히 코드를 분석해 악성코드라고 확인하고 진단하는게 아닌 특정 패커 자체를 진단하기 때문에 악성코드로 의심된다는 성격이 강하다. 하지만, 바이러스 버스터사의 통계에 따르면 2007년 1/4 분기에 접수된 샘플 중 2만 여 개를 자사의 패커 진단 기능으로 진단했고 적은 수의 정의 데이터로 높은 효율을 얻을 수 있음을 알 수 있다.

	진단 샘플	시그니처 수	비고
특정(Specific) 진단	24 만개	14 만개	특정 값. 패킹을 풀 필요 없음. 오진 가능성 낮음
일반적(Generic) 진단	6 만개	800 개	특정 변형에 대한 공통점 진단. 패킹되어 있을 경우 패킹을 풀어야 함. 오진 가능성 낮음
패커 (Packer)진	6 만개	20 개	악성코드 아닐 수 있음. 패킹 풀 필요 없

단			음. 오진 가능성 낮음

[표 4-1] 패커 진단의 효율성

► 패커 진단의 문제점

패커 진단에 여러가지 이점도 있지만 문제점도 존재한다.

첫째, 악성코드 확인이 안된 진단: 일반적으로 안티 바이러스에서 악성코드는 악의적인 행동이 확인되었을 때 진단에 추가된다. 하지만, 패커를 진단하는 것은 패커 안에 숨겨진 코드가 어떤 내용인지 전혀 알 수 없이 진단한 것이다. 악성코드 확인 없이 진단하는 건 결과적으로는 좋지만 악성코드라고 확인되지 않는 파일에 대한 진단은 논란의 여지가 분명히 있다.

둘째, 오진 가능성: 패킹 안의 내용이 아닌 패커 자체로 진단하므로 정상 파일을 진단하는 오진 가능성이 존재한다. 잘 알려지지 않은 패커를 정상 프로그램에서는 사용될 가능성이 적지만 전혀 없는게 아니며 일부 보안 프로그램은 해커들로부터 분석을 어렵게 하기 위해 상용 패커를 이용하거나 자체 패커로 자신을 보호하기도 한다.

셋째, 상용 제품 진단 어려움: 상용 패커나 널리 알려진 패커는 진단하기 매우 어렵다. 사용업체의 항의나 소송 문제뿐 아니라 해당 패커를 사용한 제품도 많으므로 진단에 사용할 패커 선정은 신중해야 한다. 예를들어 중국에서 제작된 Upack을 기본으로 진단하는 제품의 경우 Upack은 중국 이외에는 거의 사용되지 않지만 중국에서는 정상 프로그램에서도 이용된다. 만약 Upack을 기본으로 진단하는 제품이라면 중국에서 해당 안티 바이러스 제품 사용은 큰 불편이 따르므로 적어도 중국 내에서는 진단정책 변경이 불가피 할 수 있다.

► 패커에 대한 안티 바이러스 현황

기본적으로 상용 패커는 진단에서 제외된다. 진단에 사용되는 패커는 개인적으로 제작되어 일반에 알려지지 않았거나 일반에 알려졌어도 일반적으로 사용되지 않고 대부분 악성코드에서 이용이 확인된 형태이다.

포티넷의 브랸 루(Bryan Lu)가 바이러스 블루틴 2007 컨퍼런스에서 발표한 자료에 따르면 자사에서 집계한 샘플을 분석한 결과 윈도우 악성코드의 40%가 실행 압축되어 있었다. 바이러스 블루틴(Virus Bulletin) 2007년 10월호에 헝가리 바이러스 버스터(VirusBuster)의 가보르 스자파노스(Gabor Szappanos) 연구원에 따르면 와일드리스트에 오른 739개 샘플 중 54개만 패킹되어 있지 않고 나머지 92%가 패킹되어 있으며 사용된 패커는 30 가지 이상이라고 한다.

실제로 2007년 국내에서 발견된 악성코드를 검사해보면 몇몇 제품은 TR/Crypt.NSPM.Gen, Win32/NSAnti 등의 이름으로 패커 자체를 진단했음을 알 수 있다.

Antivirus	Version	Last Update	Result
AhnLab-V3	2007.10.8.0	2007.10.08	Win-Trojan/InfoStealer.24848
AntiVir	7.6.0.20	2007.10.07	TR/Crypt.NSPM.Gen
Authentium	4.93.8	2007.10.05	W32/Trojan.BERE
Avast	4.7.1051.0	2007.10.08	Win32:Agent-HWE
AVG	7.5.0.488	2007.10.07	Win32/NSAnti
BitDefender	7.2	2007.10.08	Packer.Malware.NSAnti.F
CAT-QuickHeal	9.00	2007.10.06	-
ClamAV	0.91.2	2007.10.08	Trojan.Spy-12663
DrWeb	4.44.0.09170	2007.10.07	Trojan.PWS.Gamania
eSafe	7.0.15.0	2007.10.07	suspicious Trojan/Worm
eTrust-Vet	31.2.5190	2007.10.06	Win32/NSAnti
Ewido	4.0	2007.10.07	Trojan.NSAnti.r
FileAdvisor	1	2007.10.08	-
Fortinet	3.11.0.0	2007.10.08	W32/NSAnti.R
F-Prot	4.3.2.48	2007.10.06	W32/Trojan.BERE
F-Secure	6.70.13030.0	2007.10.08	Packed.Win32.NSAnti.r
Ikarus	T3.1.1.12	2007.10.08	Trojan-PWS.OnlineGames.AWR
Kaspersky	7.0.0.125	2007.10.08	Packed.Win32.NSAnti.r
McAfee	5135	2007.10.05	-
Microsoft	1.2908	2007.10.08	Trojan:Win32/Agent!AE52
NOD32v2	2576	2007.10.07	Win32/Pacex.Gen
Norman	5.80.02	2007.10.05	-
Panda	9.0.0.4	2007.10.07	Generic Malware
Prevx1	V2	2007.10.08	-
Rising	19.44.01.00	2007.10.08	Packer.Mian007
Sophos	4.22.0	2007.10.08	-
Sunbelt	2.2.907.0	2007.10.06	Trojan-PWS.Onlinegames.AWR
Symantec	10	2007.10.08	-
TheHacker	6.2.6.079	2007.10.07	-
VBA32	3.12.2.4	2007.10.07	MalwareScope.Worm.Viking.3
VirusBuster	4.3.26:9	2007.10.07	Trojan.Onlinegames.Gen!Pac.30
Webwasher-Gateway	6.0.1	2007.10.07	Trojan.Crypt.NSPM.Gen

[그림 4-9] 패커를 진단해 알려지지 않은 신종을 진단하는 제품들

► 향후 전망

안티 바이러스 업계에서는 엄청나게 증가한 악성코드를 진단하기 위한 방안 중 하나로 패커를 진단하기 시작했다. 악성코드 제작자들은 안티 바이러스 프로그램에 대항하기 위한 새로운 무기로 패커를 선택했고 이를 적극 이용하고 있다. 악성코드 수는 급격히 증가하고 이를 모두 분석하지 못하는 현실에서 안티 바이러스 프로그램의 패킹된 파일에 대한 진단은 점점 증가할 것이다. 하지만, 이는 단점도 존재하므로 안티 바이러스 업계는 패킹 자체를 진단하는 것 뿐만 아니라 보다 다양한 패커를 해제하고 해제된 내용으로 진단하는 방식도 강화해야 할 것이다.

► 참고문헌

[1] Gabor Szappanos, Exepacker blacklisting, Virus Bulletin 20007.10 p.14-19
[2] Bryan Lu, A Deeper Look at malware – The Whole Story, Virus Bulletin 2007