ASEC REPORT

안철수연구소에서 발행하는 월간 보안 보고서

Vol. 11

안철수연구소

목 차

이달의 보안 동향

Ⅰ. 이달의 보안 동향

1. 악성코드 동향

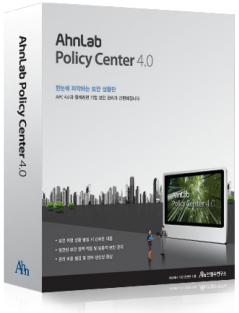
악성코드 통계

2010년 11월 악성코드 통계현황은 다음과 같다.

순위	등락	악성코드명	건수	비율
1	↑ 1	TextImage/Autorun	697,869	24.3 %
2	↓ 1	Win32/Parite	411,965	14.3 %
3	↑ 1	Win32/Induc	234,981	8.2 %
4	↑ 7	Win32/Olala.worm.57344	141,105	4.9 %
5	New	JS/Shellcode	132,117	4.6 %
6	New	Win-Trojan/Winsoft9.Gen	121,588	4.2 %
7	↑ 6	Win32/Conficker.worm.Gen	112,466	3.9 %
8	New	HTML/Cve-2010-3962	102,690	3.6 %
9	New	Win-Trojan/Overtls7.Gen	94,803	3.3 %
10	New	HTML/Agent	89,438	3.1 %
11	New	Win32/Virut	82,627	2.9 %
12	↑ 3	Win32/Palevo9.worm.Gen	82,502	2.9 %
13	↑ 1	JS/Exploit	74,468	2.6 %
14	New	Win-Trojan/Winsoft4.Gen	73,082	2.5 %
15	↑ 3	Win-Trojan/Securisk	72,542	2.5 %
16	↓ 4	Win-Trojan/Spack3.Gen	71,067	2.5 %
17	New	VBS/Autorun	70,720	2.5 %
18	↑ 2	Win32/Virut.B	70,163	2.4 %
19	New	Win32/Palevo1.worm.Gen	68,793	2.4 %
20	New	TextImage/Viking	68,695	2.4 %
			2,873,681	100 %

[표 1-1] 악성코드 감염보고 Top 20

2010년 11월의 악성코드 감염 보고는 TextImage/Autorun이 1위를 차지하고 있으며, Win32/Parite와 Win32/Induc가 각각 2위와 3위를 차지하였다. 신규로 Top20에 진입한 악성코드는 총 10건이다.



AhnLab Policy Center 4.0

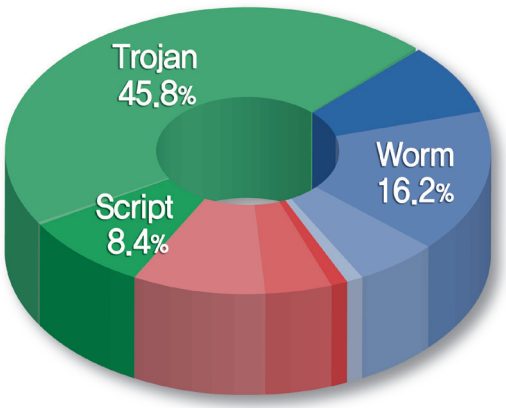
아래 표는 악성코드의 주요 동향을 파악하기 위하여 악성코드별 변종을 종합한 악성코드 대표진단명 감염보고 Top200이다.

Ranking	↑ ↓	Malicious Code	Reports	Percentage
1	–	Win-Trojan/Agent	924744	14.6%
2	↑ 1	Win-Trojan/Downloader	907157	14.3%
3	↓ 1	Win-Trojan/Onlinegamehack	671354	10.6%
4	↑ 8	Win-Trojan/Overtls	404641	6.4%
5	–	TextImage/Autorun	361356	5.7%
6	↑ 12	Win-Adware/Webside	358963	5.7%
7	↓ 1	Win32/Autorun.worm	325932	5.2%
8	↓ 1	Win32/Virut	281284	4.4%
9	–	Win32/Conficker	252658	4%
10	↑ 1	Win32/Induc	244157	3.9%
11	New	JS/EXPLOIT	239345	3.8%
12	↑ 1	Dropper/Malware	213810	3.4%
13	↑ 3	JS/Redir	166639	2.6%
14	↑ 1	Dropper/OnlineGameHack	166071	2.6%
15	↓ 7	Win-Trojan/Bho	165150	2.6%
16	↓ 2	Win32/Kido	140151	2.2%
17	↓ 13	Win-Trojan/Adload	139830	2.2%
18	↓ 8	Win-Adware/Rogue	125652	2%
19	↑ 1	Win-Trojan/Inject	117544	1.9%
20	↓ 1	Win32/Olala	116399	1.8%
			6322837	100%

[표 1-2] 악성코드 대표진단명 감염보고 Top 20

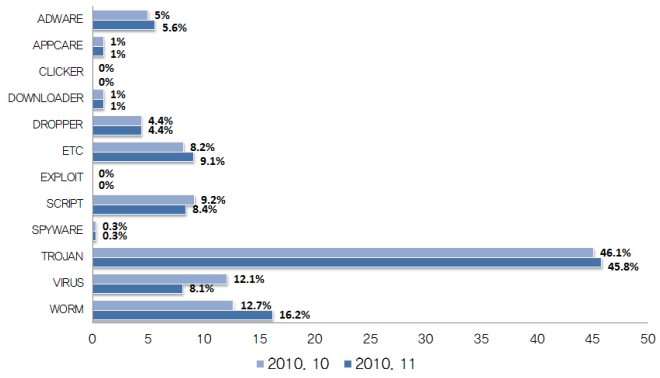
2010년 11월의 감염보고 건수는 Win-Trojan/Onlinegamehack 이 총 915,675건으로 Top20중 13.9%의 비율로 1위를 차지하고 있으며 Win-Trojan/Agent 가 810,341건으로 2위, TextImage/Autorun 이 700,200건으로 3위를 차지하였다.

아래 차트는 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.



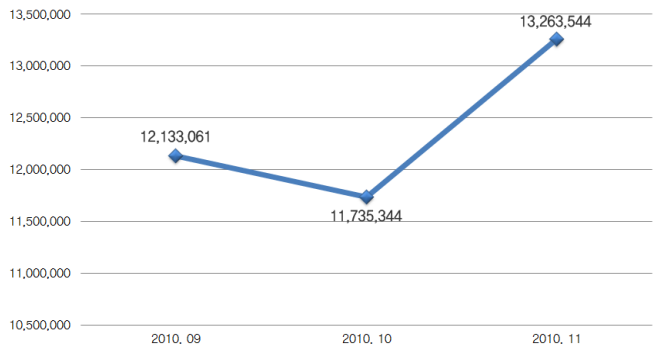
[그림 1-1] 악성코드 유형별 감염보고 비율

2010년 11 월의 악성코드 유형별 감염보고건수 비율은 트로잔(TROJAN)류가 45.8%로 가장 많은 비율을 차지하고, 웜(WORM)가 16.2%, 스크립트(SCRIPT)가 8.4%의 비율을 각각 차지하고 있다.



[그림 1-2] 악성코드 유형별 감염보고 전월 비교

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



[그림 1-3] 악성코드 월별 감염보고 건수

11월의 악성코드 월별 감염보고 건수는 13,263,544건으로 10월의 11,735,344건에 비해 1,528,200건이 증가하였다.

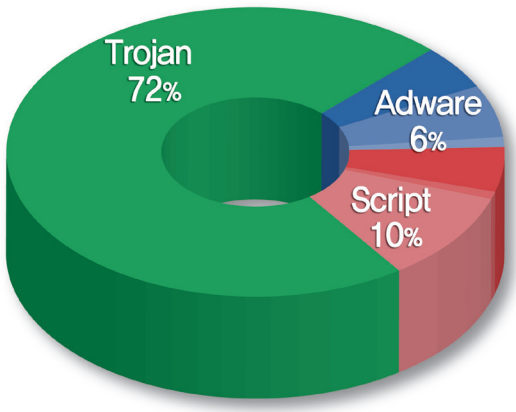
AhnLab V3 MSS

아래 표는 11월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top200이다.

순위	악성코드명	건수	비율
1	HTML/Cve-2010-3962	102,690	18.1 %
2	JS/Exploitcve20100806	57,155	10.1 %
3	Win-Trojan/Agent.749568.CE	48,812	8.6 %
4	Win-Trojan/Downloader.106496.HY	44,532	7.9 %
5	Win-Adware/KorAdware.397312	40,353	7.1 %
6	Win-Trojan/Adload.95232.AD	35,003	6.2 %
7	Win-Trojan/Bho.595456	32,715	5.8 %
8	Win-Trojan/Agent.135680.CY	21,024	3.7 %
9	Win-Adware/Srvreg.110592	20,839	3.7 %
10	Win-Trojan/Onlinegamehack.267264.D	16,737	3 %
11	Win-Trojan/Agent.170058.B	16,681	2.9 %
12	Win-Trojan/Spack.40960.B	16,283	2.9 %
13	Win-Trojan/Patched.CI	15,225	2.7 %
14	Win-Trojan/Downloader.270336.X	15,203	2.7 %
15	JS/Exploit-ie	15,145	2.7 %
16	Win-Trojan/Adload.797696.D	14,542	2.6 %
17	Script/Bursted	14,113	2.5 %
18	Win-Trojan/Onlinegamehack.57344.BQ	13,700	2.4 %
19	Win-Trojan/Downloader.198656.F	13,066	2.3 %
20	Dropper/Malware.188614	12,556	2.2 %
		566,374	100 %

[표 1-3] 신종 악성코드 감염보고 Top 20

11월의 신종 악성코드 감염 보고의 Top 20은 HTML/Cve-2010-3962가 102,690건으로 전체 18.1%를 차지하여 1위를 차지하였으며, JS/Exploitcve20100806가 57,155건 2위를 차지하였다.



[그림 1-4] 신종 악성코드 유형별 분포

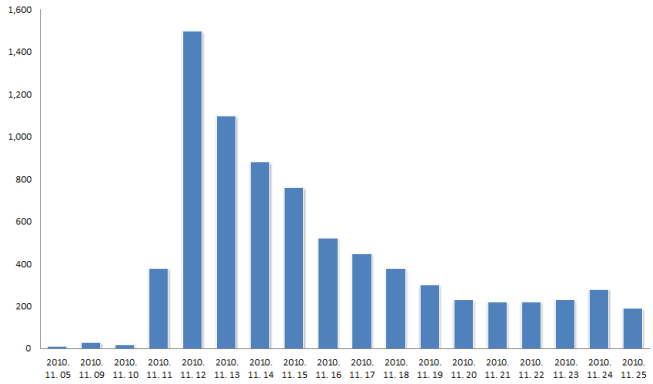
11월의 신종 악성코드 유형별 분포는 트로잔이 72%로 1위를 차지하였다. 그 뒤를 이어 스크립트가 10%, 애드웨어가 6%를 각각 차지하였다.

악성코드 이슈

한국 내 CVE-2010-3962 취약점 악용 악성코드 증가

이번 달 많이 발생했던 제로데이(Zero-Day)취약점들 중 11월4일 보고된 인터넷 익스플로러 제로데이 취약점은 발견 1주일이 지난 후 국내에서도 발견, 보고건수가 증가하였다. 이후 점차 그 수가 줄어들고 있지만 진단을 회피하는 변형의 등장도 예상할 수 있으므로 안심해서는 안 된다. 또

한 보고서를 작성하는 현재까지도 공식 보안패치가 발표되지 않았기 때문에 주의가 요구된다.



[그림1-5] JS/CVE-2010-3962 증가율

현재 JS/CVE-2010-3962 취약점을 내포한 시스템은 온라인 게임 정보를 탈취하는 악성코드들을 다운로드하게 됨으로써, 추가적인 감염 피해가 지속적으로 발견되고 있다. 이러한 웹 브라우저 취약점을 악용하는 악성코드 감염 수치가 증가하고 있다는 것은 한국 내 컴퓨터 사용자들이 방문하는 다수의 웹 사이트들이 SQL 인젝션(Injection)과 같은 공격으로 인해 악성코드 유포에 악용되는 것으로 볼 수 있다. 공식 보안패치가 발표되지 않았기 때문에 사용자들은 안티 바이러스와 같은 보안제품을 반드시 설치 사용해야 하며 MS 가 공개한 다음의 링크에서 관련 정보를 이용하여 대응책을 마련해야 한다.

http://support.microsoft.com/kb/2458511

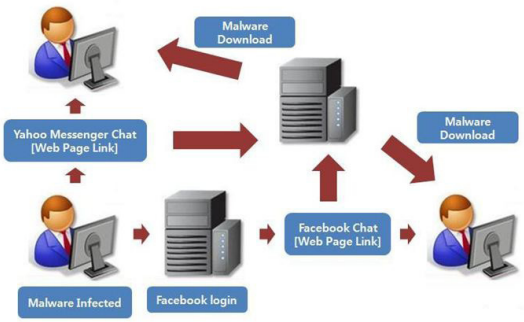
국제행사를 사칭하여 전파된 악성코드들

국제행사가 많았던 11월은 국외에서 G20 및 노벨 평화상 시상식 관련 악성코드가 보고되기도 하였다. 또한 광저우 아시안게임을 사칭한 'The 16th Asian Games[공백].exe' 란 파일명을 갖는 악성코드도 보고되었다. 해당 악성코드의 출처는 현재 명확하지 않지만, 실행 후 사용자를 속이기 위하여 손상된 The 16th Asian Games.pdf 파일을 생성한다. 이후 2곳의 특정 웹사이트로 접속을 시도하는데 감염된 컴퓨터의 이름과 운영체제 정보 IP 주소를 훔쳐낸다. G20 회의 관련 악성코드는 'G20 Issues paper' 이라는 제목의 메일로 유포 되었다. 역시 사용자를 속이기 위하여 *.DOC 문서를 보여준 후 특정 웹사이트로 접속을 시도한다. 이처럼 국제적인 행사와 사건 등은 악성코드 제작자들로부터 악성코드를 유포하는 수단으로 곧잘 이용되었다. 보통 이러한 악성코드는 메일 등으로 전달 되므로 이미 알고 있는 것처럼 메일 내 링크나 첨부파일을 클릭하거나 실행하지 않는 것이 최선의 예방책이라 볼 수 있다. 만약 의심스러운 첨부파일 등에 대한 결과를 알고 싶다면 안철수연구소 홈페이지에 있는 바이러스 신고센터를 이용하여 의심스러운 파일을 신고하면 된다.

(http://www.ahnlab.com/kr/site/securitycenter/virus/virus.do)

페이스북(facebook) 채팅 메시지로 유포되는 악성코드

대표적인 SNS인 페이스북의 채팅 메시지를 통하여 유포되는 악성코드가 확인 되었다. 일반적으로는 쪽지기능을 통하여 악성코드가 포함된 링크를 전달하는 방식이었으나 이번에 알려진 관련 악성코드 (Win-Trojan/Seint.61440.AA, Win-Trojan/Ircbrute.61440.C, Win-Trojan/Seint.69632.V)는 채팅 메시지로 악의적인 링크를 보내어 현재 온라인 사용자의 감염을 유도하는 방식이다. 유포구조의 도식은 다음과 같다.

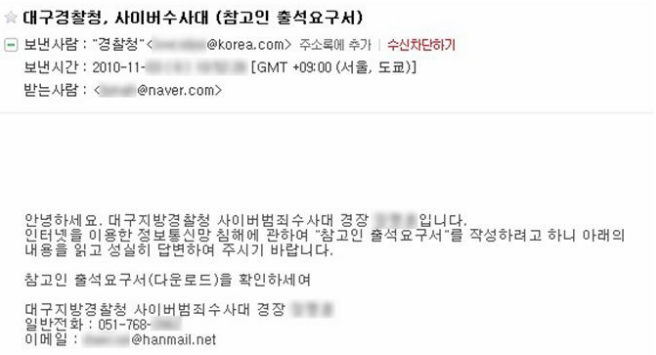


[그림1-6] 페이스 채팅 메시지 전파 관련 악성코드 유포구조 도식

이는 과거 메신저 웜의 전파 방식과 매우 유사한 사례이다. 쪽지의 경우는 실시간으로 확인이 되지 않으며 링크가 고정적인 경우 기존의 알려진 링크라면 쉽게 차단이 된다. 그러나 채팅 메시지로 링크를 전달받는 경우에는 사용자가 큰 의심없이 클릭하게 되고, 이로인해 감염이 확산되기 때문에 2차 피해가 커질 것으로 예상된다. 국내 사용자가 200만 명을 돌파하고 전세계적으로 5억 명 이상이 사용하는 페이스북 또한 관련 악성코드가 기승을 부리고 있는 상황이다. 따라서 SNS 서비스를 이용할 때 주의를 기울이며, 신뢰할 수 없는 게시글과 링크는 클릭 하지 않는 것이 바람직하다.

경찰청 사칭 악성 스팸메일

신뢰할 수 있는 발신인을 사칭한 사회 공학(Social Engineering) 기법을 이용하여 스팸메일을 발송 및 악성코드를 유포하는 사례가 꾸준히 발생되고 있다. 11월 초, "대구경찰청, 사이버수사대 (참고인 출석요구서)" 라는 제목의 악성 스팸메일로 인한 피해가 확인되었다. 아래의 그림은 실제 고객으로부터 접수된 스팸메일의 원문이다.


대구경찰청, 사이버수사대 (참고인 출석요구서)

보낸사람 : "경찰청"<[redacted]@korea.com> 주소록에 추가 | 수신차단하기

보낸시간 : 2010-11-[redacted] [GMT +09:00 (서울, 도쿄)]

받는사람 : <[redacted]@naver.com>

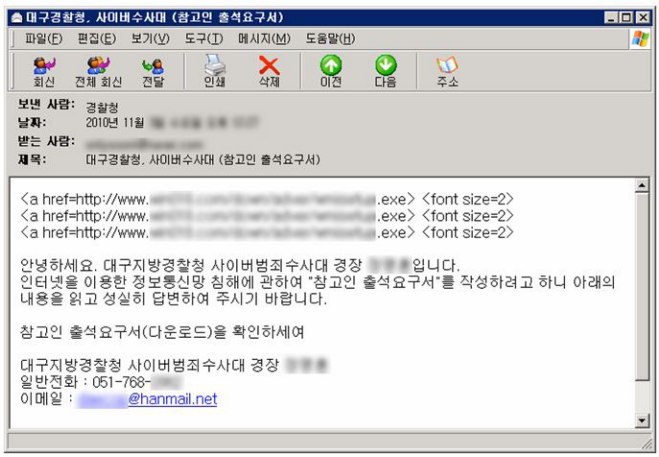
안녕하세요. 대구지방경찰청 사이버범죄수사대 경장 [redacted]입니다.
인터넷을 이용한 정보통신망 침해에 관하여 "참고인 출석요구서"를 작성하려고 하니 아래의 내용을 읽고 성실히 답변하여 주시기 바랍니다.

참고인 출석요구서(다운로드)을 확인하세여

대구지방경찰청 사이버범죄수사대 경장 [redacted]
일반전화 : 051-768-[redacted]
이메일 : [redacted]@hanmail.net

[그림1-7] 실제 고객으로부터 접수된 스팸메일 원문

메일의 원문에는 대구지방경찰청 소속 특정인을 사칭하여 '참고인 출석요구서' 파일로 위장한 악성코드를 링크 형태로 제공하여, 파일 다운로드 및 실행을 유도한다. 이 파일을 실행할 경우 악성코드(Win-Trojan/Sparats.593498)에 감염된다. 아래 그림은 메일의 원문에 포함된 태그를 텍스트 형태로 확인한 내용이며, 특정 실행파일을 다운로드 하도록 링크가 설정된 것을 확인할 수 있다.

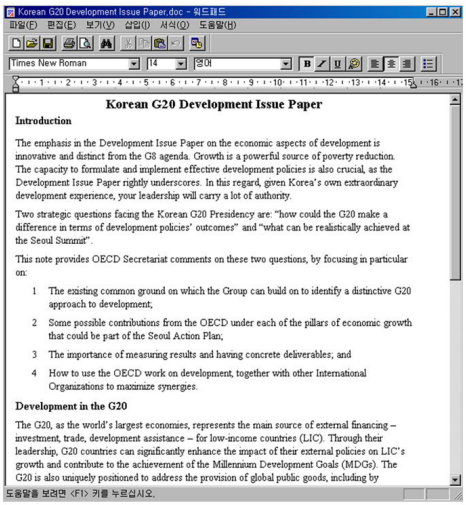


[그림1-8] 악성코드 다운로드 링크를 포함한 원문

이와 같이 어느 정도 신뢰가 가능한 발신자의 메일이라 하더라도, 연결된 링크나 첨부된 파일이 존재할 경우 다시 한번 확인하여 열람하는 사용자의 주의가 필요하다.

G20 정상회의 관련 자료 위장 스팸메일

국내에서는 발견된 바 없으나, 해외에서 G20 정상회의 관련 자료로 위장한 "G20 Issues Paper"라는 제목의 스팸메일이 확인되었다. 메일의 본문에 작성된 링크를 클릭하도록 유도한 후, 압축 파일을 다운로드하게 하는 방식이다. 이 압축파일 내부에는 워드(doc) 문서로 위장된 악성코드가 존재한다. 이 악성코드가 워드 문서라고 생각한 사용자에 의해 실행되면, 문서 파일을 실행한 것처럼 위장하는 doc 문서가 실행된다. 아래의 그림은 실행된 doc 문서이다.



[그림1-9] 문서 파일을 실행한 것처럼 위장하는 doc 문서

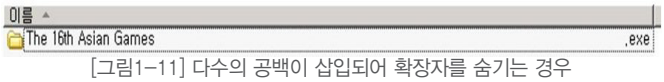
doc 문서가 실행됨과 동시에 특정 폴더에 악성코드가 생성, 시스템 시작 시 실행될 수 있도록 레지스트리 값을 설정하고 특정 URL을 통해 접속을 시도한다.

아시안 게임 관련 문서로 위장한 악성코드

제 16회 광저우 아시안 게임의 개막을 앞둔 시점에 관련 문서로 위장한 악성코드가 국내에서 발견되었다. 해당 악성코드의 경우 아래 그림과 같이 "The 16th Asian Games[공백].exe"의 이름으로, 파일명의 확장자 이전까지 다수의 공백을 삽입하여 실행파일임을 숨기게 된다. 또한 폴더 아이콘으로 위장하여 사용자로 하여금 실행을 유도한다.

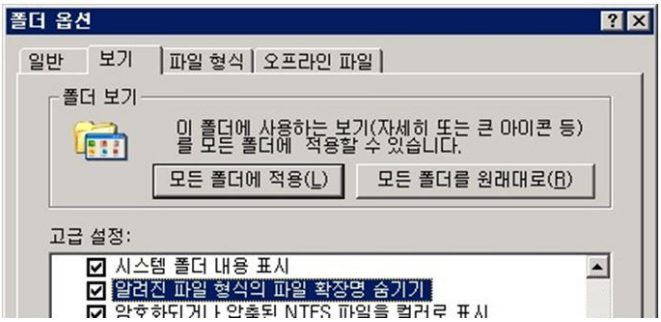
[그림1-10] 폴더 아이콘으로 위장한 악성코드

이 경우, 아래와 같이 필드의 간격 조정 및 설정 변경으로 확장자에 대한 확인이 가능하나, 일반적인 파일 보기 설정으로는 보이지 않을 수 있다.



[그림1-11] 다수의 공백이 삽입되어 확장자를 숨기는 경우

시스템 설치 시 기본으로 설정되어 있는 "알려진 파일 형식의 파일 확장명 숨기기"(Windows XP기준)를 설정할 경우에는 알려진 확장자(exe, dll 등)에 대해서는 확장자명이 나타나지 않는다.



[그림1-12] 시스템 설치 시 기본 설정

따라서 위와 같이 폴더옵션이 설정된 경우에는 아래 그림과 같이 확장자가 확인되지 않으며 사용자는 해당 파일을 폴더로 인식할 수 있다.

[그림1-13] 기본설정으로 되어있어 확장자 확인이 힘든 경우

이와 같은 방법으로 사용자가 해당 악성코드를 실행하게 되면, 특정 폴더에 PDF 파일이 생성된다. 그리고 PDF 파일이 생성된 폴더를 화면에 출

력하게 된다. 하지만 생성된 PDF 파일은 손상된 파일로, 사용자로부터 악성코드의 실행을 숨기기 위한 위장술에 지나지 않는다.

[그림1-14] 특정 폴더에 생성된 PDF 파일

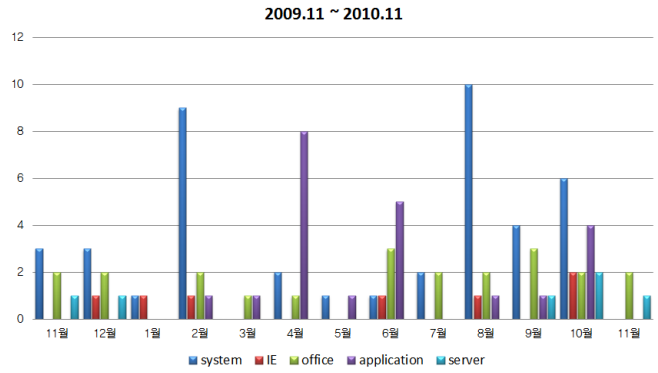
이와 같이 사회적인 관심을 끄는 국제적인 행사는 악성코드 유포자들에게는 기회가 될 수 있으며, 그 관심만큼 피해는 커질 수 있다. 때문에 사용자의 주의가 더욱 필요하다고 하겠다. 만일 이러한 의심파일이 발견되거나 실수로 실행하여 악성코드의 감염이 의심되는 경우, 안철수연구소 바이러스 신고센터를 통해 악성코드 감염여부 확인 및 조치를 안내받을 수 있다.

2. 시큐리티 동향

시큐리티 통계

11월 마이크로소프트 보안 업데이트 현황

마이크로소프트사로부터 발표된 이번 달 보안 업데이트는 3건이다.



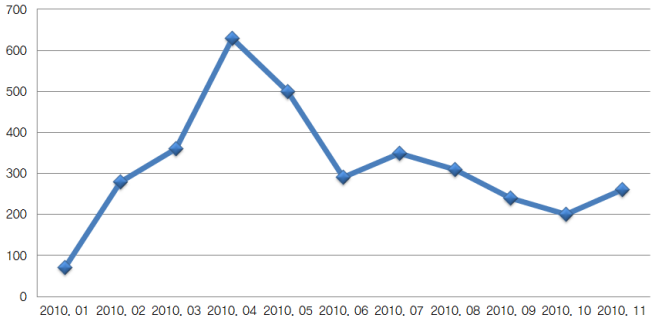
[그림 2-1] 공격 대상 기준 별 MS 보안 업데이트

위험도	취약점	PoC
긴급	MS10-087 마이크로소프트 오피스 취약점	무
중요	MS10-088 마이크로소프트 오피스 취약점	무
중요	MS10-089 Forefront UAG(Unified Access Gateway)의 취약점	무

[표 2-1] 2010년 11월 주요 MS 보안 업데이트

이번 달에는 단 3건의 패치가 발표되었다. 2건은 마이크로소프트 오피스 취약점에 관한 것이고, 나머지 한 건은 Forefront 취약점이다. 이번에 공개된 취약점과 관련해서는 공개적으로 공격코드가 세부적으로 알려진 것은 없으나, 패치관련 정보가 공개된 만큼 공개될 가능성도 있다. 발표된 패치에는 원격코드 실행취약점이 존재하는 만큼 해당 제품을 사용 중이라면 빠른 패치를 권고하는 바이다.

악성코드 침해 웹 사이트 현황



[그림 2-2] 공격 대상 기준 별 MS 보안 업데이트

위 통계는 월별 악성코드 침해 사이트 현황을 나타낸 그래프로, 전월에 비해 다소 증가하였다. 9월 초 ARP Spoofing 악성코드가 등장하면서 초기에는 다소 많은 고객들로부터 피해사례가 보고되었으나 이후 안철수연구소를 비롯한 백신업체들의 엔진반영과 국가기관의 악성코드 유포 URL차단 등의 적극적인 공동대응으로 인해서 고객들의 피해가 감소했다. 그러나 악성코드 제작자들이 지속적으로 신규 유포 지를 통해서 변종을 유포하고 있는 상황이며 이로 인해 10, 11월 양달간 다수의 변종이 발견되었는데 고정적이었던 기존의 파일명이 무작위로 변경되는 특징이 있었다. 기존에 악성코드를 유포하기 위해서 사용했던 MS10-002와 MS10-018 뿐만 아니라, 11월의 경우 보안 업데이트가 릴리즈되지 않은 IE 0-Day 취약점(CVE-2010-3962)[1]을 사용한 사례도 발견되어 사용자의 주의가 더욱 요구된다.

시큐리티 이슈

인터넷 익스플로러 제로데이(0-day) 취약점 지속 발견

인터넷 익스플로러 브라우저를 대상으로 한 취약점은 꾸준히 보고되어 왔으며, 이를 이용한 공격도 적지 않은 편이다. 이번 달에도 IE 와 관련한 제로데이 취약점이 보고되었는데, IE 6,7 그리고 8 버전 실행가능하며 CSS(Cascading Style Sheets)와 연관된 취약점이다. 이 취약점은 다음과 같은 코드가 포함되어 있는 문서를 IE 브라우저를 통해 호출하면 메모리 오류가 발생하는 것이다. 이때 EIP (Entry Instruction Point)는 사용자가 제어하는 것이 불가능하며, IE가 사용하는 mshtml 라이브러리 버전에 의존된다. 그러므로 사용하는 IE 버전에 따라 공격코드는 달라지며, 힙 스프레이(Heap Spray)를 넓게 수행할수록 성공확률은 높아지나 대신 속도는 느려지게 된다.

```
<html>
<table style=position:absolute;clip:rect(0)>
</html>
```

1.CVE-2010-3962 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3962

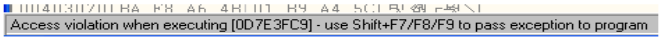
"clip" 이라는 속성은 특정영역을 드러냈다, 감췄다 하는 쓰임으로 이용되며, 자체 마스크 효과이다. 이외 사각형 이미지 영역에 가시성을 위해 사용된다. 일반적으로 사용되는 clip의 사용 형태는 아래와 같다.

```
img
{
position:absolute;
clip:rect(0px,60px,200px,0px);
}
```

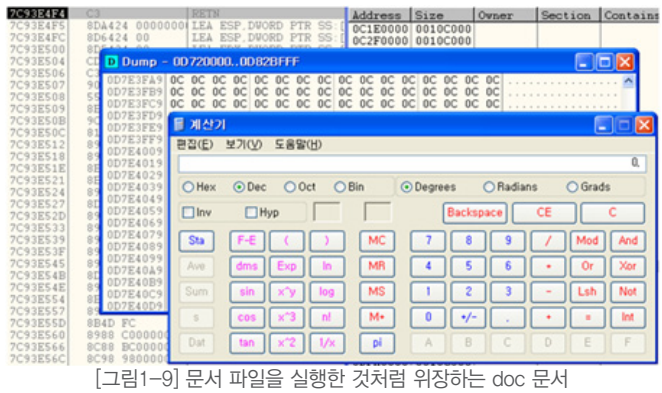
이번 취약점을 이용하여 위의 IMG와 테이블에 각각 스타일을 주고 실행하면 아래와 같이 EAX의 레지스트리 값이 다른 것을 알 수 있다.

IMG	TABLE
EAX 7E3A3398 mshtml.7E3A3398	EAX 7E3A33F1 mshtml.7E3A33F1
ECX 019B5804	ECX 019B7BC0
EDX 02000000	EDX 3FFFFFFF
EBX 0012D934	EBX 0012D6A0
ESP 0012D8AC	ESP 0012D658
EBP 0012D8B8	EBP 0012D664
ESI 00000000	ESI 00000000
EDI 019B5804	EDI 019B7BC0
EIP 7E411A8A mshtml.7E411A8A	EIP 7E411A8A mshtml.7E411A8A

이 지점에서 EAX+30이 IMG인 경우 DS:[7E3A33C8]=7E3FC90D (mshtml.7E3FC90D) 로 정상 셋팅되어 실행되지만, TABLE은 DS:[7E3A3421]=0D7E3FC9로 셋팅되어 종료된다.



만약 여기에서 0D7E3FC9에 NOP+SHELLCODE 가 들어가 있다면, 원하는 코드가 실행될 수 있다.



[그림1-9] 문서 파일을 실행한 것처럼 위장하는 doc 문서

인터넷 트래픽의 15%가 중국으로 흘렀다?

올 초, 정확히는 4월 18일 인터넷 트래픽 양의 15% 가까이가 18 분 동안 중국으로 우회 되었다는 기사가 보도됐다. 이 사실은 11월17일 미 국회에서 미국-중국의 양국관계에 관한 경제, 보안을 검토 하는 연례보고서에서 그 내용이 알려졌다. 18분 동안 중국으로 리다이렉션된 트래픽은 미국 정부, 국방부 및 군사 관련 사이트 및 델, 야후, 마이크로소프트, IBM과 같은 상업 사이트까지 많은 사이트를 포함하고 있다.

[그림2-4] ABCNEWS의 웹 페이지 화면

인터넷에서는 해당 사이트를 찾아갈 때 라우팅이라는 경로를 통해 최적의 경로를 따라 사이트를 찾아 들어간다. 정상적인 경우라면 중국을 거치지 않고 들어가야 하는데, 어떤 이유에서 해당 사이트를 찾아 들어가기까지 중국의 차이나 텔레콤을 거쳐서 정보가 흘러갔다는 것이다. 그렇다면 중국에서는 트래픽을 충분히 감시할 수 있는 상황이 되었을 것이다. 암호화되지 않은 트래픽이라면 이메일, 메신저와 같은 내용들이 감청당했을 수 있다. 이렇게 중국을 거쳐서 트래픽이 흘렀어도 사용자가 느끼기에는 큰 차이가 없었기 때문에 인지가 늦었던 것 같다. 현재 이와 같은 상황이 발생된 이유에 대해 세부적인 사항은 많이 알려져 있지 않다. 일단 사실로 밝혀진 한가지는 2010년4월18일 인터넷 트래픽의 15%가 18분 동안 중국의 차이나 텔레콤으로 흘렀다는 것이다. 무슨 일이 일어났을지는 모르지만, 정보 수집형태로 이용된다면 아주 무서운 일이 아닐 수 없다. 물론, 국내에서도 이와 같은 일이 충분히 일어날 수 있다. 만약 악성코드가 감염되어 특정한 곳을 거쳐서 트래픽이 흐르도록 조정된다면, 정보는 중간에서 감청될 수 있다. 사이버전에 효과적으로 이용될 수 있는 방법 중의 하나가 될 것이다.

3. 웹 보안 동향

웹 보안 통계

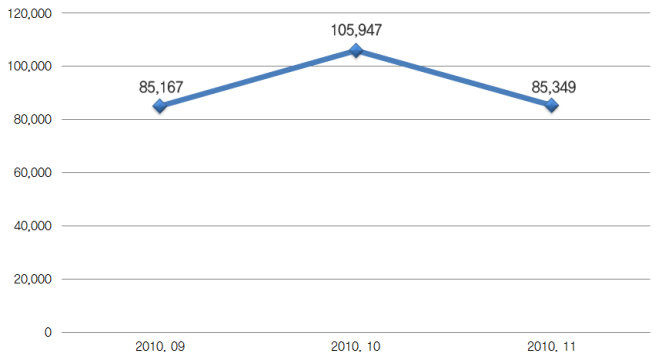
웹 사이트 보안 요약

구분	건수
악성코드 발견 건수	85,349
악성코드 유형	923
악성코드가 발견된 도메인	821
악성코드 발견된 URL	3,202

[표 3-1] 웹 사이트 보안 요약

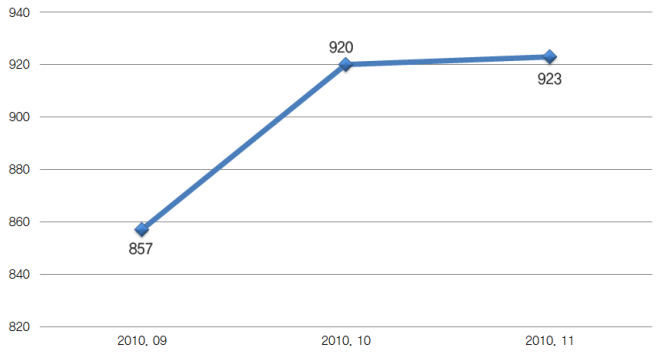
악성코드 발견 건수는 85,349건이고, 악성코드 유형은 923건이며, 악성코드가 발견된 도메인은 821건, 악성코드 발견된 URL은 3,202 건이다. 2010년 11월은 2010년 10월보다 악성코드 발견 건수, 악성코드 발견된 URL 은 다소 감소하였으나, 악성코드 유형, 악성코드가 발견된 도메인은 증가하였다.

월별 악성코드 발견 건수



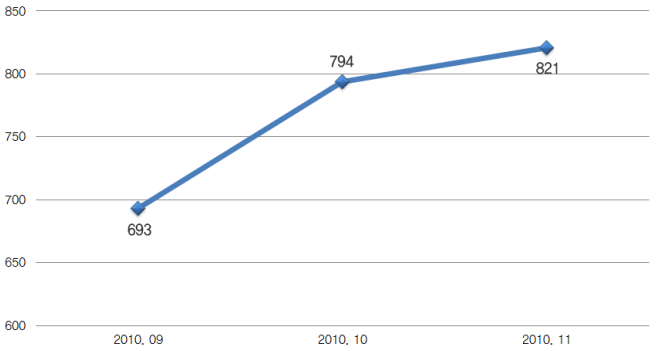
[그림 3-1] 월별 악성코드 발견 건수

월별 악성코드 유형



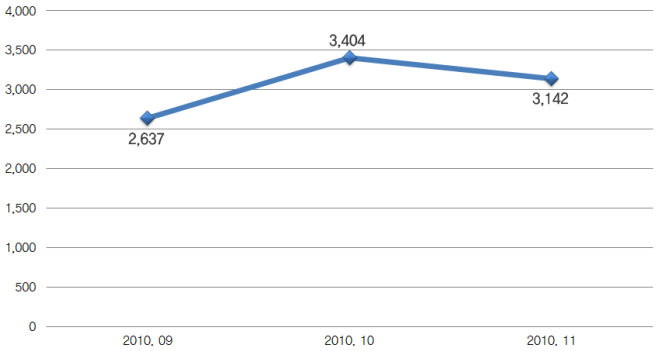
[그림 3-2] 월별 악성코드 유형

월별 악성코드가 발견된 도메인



[그림 3-3] 월별 악성코드가 발견된 도메인

월별 악성코드가 발견된 URL



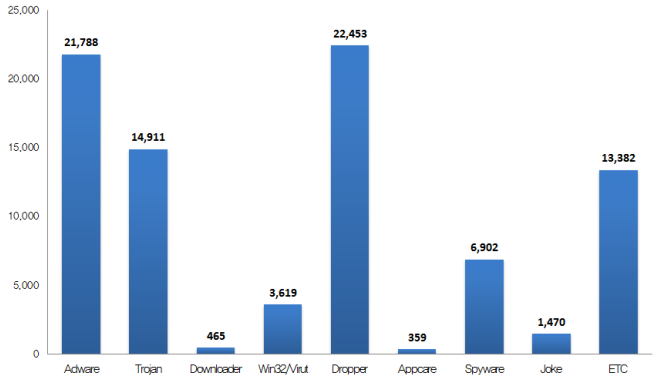
[그림 3-4] 월별 악성코드가 발견된 URL

2010년 11월 악성코드가 발견된 URL은 지난달 3,404건에 비해 92% 수준인 3,142건이다.

악성코드 유형별 배포 수

유형	건수	비율
DROPPER	22,453	26.3 %
ADWARE	21,788	25.5 %
TROJAN	14,911	17.5 %
SPYWARE	6,902	8.1 %
Win32/VIRUT	3,619	4.2 %
JOKE	1,470	1.7 %
DOWNLOADER	465	0.5 %
APPCARE	359	0.4 %
ETC	13,382	15.7 %
	85,349	100 %

[표 3-2] 악성코드 유형별 배포 수



[그림 3-5] 악성코드 유형별 배포 수

악성코드 배포 Top 10

순위	등락	악성코드명	건수	비율
1	–	Win-Adware/Shortcut.InlivePlayerActiveX.234	15,497	26.9 %
2	New	Win-Spyware/Keylogger.1226728	6,818	11.8 %
3	↑1	Win32/Induc	6,813	11.8 %
4	New	Dropper/Onlinegamehack.48640	6,298	10.9 %
5	New	Dropper/Win32.Onlinegamehack	5,687	9.9 %
6	New	Win-Trojan/Heur.554496	3,989	6.9 %
7	New	Dropper/Onlinegamehack.49152	3,768	6.5 %
8	New	Dropper/Onlinegamehack.48128.G	3,160	5.5 %
9	↓1	Win32/Virut.F	3,037	5.3 %
10	New	Win-Adware/Shortcut.Tickethom.36864	2,485	4.3 %
			57,552	100 %

[표 3-3] 악성코드 배포 Top 10

웹 보안 이슈

OWASP 2010 TOP 4

지난 Vol.06부터 OWASP 2010 Top10을 하나씩 자세히 살펴보고 있다. 그 네 번째 시간으로 OWASP 2010 Top 4 안전하지 않은 직접 객체 참조[1] 공격에 대해 알아보자.

먼저 안전하지 않은 직접 객체 참조의 주요 사항은 다음의 그림을 통해 알 수 있다.

[그림 3-6] 안전하지 않은 직접 객체 참조 개괄

1) 주요 내용

- Threat Agents(공격자) : 자신의 계정을 소유하고 있는 사용자이거나 타인의 계정을 훔치려는 익명의 외부 공격자, 자신의 행위를 숨기려고 하는 내부 사용자이다.

- Attack Vectors(공격경로) : 허가된 시스템 사용자인 공격자는 시스템 객체에서 다른 객체에 직접적으로 접근할 수 있는 파라미터(parameter) 값을 간단하게 변경한다. 이러한 것이 허가될 수 있는지를 확인해야 한다.

- Security Weakness(보안 취약점) : 애플리케이션은 웹 페이지를 생성할 때 종종 실제 이름이나 키 값을 사용한다. 애플리케이션은 사용자가 대상 객체에 대한 권한을 갖고 있는지 항상 검증하지 않는다. 결과적으로 안전하지 않은 직접 객체 참조에 대한 결함에 노출되게 된다. 이 취약점들을 탐지하기 위해 변수 값을 변경하는 테스트를 쉽게 할 수 있으며, 코드 분석을 통해 권한 부여가 적절한지를 신속하게 검증할 수 있다.

- Technical Impacts(기술적 영향) : 이 결함은 변수 값을 참조하는 모든 데이터를 위태롭게 할 수 있다. 변수 명명이 일반적이지 않다면, 공격자가 모든 가능한 데이터에 대해 쉽게 접근할 수 있다.

- Business Impacts(비즈니스 영향) : 노출되는 데이터의 비즈니스적 가치를 고려한다. 또한 취약점의 공개적 노출에 대한 비즈니스의 영향을 고려해야 한다.

2) 공격 시나리오 예

계정 정보에 접근하는 SQL 호출에 검증되지 않은 데이터를 사용하는 애플리케이션이 있다.

```
String query = "SELECT * FROM accts WHERE account = ?";
PreparedStatement pstmt =connection.prepareStatement(query , …
);
pstmt.setString( 1, request.getparameter( "acct" ));
ResultSet results = pstmt.executeQuery( );
```

공격자는 간단하게 자신의 브라우저에서 'acct' 변수의 값을 수정하여 원하는 계정 번호로 전송할 수 있다. 만약 이러한 것이 검증되지 않는다면, 공격자는 해당 사용자뿐만 아니라 다른 어떠한 사용자의 계정에도 접근할 수 있다.

```
http://example.com/app/accountInfo?acct=notmyacct
```

3) 대응책

안전하지 않는 직접 객체 참조를 방지하려면, 각 사용자들이 접근 가능한 객체를 보호하는 접근 방식의 선택이 요구된다.(예: 객체 번호, 파일명 등) :

- 사용자 혹은 세션 당 간접 객체 참조를 사용한다.

이를 통해 공격자가 허가되지 않은 자원을 직접적으로 공격 목표로 삼는 것을 방지할 수 있다. 예를 들어 자원의 데이터베이스 키를 사용하는 대신에 허용된 6개의 자원에 대하여 드롭다운 리스트 메뉴를 사용하여 현재

1.www.owasp.com, café.naver.com/securityplus

사용자가 선택하도록 허용된 1~6 중에서 선택하도록 하는 방법을 사용한다. 애플리케이션은 사용자별 간접 참조를 서버 상의 실제 데이터베이스 키로 변환한다. OWASP의 ESAPI에서는 개발자들이 직접 객체 참조를 제거할 수 있도록 순차적인 접근과 무작위 접근에 대한 예시를 제공한다.

- 접근을 확인한다.

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

[Reference]

OWASP

- OWASP Top 10–2007 안전하지 않은 직접객체참조
- ESAPI 접근 참조 맵 API
- ESAPI 접근 통제 API

– (isAuthorizedForData(), isAuthorizedForFile(), isAuthorizedForFunction() 참조)

External

- CWE 639 항목: 안전하지 않은 직접객체참조
- CWE 22 항목: Path Traversal(직접 객체 참조 공격의 예)

발행월 : 2010년 11월

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 김 재 성

감 수 상 무 조 시 행

참여연구원 ASEC 연구원
SiteGuard 연구원