ASEC REPORT

안철수연구소에서 발행하는 월간 보안 보고서

Vol. 06

안철수연구소

목 차

Ⅰ. 이달의 보안 동향

1. 악성코드 동향

악성코드 통계

2010년 6월 악성코드 통계현황은 다음과 같다.

순위	등락	악성코드명	건수	비율
1	↑ 1	TextImage/Autorun	429,086	17.4 %
2	↑ 1	Win32/Induc	275,263	11.2 %
3	↑ 1	Win-Trojan/Overtls.575488	191,221	7.8 %
4	↑ 2	JS/Redir	128,610	5.2 %
5	↑ 2	Win32/Parite	125,820	5.1 %
6	↑ 5	Win32/Olala.worm.57344	124,072	5 %
7	↑ 2	Win32/Virut.B	109,404	4.4 %
8	↑ 2	JS/Downloader	102,588	4.2 %
9	↑ 4	Win32/Conficker.worm.Gen	101,029	4.1 %
10	↓ 2	JS/Exploit	98,566	4 %
11	New	Win-Adware/Rogue.PrivacyScan.167312	97,038	3.9 %
12	New	Win-Trojan/Inject.1588224	93,837	3.8 %
13	↑ 1	ALS/Bursted	82,766	3.4 %
14	↑ 2	TextImage/Sasan	80,368	3.3 %
15	↑ 2	Win32/Virut	79,461	3.2 %
16	New	Win-Trojan/Bho.353792	79,324	3.2 %
17	↑ 1	TextImage/Viking	67,654	2.8 %
18	New	Win-Trojan/Clicker.323584	66,778	2.7 %
19	New	Win-Trojan/Adload.1133568	63,958	2.6 %
20	↓ 5	Win-Trojan/Daonol.Gen	62,514	2.5 %
			2,459,357	100 %

[표 1-1] 악성코드 감염보고 Top 20

2010년 6월의 악성코드 감염 보고는 TextImage/Autorun이 1위를 차지하고 있으며, Win32/Induc과 Win-Trojan/Overtls.575488가 각각 2위와 3위를 차지 하였다. 신규로 Top20에 진입한 악성코드는 총 5건이다.

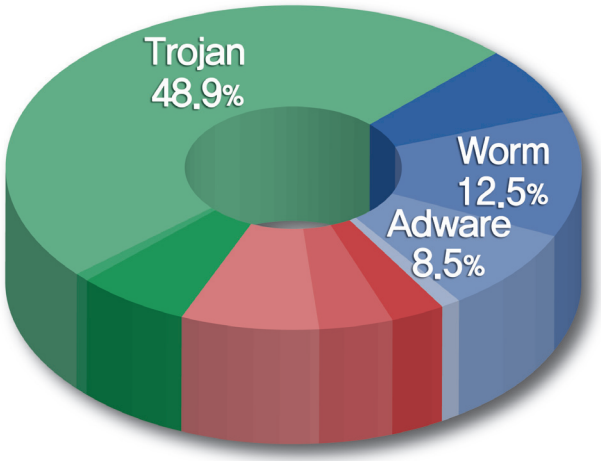
아래 표는 악성코드의 주요 동향을 파악하기 위하여, 악성코드별 변종을 종합한 악성코드 대표진단명 감염보고 Top200이다.

순위	등락	악성코드명	건수	비율
1	↑ 2	Win-Trojan/Agent	987,098	15.6 %
2	↓ 1	Win-Trojan/Onlinegamehack	694,532	11 %
3	↓ 1	Win-Trojan/Downloader	519,743	8.2 %
4	New	Win-Trojan/Adload	433,007	6.9 %
5	–	TEXTIMAGE/Autorun	431,915	6.8 %
6	–	Win32/Autorun.Worm	383,011	6.1 %
7	↑ 1	Win32/Virut	330,021	5.2 %
8	New	Win-Trojan/Bho	304,771	4.8 %
9	↑ 1	Win32/Conficker	287,818	4.6 %
10	New	Win-Adware/Rogue	280,305	4.4 %
11	↓ 2	Win32/Induc	275,325	4.4 %
12	↓ 5	Win-Trojan/Overtls	262,672	4.2 %
13	↑ 1	Dropper/Malware	209,816	3.3 %
14	↓ 1	Win32/Kido	162,153	2.6 %
15	↓ 3	Dropper/Onlinegamehack	134,694	2.1 %
16	↓ 1	Js/Redir	128,610	2 %
17	↓ 1	Win32/Parite	127,200	2 %
18	New	Win-Adware/Webside	126,480	2 %
19	New	Win32/Olala	125,536	2 %
20	New	Win-Trojan/Inject	116,961	1.9 %
			6,321,668	100 %

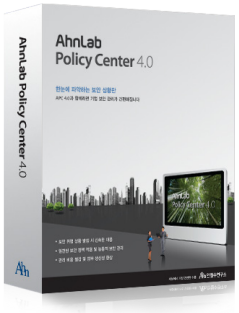
[표 1-2] 악성코드 대표진단명 감염보고 Top 20

2010년 6월의 감염보고 건수는 Win-Trojan/Agent가 총 987,098건으로 Top20중 15.6%의 비율로 1위를 차지하고 있으며, Win-Trojan/Onlinegamehack이 694,532 건으로 2위, Win-Trojan/Downloader가 519,743건으로 3위를 차지 하였다.

아래 차트는 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.

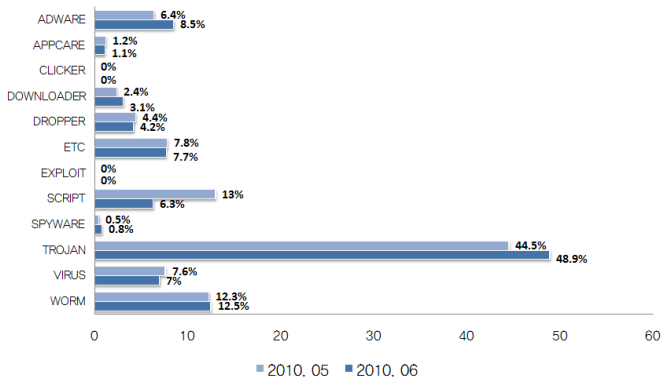


[그림 1-1] 악성코드 유형별 감염보고 비율



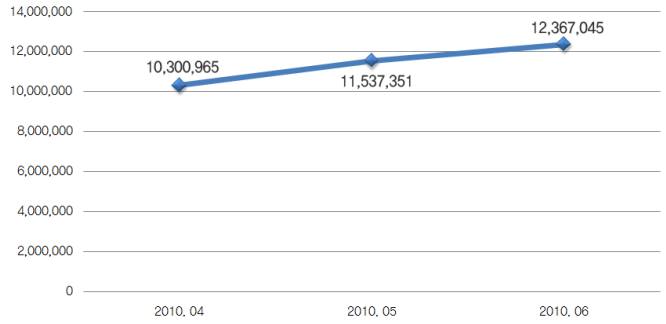
AhnLab Policy Center 4.0

2010년 6 월의 감염보고 건수는 악성코드 유형별로 감염보고건수 비율은 트로잔(TROJAN)류가 48.9%로 가장 많은 비율을 차지하고, 웜(WORM)가 12.5%, 애드웨어(ADWARE)가 8.5%의 비율을 각각 차지하고 있다.



[그림 1-2] 악성코드 유형별 감염보고 전월 비교

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



[그림 1-3] 악성코드 월별 감염보고 건수

6월의 악성코드 월별 감염보고 건수는 12,367,045건으로 5월의 악성코드 월별 감염 보고건수 11,537,351건에 비해 829,694건이 증가하였다.

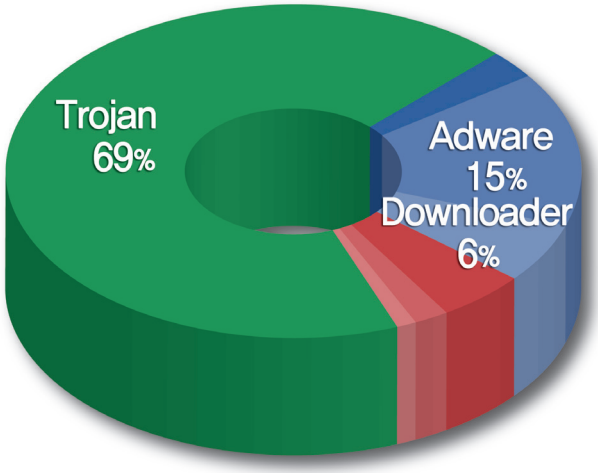
AhnLab V3 MSS

아래 표는 6월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top20이다.

순위	악성코드명	건수	비율
1	Win-Adware/Rogue.PrivacyScan.167312	97,038	10.1 %
2	Win-Trojan/Inject.1588224	93,837	9.8 %
3	Win-Trojan/Bho.353792	79,324	8.3 %
4	Win-Trojan/Clicker.323584	66,778	7 %
5	Win-Trojan/Adload.1133568	63,958	6.7 %
6	Win-Dropper/Rogue.TrueScan.1247048	50,563	5.3 %
7	Win-Trojan/Agent.107688	49,741	5.2 %
8	Win-Trojan/Adware.309248	47,309	4.9 %
9	Win-Trojan/Adload.1146880	44,830	4.7 %
10	Win-Trojan/Jascript	44,580	4.6 %
11	Win-Trojan/Downloader.210432.C	41,568	4.3 %
12	Win-Trojan/Adload.630784.C	40,676	4.2 %
13	Win-Trojan/Bho.180224.W	36,443	3.8 %
14	Win-Trojan/Adload.630784.G	33,494	3.5 %
15	Win-Adware/Rogue.NPrivacy.71420	31,339	3.3 %
16	Win-Trojan/Agent.110592.PP	31,293	3.3 %
17	Win-Trojan/Bho.718336.B	31,250	3.3 %
18	Win-Downloader/Pccap.12800	27,956	2.9 %
19	Win-Trojan/Adload.630784.F	25,018	2.6 %
20	Win-Trojan/Genome.101376.R	23,196	2.4 %
		960,191	100 %

[표 1-3] 신종 악성코드 감염보고 Top 20

6월의 신종 악성코드 감염 보고의 Top 20은 Win-Adware/Rogue. PrivacyScan. 167312가 97,038건으로 전체 10.1%를 차지하여 1위를 차지 하였으며, Win-Trojan/Inject.15882224가 93,837건 2위를 차지하였다.



[그림 1-4] 신종 악성코드 유형별 분포

6월의 신종 악성코드 유형별 분포는 트로잔이 69%로 1위를 차지하였다. 그 뒤를 이어 애드웨어가 15%, 다운로더가 6%를 각각 차지하였다.

악성코드 이슈

어도비 PDF, SWF 취약점 관련

이번에 알려진 취약점은 PDF 자체의 취약점이라기 보다는 PDF 내부에 포함 SWF 파일에 기인한다. 이것과 비슷한 취약점은 'Adobe Acrobat

Reader Flash Player Remote Code Execution(CVE-2009-1862)' 으로 보고 된 적이 있었다. 악의적인 PDF 는 다음과 같은 형태를 가지고 있다.

[그림1-5] 악의적인 PDF 문서의 구조

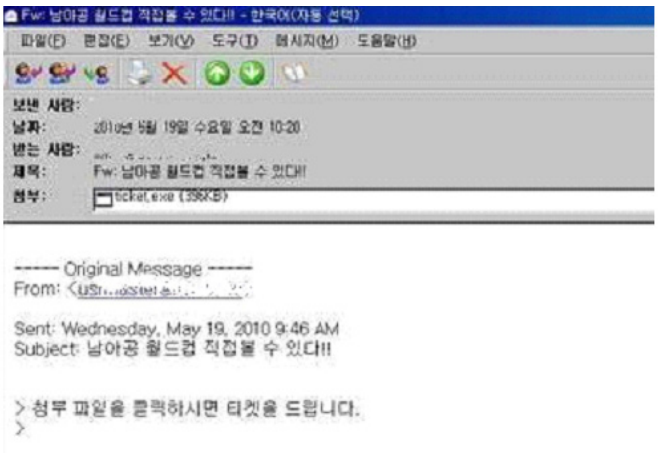
암호화된 EXE 파일은 실행 후 특정 호스트로부터 파일을 다운로드 및 실행한다. 여기서 생성된 DLL 파일은 시스템 정상파일인 qmgr.dll을 자신으로 변경하고 동작한다. 동작 후 악의적인 증상으로는 시스템 정보와 서비스 및 응용 프로그램 설치 정보를 특정 호스트로 전송 한다. PDF 와 SWF 취약점이 일반화된 요즘 해당 프로그램에 대한 보안 업데이트가 시급하다. 사용자 및 관리자들은 이러한 추세를 인지하여 자신 및 기업이 사용하고 있는 해당 프로그램에 대해 관심있는 업데이트가 필요하다.

메일을 이용한 형태의 악성코드

6월 중순, 메일에 *.html 형태의 파일이 첨부된 스팸성 메일이 지속적으로 유포 되었다. 해당 메일은 다음과 같은 형태로 되어 있었으며 메일 제목과 본문 내용은 변경 되어 지속적으로 유포 되었다.

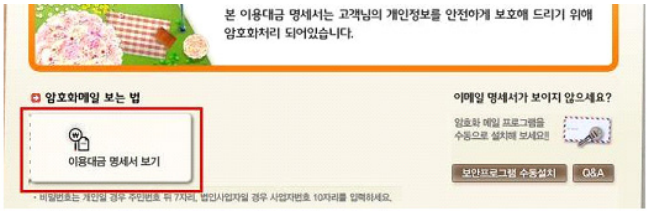
[그림1-6] 스팸성 메일 형태

첨부된 파일을 클릭하면 특정 웹 사이트로 이동하며 최종적으로 성인 약품 광고 사이트로 이동한다. 일부 변형에서는 악성코드를 다운로드 하는 웹 페이지도 알려졌으나 확인은 되지 않았다. 이처럼 월드컵 시즌에 이를 이용한 허위 메일이 기승을 부릴 가능성이 높다. 또한 *.exe 확장자와 같은 실행 가능한 파일이 아닌 스크립트를 이용한 형태의 스팸성 메일에 주의를 기울여야 한다. 또 다른 형태로는 국내 사용자를 노린 것으로 특정 카드사의 요금 명세서를 가장한 형태이다. 이와 비슷하게 5월 중순에는 다음과 같은 형태로 실행 가능한 첨부파일이 포함된 형태로 발견 되기도 하였다. 이번에 발견된 금융사 사칭 메일은 5월에 발견된 형태의 다른 변형으로 추정 된다. 형태는 각각 다음과 같다.



[그림1-7] 5월에 발견된 악성코드가 첨부된 메일 형태

이번 달에 발견된 형태는 특정 금융사의 이메일 카드 명세서로 위장 되었다. 아래 빨간 박스의 이용대금 명세서 보기를 클릭하면 실제 해당 카드사가 아닌 공격자가 설정한 호스트로 이동한다.



[그림1-8] 6월에 발견된 악성코드가 첨부된 메일 형태

그리고 다음과 같은 특정 키보드 보안 프로그램을 설치 하도록 유도하는데 이는 허위로, 실제로는 키보드 보안 프로그램이 아니다.

[그림1-9] 허위 키보드 보안 프로그램 설치를 유도

실제로는 다음과 같은 파일을 설치한다.

[그림1-10] 실제 설치되는 악성코드

해당 파일이 설치 및 실행 되면 특정 서버로부터 똑같은 형태의 메일을 받아와 발송한다. 이처럼 5월에는 월드컵 관련 및 특정 가수등과 관련된 내용을 발송 했었다. 6월에 발견된 경우에는 금융사의 신용카드 명세서를 확인하는 내용을 보내게 되는데 이는 서버로부터 메일 내용과 주소를 받아와 보내게 된다. 즉, 감염된 시스템은 악의적인 메일을 보내는 시스템이 되고 또한 특정 포탈에 대하여 분산 서비스 공격(DDoS)를 하도록 설정 되어 있기 때문에 다른 시스템과 서비스에 피해를 주는 공격도구로

변모한다. 최근 들어 메일을 이용한 악성코드 전파가 기승을 부리고 있다. 메일은 전통적으로 악성코드 전파에 즐겨 사용 되었다. 최근의 추세라면 국내의 경우 점차 정교한 한글 메시지가 포함된 형태가 늘어 날 것으로 전망 되므로 메일 내 첨부된 파일 및 링크 클릭 시 반드시 주의를 기울이고 기본적으로 안티 바이러스 제품 설치 및 악의적인 웹 사이트 여부를 판별 해줄 수 있는 평판 서비스 및 제품을 함께 이용하는 것이 좋다. 해당 파일이 설치 및 실행 되면 특정 서버로부터 똑같은 형태의 메일을 받아와 발송한다.

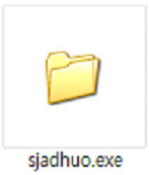
네이트온을 통해 유포되는 악성코드

네이트온을 통해 유포되는 악성코드가 많이 확산되고 있다. 네이트온을 통해 유포되는 악성코드는 주로 쪽지나 대화창을 통해 전달이 되며 유포 형태는 아래 그림과 같다.

[그림 1-11] 네이트온 악성코드 유포 형태

네이트온 악성코드는 쪽지나 대화창을 통해 URL이 전달되며 해당 URL로 접속 시 악성코드 파일을 다운로드 받게 된다. 최근 다운로드 받는 악성코드 형태가 많이 변화되고 있는데 현재까지 발견된 형태는 아래와 같다.

1. RAR 압축파일로 전달하여 압축을 해제하면 아래와 같은 폴더 아이콘으로 폴더를 가장한 EXE 파일 형태

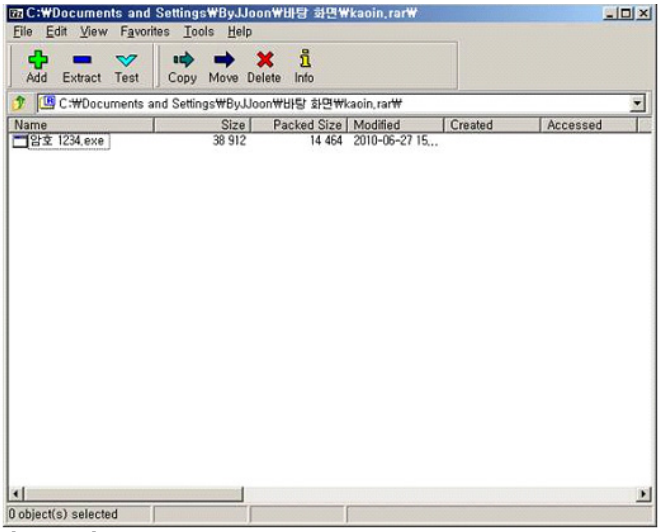


[그림 1-12] 폴더 아이콘을 위장한 악성코드

2. EXE 파일로 악성코드를 바로 전달하는 경우

3. RAR 압축파일로 전달하여 압축을 해제하면 vbs 파일이 나오는 경우

4. RAR 압축파일이나 암호가 걸려 있으며 아래 그림과 같이 암호를 유추할 수 있는 경우



[그림 1-13] RAR 압축 파일로 암호가 걸려 있으나 아래와 같이 암호를 유추할 수 있는 경우

기존에는 1, 2번과 같이 단순히 EXE 파일 혹은 압축 파일 형태로 전송했으나 최근 V3제품의ASD 엔진에서의 빠른 대응 및 제품의 압축파일까지 검사하는 기능에 의해 선방하고 있는 형태이다.

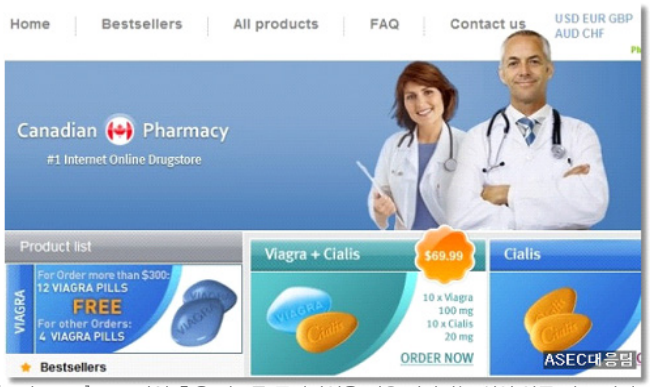
하지만 이런 점을 감안하여 최근 악성코드 제작자가 vbs 같은 스크립트 형태의 파일로 유포하여 실시간 감시를 우회하거나 압축파일에 암호를 걸어 압축파일 검사를 우회하는 형태가 발견되었으니 주의가 필요하다.

스팸메일을 통해 유포되는 악성코드의 형태

최근 아래와 같은 제목으로 스팸메일에 악성 URL의 링크를 삽입하여 접속을 유도하여 악성코드를 감염시키는 사례가 확인이 되었다.

Amazon.com: Get Ready for Cyber Monday Deals
이메일주소 has sent you a birthday ecard.
FaceBook message: intense sex therapy
Reset your Facebook password
Reset your Twitter password
FIFA World Cup South Africa... bad news
도메인명 account notification

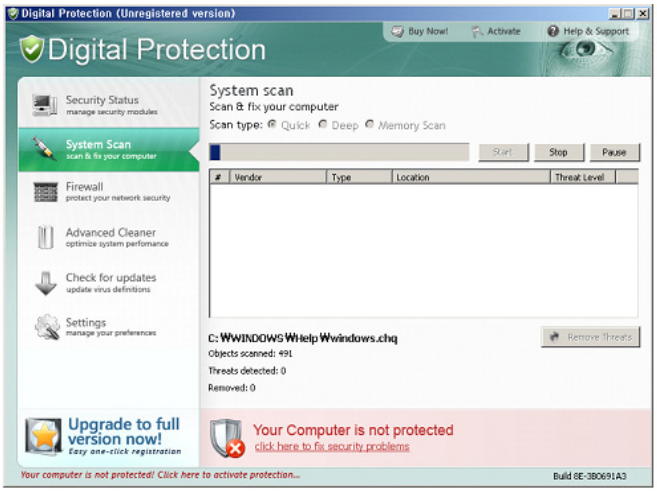
위 제목 외에도 다수의 제목이 존재하며 해당 메일에 포함된 html 파일 혹은 링크를 클릭할 경우 악성코드를 유포하는 사이트 및 성인약품 광고 사이트로 자동 접속되게 된다.



[그림 1-14] html 파일 혹은 링크를 클릭하였을 경우 나타나는 성인 약품 광고 사이트

악성코드를 유포하는 사이트는 현재 확인된 바로는 MDAC (MS06-014), JAVA(CVE-2010-0886), Adobe Acrobat Reader취약점을 이용하여 악성코드를 다운로드 및 실행을 하게 된다.

설치되는 악성코드는 아래와 같은 허위 백신이며 설치가 될 경우 치료를 위해 결제를 요구하거나 스팸 메일이 발송되는 증상이 발생한다.

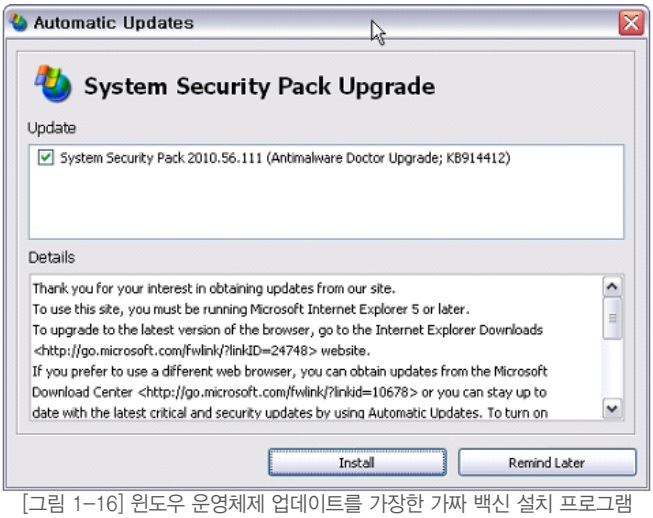


[그림 1-15] 설치되는 허위 백신

예방방법은 우선 무엇보다 중요한 것은 발신자가 불분명한 메일은 열람하지 않는 것이 첫째이며, 둘째는 Adobe Acrobat Reader나 JRE 같은 주요 어플리케이션에 대한 보안패치 및 윈도우 운영체제의 보안패치를 하는 것이다.

사회공학적 기법을 이용한 악성코드 배포

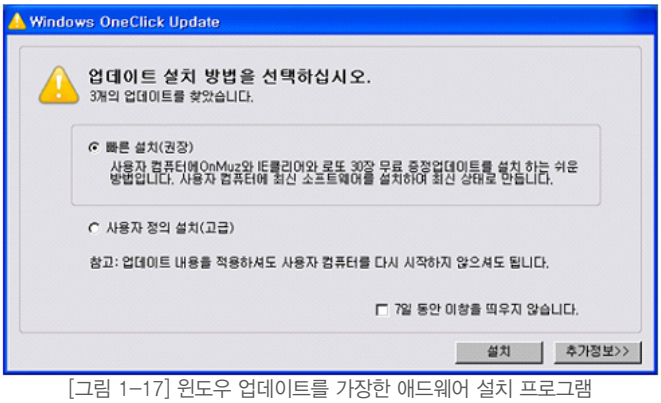
최근 Antimalware Doctor이라는 가짜 백신을 윈도우 운영체제 업데이트를 가장해서 설치하는 사례가 발견되었다.



[그림 1-16] 윈도우 운영체제 업데이트를 가장한 가짜 백신 설치 프로그램

[그림 1-16]에서 알 수 있듯 실제 윈도우 운영체제 업데이트와 동일한 형태를 가지고 있으므로 컴퓨터에 대한 전문적인 지식이 없는 일반적인 사용자들은 의심 없이 가짜 백신을 설치하게 된다. 이때 설치된 Antimalware Doctor 역시 윈도우 보안센터와 비슷한 형태로 구성되어 있어 윈도우 운영체제에서 제공되는 보안 기능으로 착각할 수 있다. 따라서 사용자는 허위/과장 진단된 결과로 유료 결제를 유도한다.

한국에서도 동일하게 윈도우 업데이트를 가장해 윈도우 부팅 시마다 애드웨어를 추가로 설치하는 사례가 발견되었었다.



[그림 1-17] 윈도우 업데이트를 가장한 애드웨어 설치 프로그램

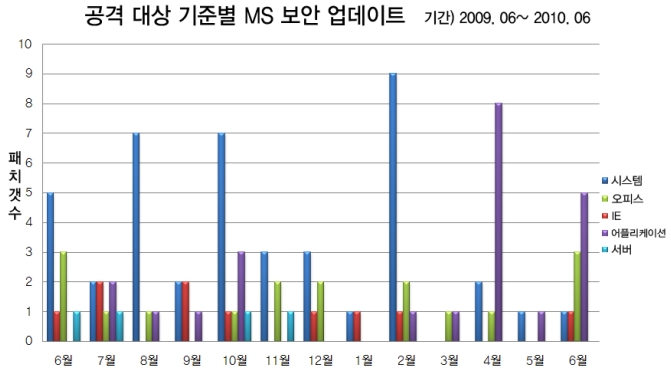
하나의 애드웨어가 설치되면 그 애드웨어가 윈도우 업데이트 형식의 다운로드 프로그램을 실행하고 또 다른 애드웨어를 다운로드 받아 설치한다. 특히 해당 업데이트를 취소하는 버튼이 없으므로 사용자는 무조건 해당 애드웨어를 설치할 수 밖에 없다. 즉, 사용자는 원하지 않는 애드웨어를 지속적으로 다운로드 받고 설치하게 되어 결국 컴퓨터를 정상적으로 사용할 수 없게 된다. 이렇듯 누구나 신뢰하는 윈도우 업데이트 프로그램으로 가장해 악성코드를 배포하는 일종의 사회공학적 기법이 적용되었으며 앞으로도 더욱더 정교한 사회공학적 기법이 적용될 것으로 예상된다. 사용자들은 프로그램을 설치하기 전에 보다 신중하게 해당 프로그램을 살펴볼 필요가 있다.

2. 시큐리티 동향

시큐리티 통계

6월 마이크로소프트 보안 업데이트 현황

마이크로소프트사로부터 발표된 이번 달 보안 업데이트는 총 10건이다.



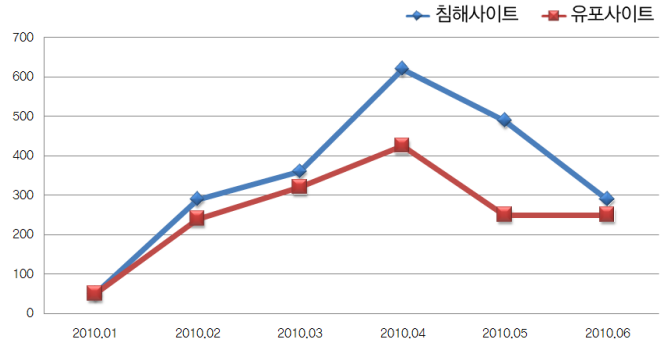
[그림 2-1] 공격 대상 기준 별 MS 보안 업데이트

위험도	취약점	POC
긴급	MS10-033 미디어 압축 해제의 취약점으로 인한 원격 코드 실행 문제점	무
긴급	MS10-035 Internet Explorer 누적 보안 업데이트	무
중요	MS10-039 Microsoft SharePoint 의 취약점으로 인한 권한 상승 문제점	무
중요	MS10-040 IIS(인터넷 정보 서비스)의 취약점으로 인한 원격 코드 실행 문제점	무

[표 2-1] 2010년 6월 주요 MS 보안 업데이트

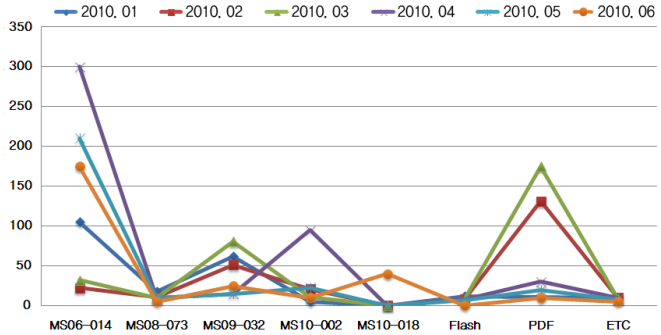
이 달에는 지난 달 MS 보안 권고문을 통해 알려진 SharePoint 제로데이 취약점에 대한 보안 업데이트(MS10-039)가 포함되어 있다. 한편, 발표된 보안 업데이들은 대부분 오피스, IIS(인터넷 정보 서비스), IE(인터넷 익스플러)와 같이 범용적으로 사용되는 어플리케이션 관련 취약점들이 많았다. 그러나, 아직까지 실제로 해당 취약점들을 이용한 공격은 보고되고 있지 않다.

악성코드 침해 웹사이트 현황



[그림 2-2] 악성코드 배포를 위해 침해된 사이트 / 배포지 수

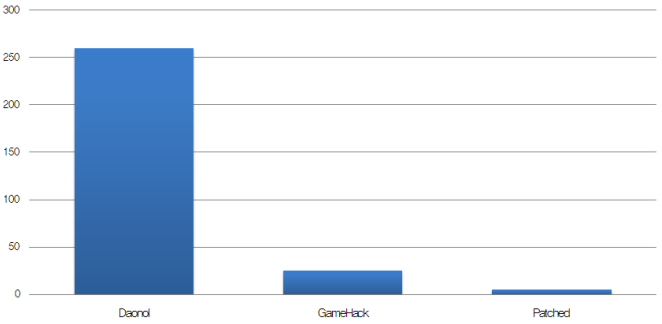
[그림 2-2]는 월별 악성코드 침해 사이트 현황을 나타낸 그래프로, 침해사이트는 2010.04월 이후로 감소세를 보이고 있지만 실제 악성코드를 유포하는 유포 사이트의 경우 전월과 비슷한 수준을 유지하고 있다.



[그림 2-3] 악성코드 배포를 위해 사용된 취약점

[그림 2-3]은 월별 침해사고가 발생한 웹사이트들에서 악성코드를 유포하기 위해서 사용했던 취약점들에 대한 통계로, 전월과 동일하게MS06-014취약점을 사용한 악성코드 유포가 가장 많았고 그 뒤를 MS10-018 취약점을 사용한 악성코드 유포 사례가 뒤를 잇고 있다.

이번 달 침해 사이트를 통해서 유포되었던 악성코드의 유형을 정리해 보면 Daonol, GameHack 그리고 Pached순이었다.



[그림 2-4] 유포된 악성코드의 유형

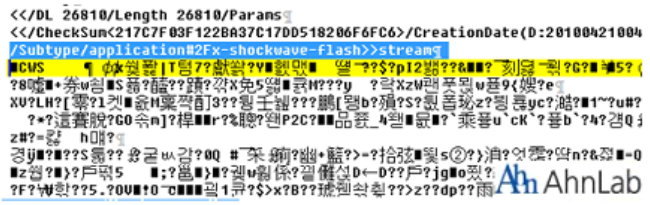
시큐리티 이슈

Adobe Reader & Flash Player 제로데이 취약점(CVE-2010-1297)

이 달 6월 5일(해외시각)에는 새로운 Adobe Acrobat Reader (PDF) 취약점이 보고 되었다. 해당 취약점은 2009년 07월에 보고되었던 **Adobe Acrobat Reader, Acrobat and Flash Player Remote Code Execution(CVE-2009-1862, APSA09-03) 취약점**과 유사하게 흥미로운 특징을 가지고 있다.

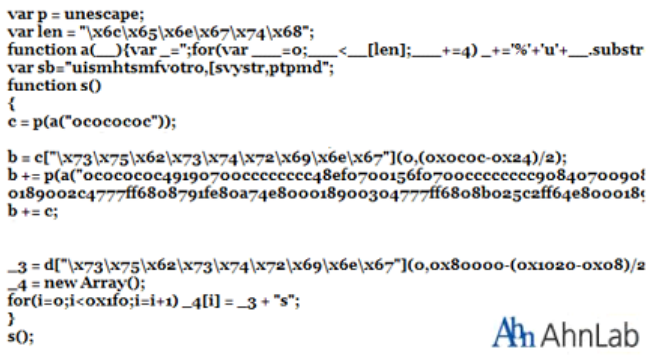
해당 취약점 또한 직접적인 Adobe Acrobat Reader상의 취약점이라기보다는 Adobe Flash Player 10.0.45.2 이하에 존재하는 취약점이 동일한 엔진(authplay.dll)을 탑재하고 있는 Adobe Acrobat Reader에 영향을 주는 형태이다.

실제 악성 PDF 파일의 내부를 살펴보면, 다음과 같이 직접적인 취약점을 내포하고 있는 압축된 Flash 파일(SWF 파일)이 포함되어 있다.



[그림 2-5] SWF 파일을 내포하는 PDF

또한, PDF 파일 내부에는 공격자가 원하는 명령을 실행하기 위해 Heap 공간에 쉘코드를 채우는 악의적인 자바스크립트가 압축형태로 포함되어 있다. 이번에 발견된 쉘코드는 ROP(Return Oriented Exploitation)라는 기존의 사용되던 방식과는 다소 다른 형태의 쉘코드가 이용되었다.



[그림 2-6] Heap-Spray 자바스크립트(쉘코드 내포)

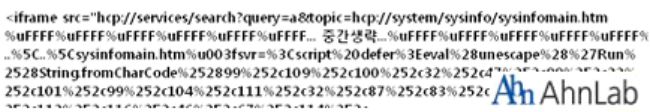
내포된 Flash 파일은 PDF 실행과 함께 취약점을 발생시키고 코드의 흐름을 공격자가 원하는 쉘코드로 점프시킨다. 쉘코드는 내부에 포함되어 있는 스트림을 디코딩하여 또 다른 악성코드("C:₩-.exe" -Win-Trojan/Downloader.32256.DF)를 드롭하여 실행하도록 제작되어 있다.

이미 Adobe사는 문제가 해결된 Adobe Flash Player 10.1.53.64 버전을 릴리즈한 상태이고, Adobe Acrobat Reader에 대한 보안패치도 6월 29일로 예고되고 있으므로 사용자들의 빠른 업데이트를 권고한다.

MS 윈도우 도움말 및 지원센터(helpctr.exe) 제로데이 취약점(CVE-2010-1885)

MS사에서는 06월 11일(한국시각)에 윈도우 도움말 및 지원센터 취약점에 대한 보안 권고문을 게시하였다. 이후, 6월 15일(한국시간)에는 실제 해외에서 해당 제로데이 취약점을 악용하는 사례가 보고되었다.

해당 취약점은 단순한 오버플로우 취약점이 아니라, 윈도우 도움말 및 지원센터 (helpctr.exe)가 HCP 프로토콜을 처리하는 과정에서의 오류로 인해 Whitelist Bypass 문제와 내부에서 사용되는 html 파일의 크로스사이트 스크립트(XSS) 취약점이 결합된 형태이다.



[그림 2-7] 취약점 스크립트

또한, 공격자는 HCP 프로토콜 요청에 대해서 사용자가 인지하지 못하도록 ASX HtmlView에서 IFRAME을 호출하는 방식으로 사용하고 있다.

실제로 해당 취약점은 다수의 단계를 거쳐서 발생하게 되고, 크로스사이트 스크립트(XSS) 취약점을 통해서 실행되는 자바스크립트 코드는 시스템 상에 또 다른 악성코드(Dropper/Selite.13193076)를 드롭하도록 이용되고 있다.

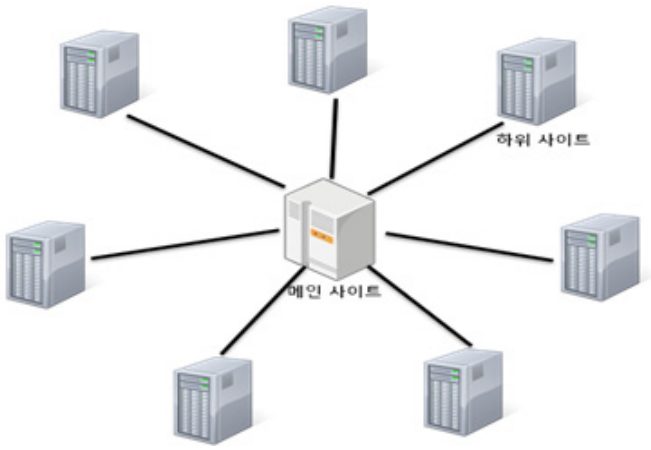
[그림2-8] XSS 자바스크립트

해당 취약점에 대한 아주 활발한 공격사례는 보고되고 있지 않으나, 현재 MS사 에서는 해당 취약점에 대한 정식 보안 업데이트를 배포하고 있지 않기 때문에 여전히 제로데이 취약점 악용 가능성이 남아있다.

침해 사이트 Case Study: 방송사 악성코드 유포사례

기존의 취약점을 이용한 악성코드 유포 사례는 특이한 점이 없었지만 [그림 2-3]에서도 볼 수 있었듯이 이번 달은 MS10-018 취약점을 사용한 악성코드 유포사례가 국내 사이트에서 상당수 발견되었다. 그 중에 침해사고가 발생한 방송사 사이트를 통해서 MS10-018취약점을 사용하여 악성코드가 유포되었던 건에 대해서 간단하게 정리해 보았다.

악성코드 유포가 유포되었던 방송사의 사이트 구조를 간단하게 나타내자면 아래와 같다.



[그림 2-9] 악성코드를 유포했던 방송사의 사이트 구조

하위 사이트들은 메인 사이트에서 필요한 콘텐트들을 링크하는 방식으로 구성되어 있었고, 이번 경우 메인 사이트의 특정 웹 페이지에 악성코드 링크가 삽입되어 있어 모든 하위 사이트에 영향을 받게 되어 있었다.

http://tri.*****.co.kr/(*****기술연구소’)
L http://www.*****.co.kr/menu_js/displayobject.js
L http://www.*****.co.kr/menu_js/sub_navi_01.js
L http://www.*****.co.kr/menu_js/sub_top.js
L http://intranet.*****.co.kr/INTRANET_COM/col**.asp (CVE-2010-0806, MS10-018)
L http://www.*****.org/common/jscalendar/doc/cl**.exe

3. 웹 보안 동향

웹 보안 통계

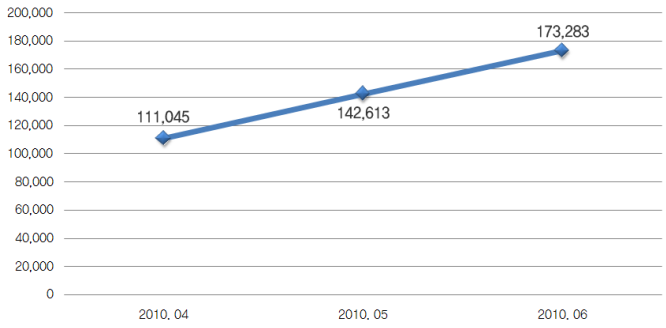
웹 사이트 보안 요약

구분	건수
악성코드 발견 건수	173,283
악성코드 유형	897
악성코드가 발견된 도메인	818
악성코드 발견된 URL	3,738
전달 악성코드 발견 건수	142,613
전달 악성코드 유형	930
전달 악성코드가 발견된 도메인	1,084
전달 악성코드 발견된 URL	4,950

[표 3-1] 웹 사이트 보안 요약

악성코드 발견 건수는 173,283건이고, 악성코드 유형은 897건이며, 악성코드가 발견된 도메인은 818건이며, 악성코드 발견된 URL은 3,738 건이다. 2010년 6월은 2010년 5월보다 악성코드 유형, 악성코드가 발견된 도메인, 악성코드 발견된 URL 은 다소 감소하였으나, 악성코드 발견 건수는 증가하였다.

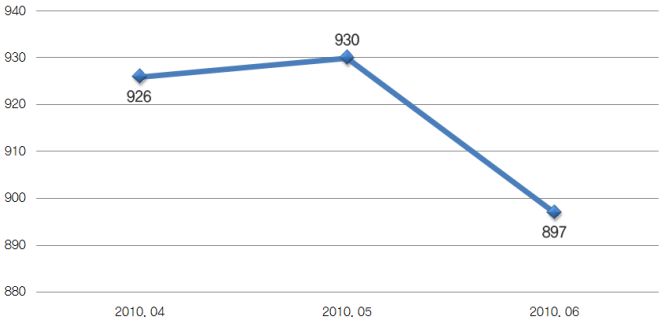
월별 악성코드 발견 건수



[그림 3-1] 월별 악성코드 발견 건수

2010년 6월 악성코드 발견 건수는 전달의 142,613건에 비해 122% 수준인 173,283건이다.

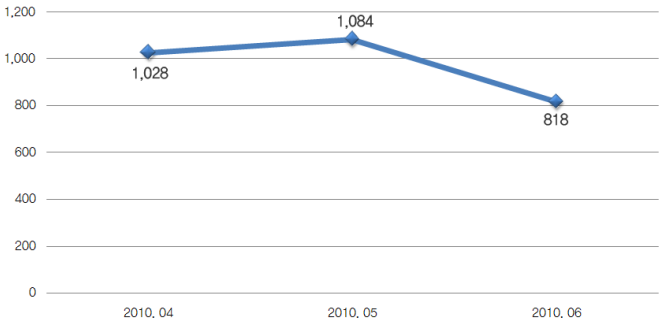
월별 악성코드 유형



[그림 3-2] 월별 악성코드 유형

2010년 6월 악성코드 유형은 전달의 930건에 비해 96% 수준인 897건이다.

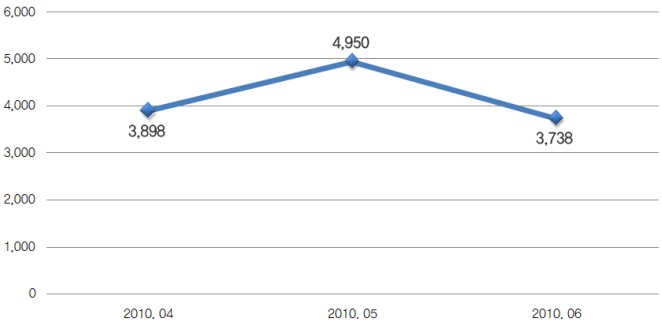
월별 악성코드가 발견된 도메인



[그림 3-3] 월별 악성코드가 발견된 도메인

2010년 6월 악성코드가 발견된 도메인은 전달의 1,084건에 비해 75% 수준인 818건이다.

월별 악성코드가 발견된 URL



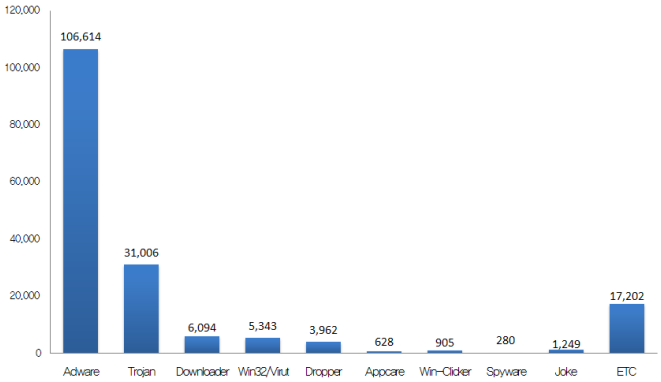
[그림 3-4] 월별 악성코드가 발견된 URL

2010년 6월 악성코드가 발견된 URL은 전달의 4,950건에 비해 76% 수준인 3,738건이다.

악성코드 유형별 배포 수

유형	건수	비율
ADWARE	106,614	61.5 %
TROJAN	31,006	17.9 %
DOWNLOADER	6,094	3.5 %
Win32/VIRUT	5,343	3.1 %
DROPPER	3,962	2.3 %
JOKE	1,249	0.7 %
WIN-CLICKER	905	0.5 %
APPCARE	628	0.4 %
SPYWARE	280	0.2 %
ETC	17,202	9.9 %
	173,283	100 %

[표 3-2] 악성코드 유형별 배포 수



[그림 3-5] 악성코드 유형별 배포 수

악성코드 유형별 배포 수에서 애드웨어(ADWARE)류가 106,614건 전체의 61.5%로 1위를 차지하였으며, 트로잔(TROJAN)류가 31,006건으로 전체의 17.9%로 2위를 차지하였다.

악성코드 배포 Top 10

순위	등락	악성코드명	건수	비율
1	↑8	Win-Adware/Woowa.28672	22,496	17.9 %
2	New	Win-Adware/Woowa.61440	20,483	16.3 %
3	New	Win-Adware/Woowa.24576	19,726	15.7 %
4	-	Win-Adware/Seveten.371968	13,691	10.9 %
5	↓4	Win-Adware/Shortcut.InlivePlayerActiveX.234	13,428	10.7 %
6	New	Win-Trojan/Infostealer.39424.E	9,188	7.3 %
7	New	Win-Trojan/Agent.197083	7,870	6.3 %
8	↓1	Win-Adware/Shortcut.IconJoy.642048	6,730	5.4 %
9	↓3	Win32/Induc	6,001	4.8 %
10	New	VBS/Agent	5,768	4.6 %
			125,381	100 %

[표 3-3] 악성코드 배포 Top 10

악성코드 배포 Top10에서 Win-Adware/Woowa.28672이 22,496건으로 1위를 차지하였으며, Top10에 Win-Adware/Woowa.61440등 5건이 새로 등장하였다.

웹 보안 이슈

OWASP Top10 2010

OWASP(Open Web Application Security Project)[1] 에서는 매년 웹 어플리케이션 환경에서 가장 중요한 위협 10[2]가지를 선정하여 발표하고 있다. 이를 통해 웹 어플리케이션 보안의 취약점을 인식하고, 예방함으로써 관련 공격으로 인한 피해를 줄이고자 하는 목적을 가지고 있다. 이번 ASEC 리포트 Vol.6에서는 최근에 발표된 OWASP Top 10을 통해 우리에게 다가온 웹 어플리케이션 위험과 예방 방법에 대해서 알아보자.

1. 인젝션

가. 위험

- SQL, OS, LDAP 인젝션과 같은 인젝션 결함은 신뢰할 수 없는 데이터가 명령어나 질의어의 일부분으로써 인터프리터에 보내 질 때 발생한다.
- 공격자의 악의적인 데이터는 예기치 않은 명령 실행이나 권한 없는 데이터에 접근하도록 인터프리터를 속일 수 있다.

나. 예방법

- 인젝션을 방지하려면 신뢰할 수 없는 데이터를 명령어와 질의로부터 항상 분리해야 한다.

2. 크로스사이트 스크립팅(XSS)

가. 위험

- XSS 결함은 적절한 확인이나 제한 없이 어플리케이션이 신뢰할 수 없는 데이터를 갖고, 그것을 웹 브라우저에 보낼 때 발생한다.
- XSS는 공격자가 피해자의 브라우저 내에서 스크립트의 실행을 허용함으로써, 사용자의 세션을 탈취하거나, 웹사이트를 변조하거나, 악의적인 사이트로 사용자를 리다이렉트 할 수 있다.

나. 예방법

- XSS를 방지하려면 활성 브라우저 콘텐츠와 신뢰할 수 없는 데이터를 항상 분리해야 한다.

3. 취약한 인증과 세션 관리

가. 위험

- 인증과 세션 관리와 연관된 어플리케이션 기능은 종종 올바로 구현되지 않는다. 그 결과, 공격자로 하여금 다른 사용자의 신분으로 가장할 수 있도록 패스워드, 키, 세션 토큰 체계를 위태롭게 하거나, 구현된 다른 결함들을 악용할 수 있도록 허용한다.

1. 기업/기관이 신뢰할 수 있는 어플리케이션을 개발, 구입, 유지할 수 있도록 어플리케이션 보안 툴, 표준, 연구결과 등을 공개적으로 제안하는 커뮤니티(http://www.owasp.org)

2. Security Plus 한글 번역 참고(http://cafe.naver.com/securityplus)

나.예방법

– 개발자들은 아래와 같은 권장사항을 준수하여야 한다.

. 강력한 인증 및 세션 관리 통제의 단일체계를 유지해야 한다.

. 세션 ID를 도용하는데 사용될 수 있는 XSS 취약점을 막기 위해 노력해야 한다.

4. 안전하지 않은 직접 객체 참조

가. 위험

– 직접 객체 참조는 파일, 디렉토리, 데이터베이스 키와 같이 내부적으로 구현된 객체에 대해 개발자가 참조를 노출할 때 발생한다.

– 접근 통제에 의한 확인이나 다른 보호가 없다면, 공격자는 이 참조를 권한 없는 데이터에 접근하기 위해 조작할 수 있다.

나. 예방법

– 사용자 혹은 세션 당 간접 객체 참조를 이용한다.

– 신뢰할 수 없는 소스로부터 직접 객체 참조가 사용되면, 각각의 사용에 대해 요청한 객체가 사용자에게 접근이 허용되었는지 확인하기 위해서 반드시 접근 통제 확인을 포함해야만 한다.

5. 크로스 사이트 요청 변조(CSRF)

가. 위험

– CSRF 공격은 로그온된 피해자의 브라우저가 취약한 웹 어플리케이션에 피해자의 세션 쿠키와 어떤 다른 자동으로 포함된 인증 정보를 갖고 변조된 HTTP 요청을 보내도록 강제한다.

– 이것은 공격자가 피해자의 브라우저로 하여금 취약한 어플리케이션이 피해자로부터의 정당한 요청이라고 착각하게 만드는 요청들을 생성하도록 강제하는 것을 허용한다.

나.예방법

– CSRF를 예방하는 방법은 각각의 HTTP 요청 URL이나 Body 내에 예측할 수 없는 토큰을 포함하는 것이다. 생성된 토큰은 최소한 사용자 세션 별로 반드시 고유값을 사용하되 각각의 요청마다 고유할 수도 있다.

6. 보안상 잘못된 구성

가. 위험

– 훌륭한 보안은 어플리케이션, 프레임워크, 어플리케이션 서버, 웹 서버, 데이터베이스 서버와 플랫폼에 대해 보안 구성이 제대로 정의되고 적용되도록 용구 한다.

– 대부분이 보안을 기본적으로 탑재하지 않기 때문에 이 모든 설정은 정의되고, 구현되고, 유지되어야 한다. 이것은 어플리케이션에서 사용되는 모든 코드 라이브러리를 포함하여 모든 소프트웨어가 최신의 상태를 유지하는 것을 포함한다.

나. 예방법

– 적절히 보호되는 또 다른 환경 구축을 쉽고 빠르게 만들 수 있는 반복 가능한 보안 강화 프로세스는 개발, 품질 보증, 생산 환경 모두에서 동일하게 구성되어야 한다.

– 모든 새로운 소프트웨어 업데이트와 패치를 각각의 배치환경에서 시기 적절하게 배포와 최신 수준을 유지하기 위한 프로세스가 있어야 한다.

7. 안전하지 않은 암호 저장

가. 위험

– 많은 웹 어플리케이션들이 적절한 암호나 해쉬를 갖고 신용카드 번호, 주민등록번호, 그리고 인증 신뢰 정보와 같은 민감한 데이터를 적절히 보호하지 않는다.

– 공격자는 자격 도난, 신용카드 사기, 또는 다른 범죄를 저지르기 위해 적절하지 못하게 보호된 데이터를 훔치거나 조작할 수 있다.

나. 예방법

– 민감한 데이터를 보호하려고 하는 위협(예, 내부자 또는 외부 사용자의 공격) 을 고려해야 한다.

– 위협으로부터 방어하기 위한 방법으로, 모든 민감한 데이터가 암호화 하였음을 확실히 해야 한다.

8. URL 접근 제한 실패

가. 위험

– 많은 웹 어플리케이션들이 보호된 링크나 버튼을 표현하기 전에 URL 접근 권한을 확인하다. 그러나, 어플리케이션은 이 페이지들이 접근될 때마다 유사한 접근 통제 확인이 필요하다

– 공격자는 감춰진 페이지에 접근하기 위해 URL을 변조할 수 있다.

나. 예방법

– 허가되지 않은 URL 접근을 방지하기 위해 각각의 페이지에 적절한 인증 및 접근 제어를 요구하는 접근 방식의 선택이 요구된다. 어플리케이션 코드 외부의 하나 또는 여러 컴포넌트에서 이러한 보호를 제공한다.

9. 불충분한 전송 계층 보호

가. 위험

– 어플리케이션은 종종 민감한 네트워크 트래픽의 인증, 암호화, 그리고 비밀성과 무결성을 보호하는데 실패한다.

– 실패할 때에는 대체로 약한 알고리즘을 사용하거나, 만료 또는 유효하지 않은 인증서를 사용하거나 또는 그것을 올바로 사용하지 않을 때이다.

나. 예방법

– 모든 민감한 페이지는 SSL을 요구하라. 이 페이지에 대한 non-SSL 요청은 SSL페이지로 리다이렉트 되어야 한다.
– 모든 민감한 쿠키는 'secure' 플래그를 설정하라.
– 단지 강력한 알고리즘(FIPS 140-2 호환)만을 지원하는 SSL 공급업체를 구성하라.

10. 검증 되지 않은 리다이렉트와 포워드

가. 위험

– 웹 어플리케이션은 종종 사용자들을 다른 페이지로 리다이렉트 하거나 포워드 한다. 그러나, 목적 페이지를 결정하기 위해 신뢰되지 않는 데이터를 사용한다.
– 적절한 확인이 없다면, 공격자는 피해자를 피싱 사이트나 악의적인 사이트로 리다이렉트 할 수 있고, 포워드를 권한 없는 페이지의 접근을 위해 사용할 수 있다.

나. 예방법

– 단순히 리다이렉트와 포워드의 사용을 피해야 한다.
– 만약 사용한다면, 목적지를 계산하는 사용자 파라미터를 포함하지 마라.
– 목적 파라미터를 피할 수 없다면, 제공된 값이 유효한지, 그 사용자에게 허용된 것인지를 확실히 하라.

지금까지 OWASP에서 발표한 웹 어플리케이션 보안 위험 및 예방법에 대해서 간략하게 알아 보았다. 향후 각 위험 별로 자세한 내용을 통해 좀 더 상세한 내용을 전할 예정이다.

Ⅱ. 2분기 보안 동향

1. 악성코드 동향

악성코드 통계

2010년 2분기 악성코드 통계현황은 다음과 같다.

순위	등락	악성코드명	건수	비율
1	↑ 1	TextImage/Autorun	1,299,470	17.7 %
2	↓ 1	Win32/Induc	892,732	12.2 %
3	New	JS/Agent	641,316	8.8 %
4	New	Win-Trojan/Overtls.575488	466,906	6.4 %
5	↓ 2	Win32/Parite	386,228	5.3 %
6	↑ 2	Win32/Olala.worm.57344	337,590	4.6 %
7	↓ 3	Win32/Virut.B	316,322	4.3 %
8	↓ 2	Win32/Conficker.worm.Gen	297,022	4.1 %
9	New	JS/Redir	281,426	3.8 %
10	↑ 2	ALS/Bursted	269,169	3.7 %
11	↑ 3	JS/Exploit	258,476	3.5 %
12	↓ 1	TextImage/Sasan	248,015	3.4 %
13	↓ 6	Win32/Virut	242,750	3.3 %
14	New	JS/Downloader	232,934	3.2 %
15	↑ 3	Win-Trojan/Daonol.Gen	230,911	3.2 %
16	New	HTML/IFrame	220,648	3 %
17	↓ 4	TextImage/Viking	204,325	2.8 %
18	↓ 9	Win32/Palevo.worm.Gen	176,299	2.4 %
19	↓ 3	Win32/Traxg.worm.61440	171,275	2.3 %
20	New	Win32/Autorun.worm	147,478	2 %
			7,321,292	100 %

[표 4-1] 악성코드 감염보고 2 분기 Top 20

2010년 2분기 악성코드 감염 보고는 TextImage/Autorun이 1위를 차지하고 있으며, Win32/Induc과 JS/Agent가 각각 2위와 3위를 차지 하였다. 신규로 Top20에 진입한 악성코드는 총 6건이다.

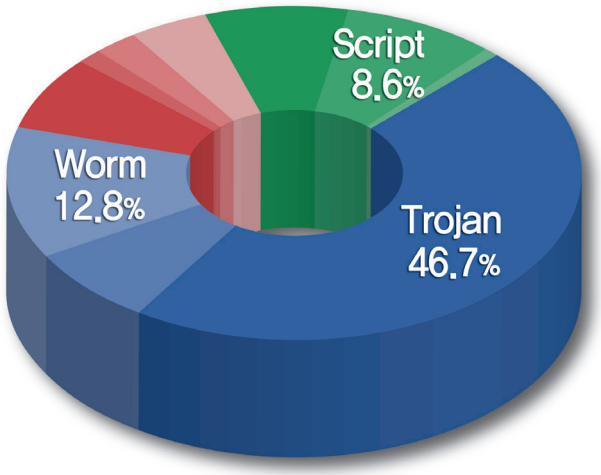
아래 표는 악성코드의 주요 동향을 파악하기 위하여, 악성코드별 변종을 종합한 악성코드 대표진단명 감염보고 Top200이다.

순위	등락	악성코드명	건수	비율
1	↑ 1	Win-Trojan/Agent	2,305,201	13.7 %
2	↓ 1	Win-Trojan/Onlinegamehack	2,228,361	13.2 %
3	–	Win-Trojan/Downloader	1,685,830	10 %
4	↑ 1	TextImage/Autorun	1,308,798	7.8 %
5	↑ 3	Win32/Autorun.worm	1,019,568	6.1 %
6	↑ 1	Win32/Virut	915,019	5.4 %
7	↓ 3	Win32/Induc	892,974	5.3 %
8	↓ 2	Win32/Conficker	851,594	5.1 %
9	New	JS/Agent	642,194	3.8 %
10	New	Win-Trojan/Overtls	623,083	3.7 %
11	New	Win-Trojan/Bho	585,767	3.5 %
12	New	Win-Trojan/Adload	482,104	2.9 %
13	↑ 2	Win32/Kido	477,945	2.8 %
14	↑ 2	Dropper/Onlinegamehack	471,956	2.8 %
15	New	Dropper/Malware	455,420	2.7 %
16	↑ 1	Win-Adware/Rogue	399,207	2.4 %
17	↓ 4	Win32/Parite	390,365	2.3 %
18	↓ 6	Win32/Palevo	367,858	2.2 %
19	↓ 1	Win-Trojan/Daonol	365,041	2.2 %
20	↓ 10	Win-Trojan/Daonol	357,581	2.1 %
			16,825,866	100%

[표 4-2] 악성코드 대표진단명 감염보고 2분기 Top 20

2010년 2분기 사용자 피해를 주도한 악성코드들의 대표진단명을 보면 Win-Trojan/Agent가 총 보고 건수 2,305,201건으로 전체의 13.7%를 차지하여 1위를 차지하였다. 그 뒤를 Win-Trojan/Onlinegamehack이 2,228,361건으로 13.2%, Win-Trojan/Downloader가 1,685,830건으로 10%를 차지하여 2위와 3위를 차지 하였다.

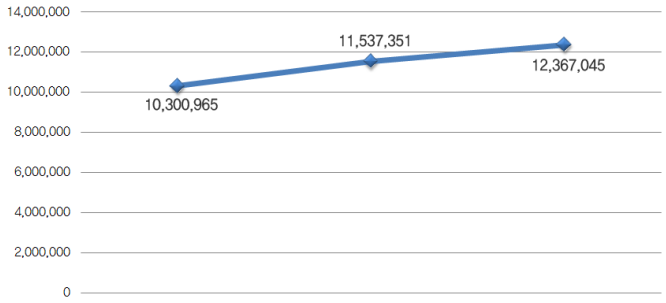
아래 차트는 2010년 2분기 동안 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.



[그림 4-1] 악성코드 유형별 2분기 감염보고 비율

AhnLab SiteGuard Pro & Security Center

악성코드 유형별로 감염보고건수 비율은 트로잔(TROJAN)류가 46.7%로 가장 많은 비율을 차지하고 있으며, 다음으로 웜(WORM)이 12.8%, 스크립트(SCRIPT)가 8.6%의 비율을 각각 차지하고 있다.



[그림 4-2] 악성코드 2분기 감염보고 건수

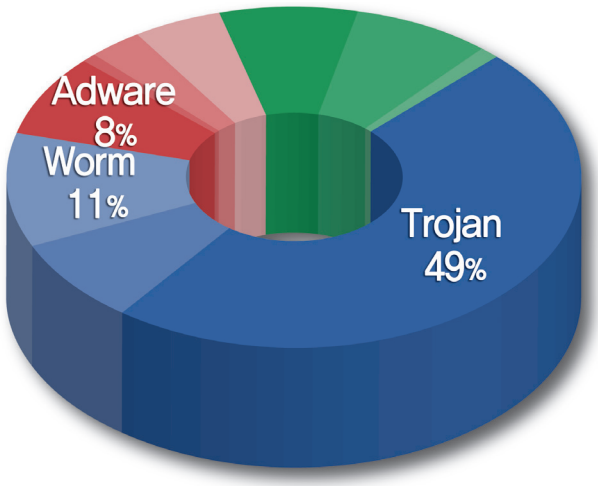
2010년 2분기의 악성코드 2분기 감염보고 건수는 34,205,361건으로 2010년 1분기의 악성코드 2분기 감염 보고건수 31,486,648건에 비해 2,718,713건이 증가하였다.

아래 표는 2010년 2분기에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top200이다.

순위	악성코드명	건수	비율
1	Win-Trojan/Overtls.575488	466,906	7 %
2	Win-Adware/Rogue.PrivacyScan.167312	97,038	1.5 %
3	Win-Trojan/Inject.1588224	93,837	1.4 %
4	Win-Trojan/Securisk	87,356	1.3 %
5	Win-Trojan/Bho.353792	79,324	1.2 %
6	Win-Trojan/Clicker.323584	66,778	1 %
7	Win-Trojan/Adload.1133568	63,958	1 %
8	Win-Trojan/Agent.106496.QU	62,784	0.9 %
9	Win-Trojan/Agent.240222	53,890	0.8 %
10	Win-Trojan/Unovt.630784	52,444	0.8 %
11	Win-Dropper/Rogue.TrueScan.1247048	50,563	0.8 %
12	Win-Trojan/Agent.107688	49,741	0.7 %
13	Win-Trojan/Downloader.1134080	48,718	0.7 %
14	Win-Trojan/Downloader.209920.F	47,602	0.7 %
15	Win-Trojan/Adware.309248	47,309	0.7 %
16	Win-Trojan/Adload.630784.B	45,803	0.7 %
17	Win-Trojan/Bho.923136	45,247	0.7 %
18	Win-Trojan/Adload.1146880	44,830	0.7 %
19	Win-Trojan/Jascript	44,580	0.7 %
20	Win-Trojan/Banker.385008	43,944	0.7 %
		1,592,652	23.9 %

[표 4-3] 신종 악성코드 감염보고 Top 20

2010년 2분기의 신종 악성코드 감염 보고의 Top 20은 Win-Trojan/Overtls.575488가 466,906건으로 전체 7%를 차지하여 1위를 차지 하였으며, Win-Adware/Rogue.PrivacyScan.167312가 97,038건 2위를 차지 하였다.



[그림 4-3] 신종 악성코드 분기 유형별 분포

2010년 2분기의 신종 악성코드 유형별 분포는 트로잔이 49%로 1위를 차지하였다. 그 뒤를 이어 웜이 11%, 애드웨어(ADWARE)가 8%를 각각 차지하였다.

악성코드 이슈

2010년 2분기를 결산해보면 2분기에 있었던 사회적인 이슈들을 이용한 공격들이 주로 발견되었다. 남아공 월드컵과 관련 악성코드가 발견되거나, 스마트폰의 확산에 따른 Windows Mobile 계열의 악성코드, 트위터 열풍에 따른 트위터 봇넷 등이 주요 이슈로 볼 수 있다.

남아공 월드컵을 이용한 악의적인 PDF 문서

4월에는 Adobe Acrobat Reader의 잘못된 TIFF 이미지 파싱 관련 취약점을 이용한 악성코드 유포 사례가 국외에서 발견, 보고 되었다. 여기에 사용된 주제는 2010 남아공 월드컵 관련 내용으로 위장 되어 있었다. 악의적인 PDF 는 기존에 알려진 CVE-2010-0188 취약점을 가지고 있었다. 메일로 전송 되었던 해당 악성코드는 취약한 Adobe Acrobat Reader에서 읽혀진 경우 TIFF 파일에 대한 잘못된 파싱과 이를 통하여 쉘코드가 실행 되며, 이후 특정 폴더에 악성코드 파일을 생성하고 정보의 유출을 시도 할 것으로 보인다.

Windows Mobile 계열에서 동작하는 악성코드 국내발견 주의보

4월에는 국내에서 윈도우 모바일 계열 (5.0, 6.1, 6.5버전) 에서 동작하는 스마트폰 악성코드인 WinCE/TredDial.a (일명 3D Antiterrorist)가 발견, 보고 되었다. 해당 악성코드는 게임 어플리케이션에 포함 되어 발견 되었다. 해당 악성코드의 실행 후 증상은 임의로 특정 전화번호의 국제전화를 무단으로 발신 하도록 되어 있었다. 이 경우 사용자에게 원치 않는 통신비가 과금 되는 상황이 발생 된다. 이용된 게임명은 '3D Antiterrorist' 이며 다음과 같은 'antiterrorist3d.cab' 파일명을 가지고 있다. 실행 시에는 Program Files 폴더에 reg.exe가 설치되며, 시스템 폴더에 smart32.exe라는 이름으로 해당 파일을 복사한다. 또한 해외 Premium-rate number에 국제전화를 시도하여 국제전화 과금을 발생시킨다.

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

문서파일에 포함된 악성코드 주의

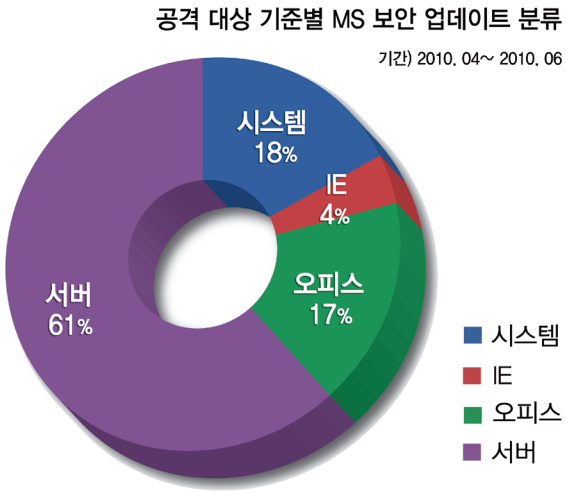
5월에는 메일을 통해 유포되는 악성코드 중 DOC 혹은 RTF 등의 확장자의 문서를 이용한 악성코드 유포 사례가 확인되었다. 문서파일에 첨부된 파일을 실행하면 문서 내부에 특정 아이콘이 나타나며 클릭을 유도하게 된다. 만일, 클릭을 하게 되면 경고 창이 나타나며 [확인] 버튼을 누를 경우 문서 내부에 포함된 악성코드가 실행이 된다. 최근 악성코드 유포 기법이 점점 다양해지며 발전되고 있어 이러한 발신인이 불분명한 메일을 통해 첨부되는 문서나 기타 첨부파일은 되도록이면 실행하지 않는 것을 권장한다.

2. 시큐리티 동향

시큐리티 통계

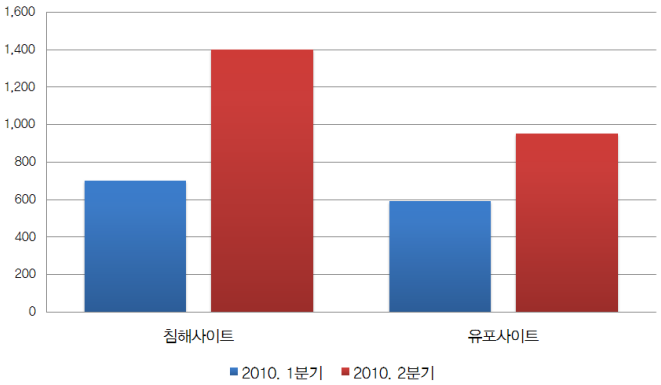
2010년도 2분기 마이크로소프트 보안 업데이트 현황

2010년 2분기에 마이크로소프트사는 지난 해 상반기보다 다소 증가된 총 40건의 보안 업데이트를 발표하였다.



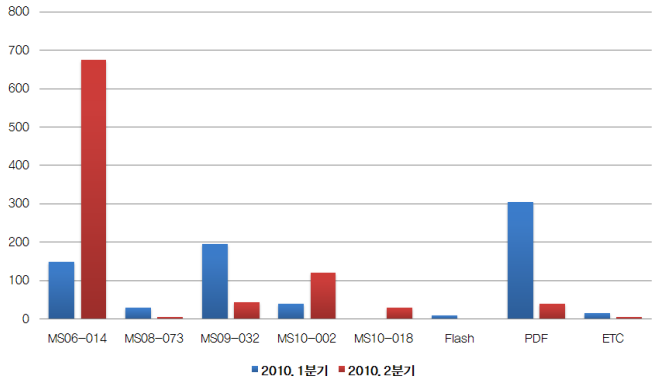
[그림 5-1] 2010년 2분기 보안업데이트 현황

악성코드 침해 웹사이트 현황



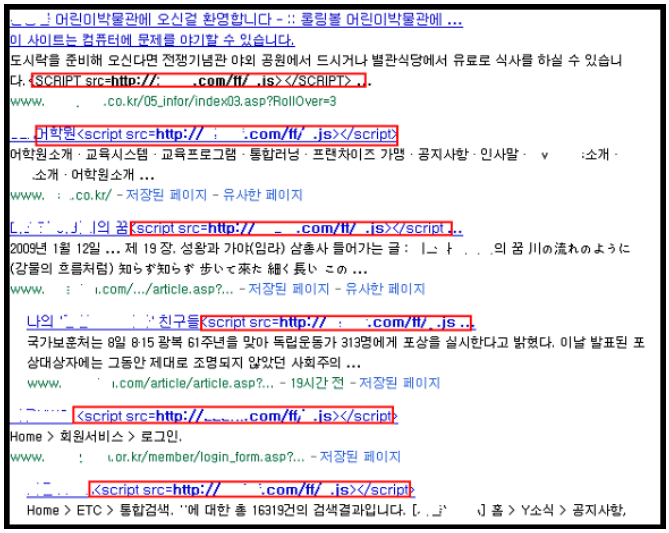
[그림 5-2] 악성코드 배포를 위해 침해된 사이트 / 배포지 수

[그림 5-2]는 분기별 악성코드 침해 및 유포 사이트 현황을 나타낸 그래프로, 올해 2 분기는 1분기에 비해 약 2배 이상 악성코드 유포행위가 탐지되었다. 올해 2분기 침해사고 사이트를 통해서 유포되었던 악성코드를 살펴보면 1분기와 유사한 형태로 Daonol이 가장 많았고 OnlineGame-Hack, AutoRun, Virus등이 그 뒤를 따랐다.



[그림 5-3] 악성코드 배포를 위해 사용된 취약점

[그림 5-3]은 분기별 침해사고가 발생한 웹사이트들에서 악성코드를 유포하기 위해서 사용했던 취약점들에 대한 그래프로, 개별 취약점 별로 살펴보면 2분기에도 여전히 MS06-014취약점을 사용한 공격이 많았고 MS09-032취약점을 사용한 악성코드 유포는 1분기에 비해 급감했지만 그 대신 MS10-002취약점을 사용한 악성코드 유포는 1분기에 비해 약 2배정도 증가했다. 그리고 최근에 발견된 MS10-018을 사용한 악성코드 유포는 Mass SQL Injection공격에 이용되면서 국내 많은 사이트들에 이용되기도 했다.



[그림 5-4] MS10-018취약점이 사용된 침해 사이트

시큐리티 이슈

Adobe Reader & Flash Player 제로데이 취약점

지난 2분기에도 Adobe사의 대표 제품군인 Adobe Acrobat Reader관련 새로운 제로데이(0-day) 취약점(일명, PDF 취약점)이 발표되었다. 이러한 PDF 취약점 공격은 입사이력서나 유명 보안업체의 업데이트 권고와 같은 다양한 컨텐츠를 수반하는 위장된 메일 형태나 웹을 통해 사용자를 위협하고 있다. 특히, 새롭게 보고된 Adobe Acrobat and Reader authplay.dll 코드 실행(CVE-2010-1297,APSA10-01) 취약점은 기존의 직접적인 Adobe Acrobat Reader 상에서 발생되는 취약점과는 달리, 어플리케이션 내부에 탑재되어 있는 외부 처리엔진 상의 오류로 인하여 연쇄적 취약점이 발생한 사례라고 볼 수 있다. 이와 유사한 사례는 작년과 올해 1분기에도 존재하였다. 해당 취약점은 Adobe Flash Player 10.0.45.2 이하에 존재하는 flash 파싱엔진(authplay.dll)으로 인하여 발생되었고, 최근 이처럼 복잡한 어플리케이션간의 상호호환성은 취약점의 연쇄적 발생이라는 또 다른 보안위협을 유발하기도 한다는 점에 주목해야 할 것이다.

매력적인 공격매체로 자리잡은 트위터

최근 가장 유명한 소셜 네트워크 서비스(SNS)인 트위터는 공격자들에게도 아주 매력 있는 공격매체가 되고 있다. 작년에 이미 트위터 서비스를 공격자의 명령 서버(C&C)로 이용하는 사례가 보고된 바 있고, 상반기에는 보다 손쉽게 명령서버를 구축하여 활용할 수 있는 "TwitterNet Builder"라는 자동화툴이 발견되었다. 악용 가능한 트위터 계정정보를 입력하고 클릭 한번으로 새로운 좀비프로그램(Bot)이 생산되고, 이를 통해 DDoS 공격을 비롯한 다양한 공격을 수행할 수 있다. 또한, 2분기에는 단축 URL을 악용한 스팸메일 유포나 간접적으로 트위터 사용자 암호 리셋 메일 및 팔로잉(Following) 요청메일을 위장한 악성코드 배포 사례들도 보고되었다. 이처럼 트위터의 사용계층이 두터워지고, 그 활용범위도 개인 및 기업의 마케팅, 홍보 등으로 확장되면서 트위터를 활용한 공격방식도 보다 다양하고 활발해질 것으로 예상된다.

국내카드사 이용대금 명세서로 위장한 악성코드 등장

우리는 과거 종이 우편시대에서 전자메일을 통해 각종 명세서를 전달받아 처리하는 시대를 살고 있다. 하지만, 최근 스팸발송 기능을 갖는 악성코드의 활발한 활동으로, 메일함 속의 모든 메일들을 온전하게 믿을 수 없는 게 현실이다. 2분기에는 국내 유명 카드사의 이용대금명세서를 위장한 스팸메일이 발견되었고, 이를 통해 배포되는 악성코드에서 유명 국내 포털사이트로의 트래픽이 발견되어 큰 관심이 되기도 하였다. 공격에 이용된 스팸메일은 보안 카드명세서에서 정상적인 보안 프로그램을 설치하는 기능을 이용하여 악성코드를 대신 설치하도록 제작되어 있다. 실제 설치되는 악성코드는 공격자의 명령서버(C&C)로 부터 XML형태의 공격명령을 전달받고, 이 명령 속에서 한글로 된 카드 이용 대금 명세서 메일본체도 발견되었다. 이러한 서버/클라이언트 구조의 공격은 공격자가 자유롭게 공격명령을 변경할 수 있기 때문에 언제든지 좀비 프로그램으로 변신하여 또 다른 DDoS 공격을 수행할 수 있는 위험성을 갖고 있다.

윈도우 도움말 센터 제로데이 취약점

지난 1분기에 이어 2분기에도 새로운 제로데이 취약점들이 보고되었다. 가장 최근에 발표된 제로데이 취약점인 윈도우 도움말 센터(Windows Help and Support Center) 취약점(CVE-2010-1885)은 윈도우 도움말 센터(helpctr.exe)를 통해hcp 프로토콜을 처리하는 과정에서 발생하는 디자인 상의 오류와 관련 html 페이지상의 크로스사이트 스크립트(XSS) 취약점이 결합되어 발생한다. 실제 공격에서는 사용자에게 프로토콜 사용에 대한 접근을 알리지 않도록 ASX HtmlView를 이용한 우회방법이 사용되고 XSS취약점을 통해 공격자가 원하는 코드를 배치파일로 만들어 실행하는 형태가 많이 보고되고 있다. 아직까지 해당 제로데이 취약점을 해결하기 위한 제품벤더(MS)로부터의 정식패치가 배포되지 않았기 때문에 임시적으로 MS사가 제공하는 Hotfix를 사용하는 것도 방법이 될 수 있다.

3. 웹 보안 동향

웹 보안 통계

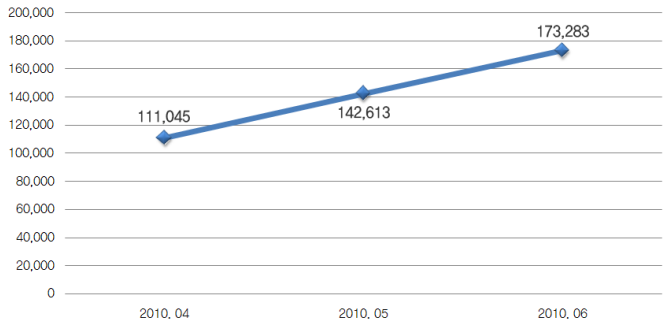
웹사이트 보안 요약

구분	건수
악성코드 발견 건수	426,941
악성코드 유형	2,753
악성코드가 발견된 도메인	2,930
악성코드 발견된 URL	12,586

[표 6-1] 웹 사이트 보안 요약

2010년 2분기 악성코드 발견 건수는 426,941건이고, 악성코드 유형은 2,753건이며, 악성코드가 발견된 도메인은 2,930건이며, 악성코드 발견된 URL은 12,586건이다. 본 자료는 안철수연구소의 웹 보안 제품인 SiteGuard의 2010년 2분기 자료를 바탕으로 산출한 통계정보이다.

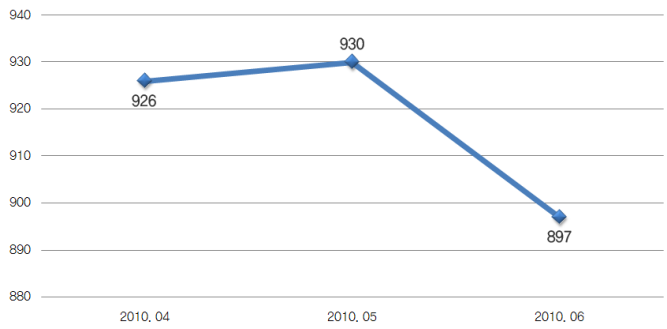
2분기 악성코드 발견 건수



[그림 6-1] 2분기 악성코드 발견 건수

2010년 2분기 악성코드 발견 건수는 전분기의 798,502건에 비해 53% 수준인 426,941건이다.

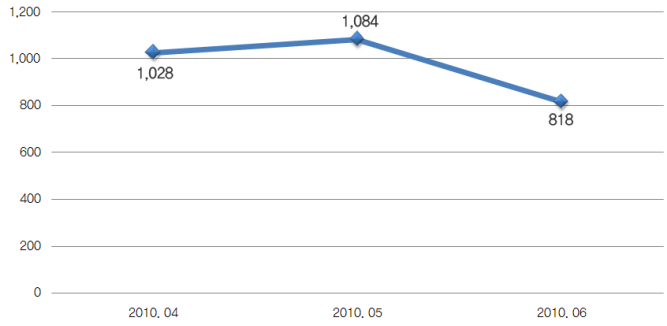
2분기 악성코드 유형



[그림 6-2] 2분기 악성코드 유형

2010년 2분기 악성코드 유형은 전분기의 1,783건에 비해 154% 수준인 2,753건이다.

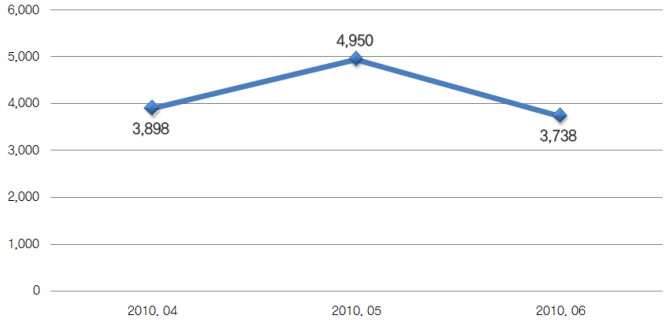
2분기 악성코드가 발견된 도메인



[그림 6-3] 2분기 악성코드가 발견된 도메인

2010년 2분기 악성코드가 발견된 도메인은 전분기의 2,917건과 비슷한 수준인 2,930건이다.

2분기 악성코드가 발견된 URL



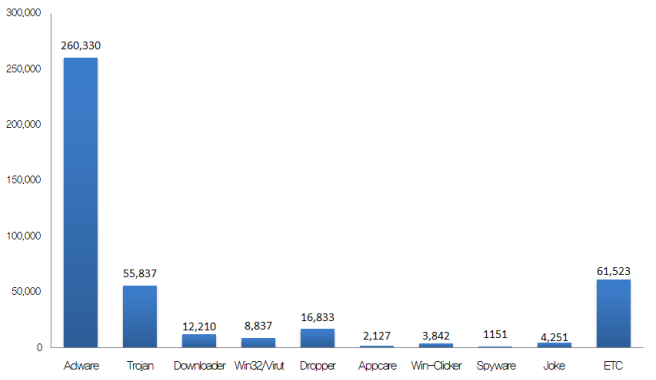
[그림 6-4] 2분기 악성코드가 발견된 URL

2010년 2분기 악성코드가 발견된 URL은 전분기의 12,214건에 비해 103% 수준인 12,586건이다.

악성코드 유형별 배포 수

유형	건수	비율
ADWARE	260,330	61 %
TROJAN	55,837	13.1 %
DROPPER	16,833	3.9 %
DOWNLOADER	12,210	2.9 %
Win32/VIRUT	8,837	2.1 %
JOKE	4,251	1 %
WIN-CLICKER	3,842	0.9 %
APPCARE	2,127	0.5 %
SPYWARE	1,151	0.3 %
ETC	61,523	14.4 %
	426,941	100 %

[표 6-2] 악성코드 유형별 배포 수



[그림 6-5] 악성코드 유형별 배포 수

악성코드 유형별 배포 수에서 애드웨어(ADWARE)류가 260,330건 전체의 61%로 1위를 차지하였으며, 트로잔(TROJAN)류가 55,837건으로 전체의 13.1%로 2위를 차지하였다.

악성코드 배포 Top 10

순위	등락	악성코드명	건수	비율
1	–	Win-Adware/Shortcut.InlivePlayerActiveX.234	63,563	24.9 %
2	New	Win-Adware/Woowa.28672	26,514	10.4 %
3	New	Win-Adware/Juneip.645632	24,747	9.7 %
4	New	Win-Adware/Seveten.371968	24,713	9.7 %
5	↑ 1	Win32/Induc	22,918	9 %
6	New	Win-Adware/Woowa.61440	20,485	8 %
7	New	Win-Adware/Woowa.24576	19,726	7.7 %
8	New	Win-Adware/Juneip.644096	19,465	7.6 %
9	↓ 1	Win-Adware/Shortcut.IconJoy.642048	19,325	7.6 %
10	New	HTML/IFrame	14,237	5.6 %
			255,693	100 %

[표 6-3] 악성코드 배포 Top 10

악성코드 배포 Top10에서 Win-Adware/Shortcut.InlivePlayerActiveX.234이 63,563건으로 1위를 Win-Adware/Woowa.28672이 26,514건 2위를 기록하였다.

웹 보안 이슈

2010년 2분기 웹 보안 이슈를 결산해 보면, 구글 그룹스와 스팸메일이 결합된 악성코드가 나타났으며, 사회공학적 방법을 이용한 facebook 패스워드 리셋과 관련한 스팸메일과 맥아피 오진 사고를 위장한 허위백신 유포 등의 이슈가 있었다.

Face Book 패스워드 리셋 한다는 스팸 메일

4월에 발생한 이슈로 인터넷상에서 인기를 끌고 있는 facebook의 계정과 비밀번호 150만개를 2.5센트라는 가격으로 판매한다는 내용의 사건에 대해 facebook에서 강력한 대응 방침을 밝히고 난 후, facebook에서 고객의 안전을 위해 facebook 비밀번호를 변경한다는 허위사실을 유포하는 스팸메일에 악성코드를 첨부하여 발송하는 사건이 있었다. 스팸 메일에 첨부된 파일은Microsoft Office Word 파일의 아이콘을 사용하여 메일 수신자가 악성코드를 자연스럽게 실행하도록 위장하고 있다. 해당 파일은 현재 V3제품 군에서 Win-Trojan/Bredolab.48640.B 진단명으로 진단 및 치료가 가능하다.

맥아피 오진 사고 소식으로 위장해 구글 검색 결과로 허위 백신 유포

해외 시각으로 4월 21일 미국 보안 업체인 맥아피(McAfee)에서 정상 윈도우 (Win dows) 시스템 파일인 svchost.exe를 W32/Wecorl.a 악성코드로 잘못 진단 하는 오진(False Positive) 사고가 발생하였다. 이러한 맥아피의 오진 사고를 이용하여 구글(Google) 검색 엔진에서 검색 순위를 상위로 조정하여 악성코드를 유포하는 웹 사이트로 컴퓨터 사용자들을 유도하는 블랙 햇(BlackHat) SEO(Search Engine Optimization) 기법을 통해 허위 백신의 유포를 시도한 사례가 발견되었다. 이 번에 구글 검색 엔진을 통해 유포된 허위 백신은 이번 맥아피의 오진 사고와 관련된 단어들을 검색하게 될 경우에 악성코드를 유포하는 웹 사이트를 검색 첫 번째 페이지로 위치하여 컴퓨터 사용자들의 방문을 유도하였다.

구글 그룹스(Google Groups)와 스팸메일이 결합된 악성코드

5월에 발생한 이슈로 상호 정보를 교환하고 싶은 사람들간에 가상의 그룹을 만들고 게시판을 통해 공지사항, 파일 등을 손쉽게 그룹원들에게 전파할 수 있는 구글 클라우드 컴퓨팅 서비스 중 하나인 구글 그룹스(Goolge Groups)를 통해 스패머 (Spammer)들이 스팸 메일에 악성코드를 첨부하여 전파하는데 활용하는 사례가 발견되었다. 이 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 설치 파일을 가장한 실행파일 아이콘이 나타나며, 해당 파일을 실행할 경우 악성코드가 설치된다.

AhnLab V3 Zip

Ⅲ. 해외 보안 동향

1. 중국 2분기 악성코드 동향

중국 지앙민 6월 보안 위협 동향 분석 발표

7월 7일 중국 보안 업체인 지앙민(JiangMin)에서는 중국에서 6월 한달 동안 발생한 다양한 보안 위협들을 정리하여 중국 CNET “江民发布6月病毒与网络安全信息报告”을 통해 발표 하였다.

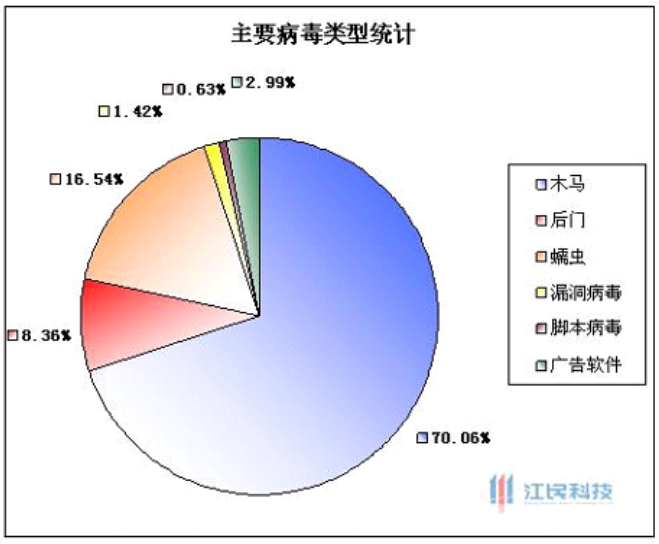
이 번 지앙민을 통해 발표된 중국의 6월 보안 위협 동향의 전체적인 특징을 요약하면 다음과 같이 정리 할 수 있다.

1) 5월 대비 전체 악성코드 수치의 4% 감소
2) 트로이목마가 전체 악성코드의 70% 차지
3) 마이크로소프트(Microsoft)의 인터넷 익스플로러(Internet Explorer) 취약점인 MS10-018 악용 증가

지앙민에서 발표한 6월 한 달 동안 중국에서 발견한 악성코드의 수치는 아래 이미지와 같다.

[그림7-1] 지앙민 집계 2010년 1월에서 6월까지 악성코드 감염 통계

지앙민에서는 4월과 5월에는 증가세를 보였지만 6월에 이르러서는 5월 대비 5% 정도 감소한 수치를 보였다고 하나 2010년 2분기인 4월에서 6월까지의 전체적인 악성코드의 발견 수치가 1분기와 비교하여서는 완만한 상승선을 그리고 있는 것을 알 수가 있다. 그리고 전체 악성코드 분포도에 있어서 트로이목마가 약 70%, 웜이 16% 그리고 백도어가 약 8% 순서로 차지하고 있는 것을 아래 이미지를 통해 잘 알 수가 있다.



[그림 7-2] 지앙민 집계 2010년 6월 악성코드 형태별 분류

이렇게 트로이목마가 전체의 70%를 차지한다는 점을 통해 중국 역시 한국을 비롯한 전 세계적으로 비슷한 추세를 그리고 있는 것을 잘 알 수 있다. 그리고 6월 한 달 동안 가장 많이 악용된 취약점으로는 3월 9일 알려진 마이크로소프트의 인터넷 익스플로러(Internet Explorer) 취약점인 MS10-018의 악용을 꼽고 있다. 해당 취약점은 4월 8일 중국 보안 업체인 라이징(Rising)에서도 역시 급격한 악용이 발생하고 있음을 중국 언론을 통해 알린 바가 있다.

[그림7-3] 라이징 집계 MS10-018 취약점을 악용한 공격 통계

당시 라이징에서는 위와 같은 이미지를 통해 공격이 최초 알려진 3월에서부터 같이 4월 7일까지 총 1839 만 회가 발생하였으며 4월 7일 하루 동안에만 중국 내부에서 310 만 건이 발견 한 것으로 밝혔다.

이 외에 지앙민에서는 6월 한 달 동안 높은 감염율을 보였던 악성코드 TOP 5로 다음을 선정하고 있다.

Checker/Autorun
Worm/Kido.aeb
Checker/HideFolder

VBS/Fineboy.a

Exploit.CVE-2010-0806

TOP 5에 선정된 악성코드를 보면 취약점을 악용하는 형태의 악성코드인 Kido(Win32/Conficker.worm)과 MS10-018(JS/CVE-2010-0806) 포함되어 있는 것으로 미루어 중국 내에서 아직 윈도우 보안 패치가 적용되지 않은 시스템이 다수 존재하는 것을 알 수 있다. 그리고 외장형 장치 드라이버인 USB를 통해 전파되는 Checker/Autorun가 포함된 점 역시 한국과 유사하게 Autorun 웜의 감염율이 비교적 높은 것을 잘 알 수 있다.

2. 일본 2분기 악성코드 동향

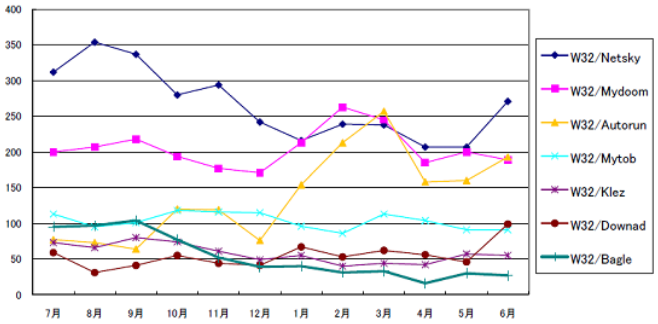
2010년 2분기에 일본에서 발생한 주요 보안 이슈는 악성 스크립트가 삽입된 웹 사이트로 인한 사용자 피해가 증가하고 있는 것과 컨피커 웜(Win32/ Conficker.worm)에 의한 감염 피해가 지속적으로 발생하고 있는 것을 들 수 있다. 가짜백신(Win-Trojan/FakeAV)과 같은 악성코드에 의한 피해 또한 올 초부터 일본에서 지속적인 피해를 유발하고 있는 것으로 보인다. 웹사이트의 불법적인 변조로 인한 악성코드 유포는 이미 전 세계적으로 발생하고 있는 문제이고 일본에서도 작년부터 이러한 유형의 공격이 많이 발생하고 있는 상황이다. 아래의 [표8-1]은 일본 트랜드마이크로에서 발표한 2010년 상반기 악성코드 피해현황을 집계한 것이다.

순위	악성코드명	악성코드유형	피해건수	과거순위
1 위	MAL_OTORUN	기타	315 건	1 위
2 위	WORM_DOWNAD	웜	266 건	2 위
3 위	JS_ONLOAD	자바스크립트	124 건	신규
4 위	TROJ_FAKEAV	트로이목마	112 건	권외
5 위	MAL_HIFRM	스크립트	96 건	8 위
6 위	BKDR_AGENT	백도어	91 건	3 위
7 위	JS_GUMBLAR	자바스크립트	85 건	신규
8 위	JS_IFRAME	자바스크립트	70 건	7 위
9 위	WORM_AUTORUN	웜	68 건	권외
10 위	TROJ_BREDOLAB	트로이목마	62 건	신규

[표 8-1] 2010년 상반기 악성코드 피해 현황 〈자료출처 : 일본 트렌드마이크로사[1]〉

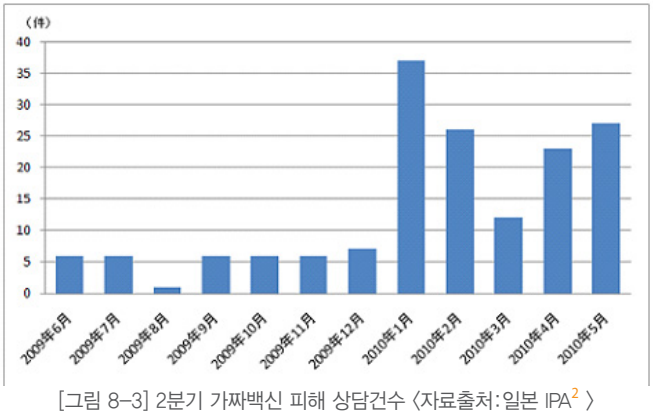
표의 내용에서 주목해야 할 점은 온로드(JS_ONLOAD)나 검블러(JS_GUMBLAR)와 같은 스크립트 형태의 악성코드에 의한 피해가 다수를 차지하고 있는 것이다. 이 악성코드들은 대부분 보안이 취약한 홈페이지에 불법으로 삽입되거나 공격자가 게시판 등에 악의적인 목적으로 업로드를 하는 방식으로 전파된다. 이러한 악성 스크립트들은 사용자의 PC에 실행되더라도 악성코드 자체로 인한 피해는 미약하지만 트로이목마와 같은 또 다른 악성코드를 감염시키는 것을 목적으로 하는 경우가 대부분이고 이로 인한 2차 감염의 가능성이 높으므로 주의가 필요하다.

오토런 악성코드와 컨피커 웜(WORM_DOWNAD) 또한 여전히 많은 피해를 유발하고 있는 것을 볼 수 있다.



[그림8-1] 2분기 악성코드 감염 피해 현황 〈자료출처:일본 IPA〉

위 그림은 일본 IPA에서 발표하는 보안 리포트의 내용 중 2분기 악성코드 감염 피해 현황을 집계한 자료이다. 컨피커 웜의 감염 피해가 이전부터 지속적으로 유포되고 있는 전통적인 이메일 웜에 견줄 수 있을 정도로 많이 유포되고 있는 것을 볼 수 있다. 최근 발견되는 악성코드 중 OS의 보안 취약점을 원격에서 공격하여 자신을 복제하는 웜의 기능을 하는 악성코드가 많지 않음을 고려 했을 때 컨피커 웜의 감염 피해가 이와 같이 지속적으로 발생하고 있는 것은 이 악성코드의 강력한 전파력을 짐작할 수 있게 해준다. 가짜 백신으로 인한 피해는 올해 초부터 일본에서 크게 이슈가 되고 있는 상황이다. 아래의 [그림8-2]은 일본 IPA에서 발표한 월간 보고서의 내용 중 가짜 백신 감염 피해 상담현황을 집계한 자료로 올 초부터 가짜 백신으로 인한 피해가 급격하게 늘어난 것을 알 수 있다.



[그림 8-3] 2분기 가짜백신 피해 상담건수 〈자료출처:일본 IPA[2] 〉

이러한 가짜백신은 스팸메일이나 웹 사이트 등 매우 다양한 경로를 통해 유포되고 여러 형태의 변형이 제작되고 있는 상황이므로 PC 사용자가 감염 되기 전 백신 프로그램과 같은 보안 소프트웨어에서 이러한 악성코드를 신속하게 차단하는 것은 현실적인 어려움이 있다. 따라서 PC 사용자는 주기적인 OS의 보안패치뿐 아니라 스팸메일의 첨부파일을 실행해 보는 것과 같이 사용자의 실수로 인한 감염을 예방하기 위해 각별한 주의가 필요하다.

1.http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20100702082212.html

2.http://www.ipa.go.jp/security/txt/2010/06outline.html

3. 세계 2분기 악성코드 동향

2010년 2분기는 1분기와 동일하게 허위 백신 프로그램의 극성, 타겟 공격, Adobe Acrobat Reader에 대한 제로데이(0-day) 취약점 공격, 이슈 검색어를 이용한 악성코드 배포 증가 특징을 가지고 있다.

비트디펜더(BitDefender)에 따르면[1] 쿠키(Cookie)이외에 오토런 웜(Autorun worm)이 생성하는 autorun.inf 와 PDF 파일 취약점을 이용한 악성코드, 컨피커웜 (Conficker worm)이 높은 순위를 차지하고 있다. 이셋(Eset)은 글로벌 위협 리포트(Global threat report)[2]를 통해 현재 널리 퍼져있는 악성코드는 컨피커이며 오토런 웜에 의해 만들어지는 autorun.inf 파일, 온라인게임 계정 탈취 트로이목마가 상위권에 올려져 있다. 포티넷(Fortinet) 통계에 따르면[3] 6월은 실제 취약점 공격코드를 포함한 주소로 유도하는 리다이텍트(Redirect) 스크립트가 1위를 차지하고 있으며 상위권에 새스피스(Sasfis) 봇넷[4] 이 차지하고 있다. 5월에는 허위보안 프로그램의 일종인 페이크얼럿(Fakealert), 오토런 웜 등이 차지하고 있다.[5] 카스퍼스키연구소 5월 통계에 따르면[6] 컨피커 웜(Conficker worm)이 여전히 1위, 3위, 4위를 달리고 있다. 또한 샐리티 바이러스(Sality virus)와 바이럿 바이러스(Virut virus)도 여전히 높은 순위를 차지하고 있다.

악성코드 배포 방식은 여전히 해킹된 웹사이트로 웹브라우저 취약점을 이용해 전파된다. 하지만, 검색 엔진 최적화(SEO, Search Engine Optimization)를 이용한 방식도 널리 이용되고 있다. 악성코드 배포자들은 이슈 되는 검색어를 파악해 악성코드를 포함한 웹사이트를 검색 결과 상위에 노출시켜 사용자가 검색 결과를 클릭하여 악성코드 유포 사이트로 연결되게 한다.

이외 여러 백신 통계를 통해 USB 플래쉬 드라이브(USB flash drive)를 통한 악성코드 전파 방식도 높은 것을 알 수 있다. 이외 현재는 널리 이용되지 않지만 정상 소프트웨어에 악의적인 코드를 몰래 삽입하는 방식도 눈길을 끌었다. 오픈소스 IRC 서버인 언리얼IRCd(UnrealIRCd) 3.2.8.1에 백도어가 포함되어 있는 사실이 확인되었다.[7] 2009년 11월부터 백도어 기능이 포함되어 있었던 것으로 확인되었다.

스마트폰과 OSX 악성코드도 조금씩 등장하고 있다. 한가지 흥미로운 점은 스마트폰 악성코드의경우 중국 게임 및 codecpack에 포함되었는데 정상적인 프로그램 제작 과정에 해커가 침투해 악성코드를 심어 둔 것으로 보인다. 6월 18일 발표된 OSX 10.6.4에는 OSX/Pinhead.B(HellRTS)에 대한 보호 기능이 추가되었다.[8] 아직 스마트폰과 OSX 악성코드가 큰 위협은 아니지만 계속 관심을 가져야 할 것이다.

1.http://www.bitdefender.com/site/VirusInfo/realTimeReporting/90/wks

2.http://www.eset.com/resources/threat-trends/Global_Threat_Trends_June_2010.pdf

3.http://www.fortiguard.com/report/roundup_june_2010.html

4.http://www.fortiguard.com/analysis/sasfisanalysis.html

5.http://www.fortiguard.com/report/roundup_may_2010.html

6.http://www.securelist.com/en/analysis/204792121/Monthly_Malware_Statistics_May_2010

7.http://www.securelist.com/en/blog/2205/Unreal_Backdoored_IRC_Server

8.http://www.appleinsider.com/articles/10/06/18/apple_quietly_includes_malware_prevention_update_in_mac_os_x_10_6_4.html

발행월 : 2010년 7월
ASEC REPORT 집필진

편 집 장 선임 연구원 허 종 오

집 필 진 선임 연구원 김 소 헌
선임 연구원 심 선 영
선임 연구원 장 영 준
선임 연구원 정 진 성
선임 연구원 차 민 석
선임 연구원 허 종 오
주임 연구원 박 시 준
주임 연구원 안 창 용
연구원 박 영 준

감 수 상 무 조 시 행

참여연구원 ASEC 연구원
SiteGuard 연구원