ASEC REPORT

안철수연구소에서 발행하는 월간 보안 보고서

Vol. 10

안철수연구소

목 차

이달의 보안 동향

악성코드 동향 1
악성코드 통계 1
악성코드 이슈 2

시큐리티 동향 5
시큐리티 통계 5
시큐리티 이슈 5

웹 보안 동향 7
웹 보안 통계 7
웹 보안 이슈 9

Ⅰ. 이달의 보안 동향

1. 악성코드 동향

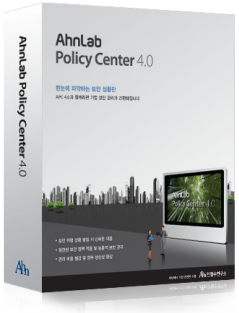
악성코드 통계

2010년 10월 악성코드 통계현황은 다음과 같다.

순위	등락	악성코드명	건수	비율
1	↑ 7	Win32/Parite	819,759	23.5 %
2	↑ 1	TextImage/Autorun	437,527	12.5 %
3	↑ 4	JS/Cve-2010-0806	309,949	8.9 %
4	–	Win32/Induc	218,878	6.3 %
5	New	Win-Trojan/Overtls4.Gen	207,871	6 %
6	New	Win-Trojan/Agent.36864.BSD	127,643	3.7 %
7	New	Win-Trojan/Totoran.Gen	127,185	3.6 %
8	New	JS/Agent	125,487	3.6 %
9	↑ 11	JS/Downloader	122,434	3.5 %
10	New	JSP/Agent	120,419	3.5 %
11	↓ 2	Win32/Olala.worm.57344	115,718	3.3 %
12	↓ 6	Win-Trojan/Spack3.Gen	113,877	3.3 %
13	↑ 1	Win32/Conficker.worm.Gen	92,156	2.6 %
14	↓ 12	JS/Exploit	91,101	2.6 %
15	New	Win32/Palevo9.worm.Gen	83,825	2.4 %
16	New	Win-Trojan/Dllbot.128519	82,612	2.4 %
17	New	Win-Trojan/Agent.129231	78,530	2.3 %
18	↓ 2	Win-Trojan/Securisk	78,397	2.2 %
19	New	Win32/Virut.F	67,946	1.9 %
20	↓ 1	Win32/Virut.B	67,113	1.9 %
			3,488,427	100 %

[표 1-1] 악성코드 감염보고 Top 20

2010년 10월의 악성코드 감염 보고는 Win32/Parite이 1위를 차지하고 있으며, TextImage/Autorun과 JS/Cve-2010-0806가 각각 2위와 3위를 차지 하였다. 신규로 Top20에 진입한 악성코드는 총 9건이다.



AhnLab Policy Center 4.0

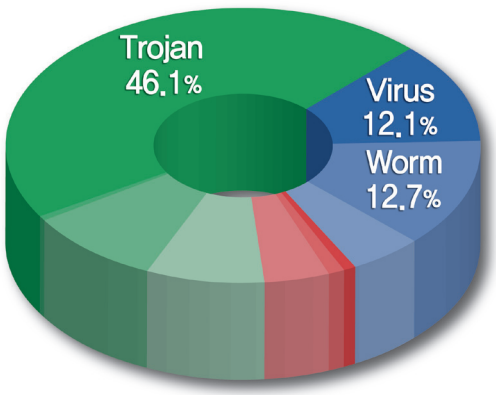
아래 표는 악성코드의 주요 동향을 파악하기 위하여, 악성코드별 변종을 종합한 악성코드 대표진단명 감염보고 Top200이다.

순위	등락	악성코드명	건수	비율
1	↑ 2	WIN-TROJAN/AGENT	856,817	14%
2	↑ 16	WIN32/PARITE	820,974	13.4%
3	↓ 2	WIN-TROJAN/ONLINEGAMEHACK	672,577	11%
4	–	WIN-TROJAN/DOWNLOADER	537,303	8.8%
5	↑ 1	TEXTIMAGE/AUTORUN	439,719	7.2%
6	↑ 9	JS/CVE-2010-0806	309,949	5.1%
7	↑ 2	WIN32/CONFICKER	270,856	4.4%
8	↓ 1	WIN32/AUTORUN.WORM	265,709	4.3%
9	↑ 1	WIN32/VIRUT	260,375	4.3%
10	↓ 2	WIN32/INDUC	219,112	3.6%
11	New	WIN-TROJAN/OVERTLS4	207,871	3.4%
12	↑ 1	DROPPER/MALWARE	172,202	2.8%
13	↑ 6	WIN-TROJAN/ADLOAD	159,099	2.6%
14	–	WIN32/KIDO	154,336	2.5%
15	↑ 2	DROPPER/ONLINEGAMEHACK	144,379	2.4%
16	New	WIN32/PALEVO	135,759	2.2%
17	New	WIN-TROJAN/TOTORAN	127,185	2.1%
18	New	JS/AGENT	126,036	2.1%
19	New	JS/DOWNLOADER	122,543	2%
20	New	JSP/AGENT	120,419	2%
			6,123,220	100

[표 1-2] 악성코드 대표진단명 감염보고 Top 20

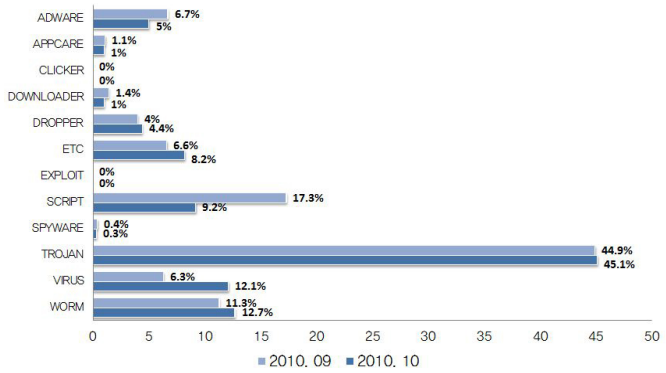
2010년 10월의 감염보고 건수는 Win-Trojan/Agent가 총 856,917건으로 Top20중 14%의 비율로 1위를 차지하고 있으며, Win32/Parite이 820,974건으로 2위, Win-Trojan/Onlinegamehack이 672,577건으로 3위를 차지 하였다.

아래 차트는 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.



[그림 1-1] 악성코드 유형별 감염보고 비율

2010년 10 월의 감염보고 건수는 악성코드 유형별로 감염보고건수 비율은 트로잔(TROJAN)류가 46.1%로 가장 많은 비율을 차지하고, 웜(WORM)이 12.7%, 바이러스(VIRUS)가 12.1%의 비율을 각각 차지하고 있다.



[그림 1-2] 악성코드 유형별 감염보고 전월 비교

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

[그림 1-3] 악성코드 월별 감염보고 건수

10월의 악성코드 월별 감염보고 건수는 11,735,344건으로 9월의 악성코드 월별 감염 보고건수 12,133,061건에 비해 397,717건이 감소하였다.

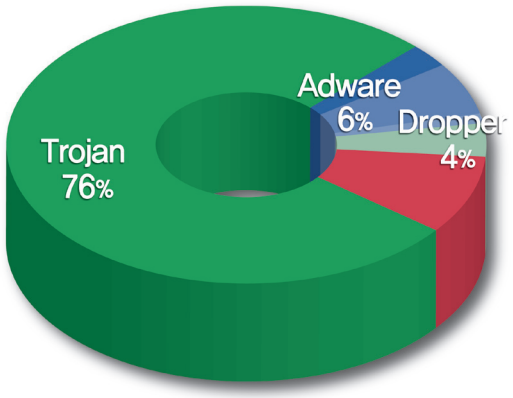
AhnLab V3 MSS

아래 표는 10월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top20이다.

순위	악성코드명	건수	비율
1	Win-Trojan/Agent.36864.BSD	127,643	17.2 %
2	JSP/Agent	120,419	16.3 %
3	Win-Trojan/Dllbot.128519	82,612	11.2 %
4	Win-Trojan/Agent.129231	78,530	10.6 %
5	Win-Trojan/Downloader.16040	56,890	7.7 %
6	Win-Trojan/Agent.106496.VF	38,420	5.2 %
7	Win-Trojan/Downloader.36864.PM	37,320	5 %
8	Win-Adware/PinSearch.81920	26,937	3.6 %
9	Win-Adware/BHO.PinSearch.57344	24,369	3.3 %
10	Win-Trojan/Agent.106496.VN	18,089	2.4 %
11	Win-Trojan/Downloader.102256	17,379	2.3 %
12	Win-Trojan/Kraprootkit.840192	16,493	2.2 %
13	Win-Trojan/Agent.676352.E	12,966	1.8 %
14	Win-Trojan/Onlinegamehack.57344.BN	12,798	1.7 %
15	Win-Trojan/Onlinegamehack.57344.BL	12,278	1.7 %
16	Win-Dropper/Barcon.161374	12,231	1.7 %
17	Win-Trojan/Downloader.170079	11,513	1.6 %
18	Win-Trojan/Adload.708608.B	11,444	1.5 %
19	Win-Adware/PinSearch.10752.B	11,122	1.5 %
20	Win-Trojan/Adload.640000.E	10,835	1.5 %
		740,288	100 %

[표 1-3] 신종 악성코드 감염보고 Top 20

10월의 신종 악성코드 감염 보고의 Top 20은 Win-Trojan/Agent.36864.BSD가 127,643건으로 전체 17.2%를 차지하여 1위를 차지하였으며, JSP/Agent가 120,419건 2위를 차지하였다.



[그림 1-4] 신종 악성코드 유형별 분포

10월의 신종 악성코드 유형별 분포는 트로잔이 76%로 1위를 차지하였다. 그 뒤를 이어 애드웨어가 6%, 드롭퍼가 4%를 각각 차지하였다.

악성코드 이슈

스턱스넷(Stuxnet) 웜의 전용백신으로 위장한 악성코드 등장

스턱스넷 웜에 대한 소식이 언론에 알려지면서 해당 악성코드의 파괴력과 잠재적인 위협이 연일 매스컴을 타고 있다. 이에 뒤질세라 이를 교묘히

이용한 가짜 전용백신 형태의 악성코드(Win-Trojan/Deltree.75776.C)가 등장 하였다. 해당 악성코드는 다음과 같은 아이콘을 가지고 있다. 그리고 마이크로소프트(Microsoft) 사에서 제작한 것 처럼 자신을 위장하고 있다.

[그림1-5] 가짜 Stuxnet 웜 전용백신 아이콘

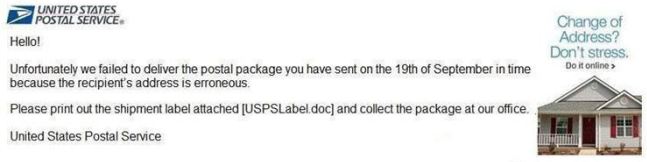
악성코드가 실행되면 다음과 같은 내용을 갖고 있는 특정한 배치파일을 실행하여 C:₩ 드라이브 내 파일을 모조리 삭제 하도록 한다. 따라서 재부팅 시 정상적으로 부팅이 되지 않을 수 있다.

[그림1-6] 가짜 스턱스넷 웜 전용백신이 수행하는 배치 명령

스턱스넷 웜에 대한 위협이 알려지면서 이를 예방하거나 감염된 사실을 확인 하려는 시도가 증가 하였다. 이러한 틈을 노리고 가짜 전용백신이나와 오히려 시스템에 피해를 주고 있다. 우리가 쉽게 지나치는 보안상식 중 하나는 공식적으로 안티 바이러스 업체에서는 전용백신을 메일에 첨부하여 고객에게 대량으로 발송하거나 자신의 홈페이지가 아닌 출처가 불분명한 웹 사이트에 업로드 하지 않는다는 것이다. 따라서 사용자들은 전용백신을 다운로드 받기 전 반드시 파일이 업로드 된 위치가 안티 바이러스 홈페이지인지 그리고 공신력이 있거나 믿을 만한 곳인지 한번쯤 확인 하시길 바란다.

메일 본문이 이미지로 제작된 허위 USPS 운송 메일 유포

궁극적으로 가짜 백신 설치를 목적으로 하는 형태의 허위 USPS(United States Postal Service) 운송 메일로 위장한 악성코드가 발견, 보고 되었다. 기존에 알려진 Oficla 악성코드 변형은 메일 제목으로 "USPS Delivery Problem NR[임의의 숫자]" 를 가지고 있으며 메일 본문에는 xxs664.jpg(27,692 바이트)의 JPEG 파일로 처리하여 다음과 같은 형태를 가지고 있다.

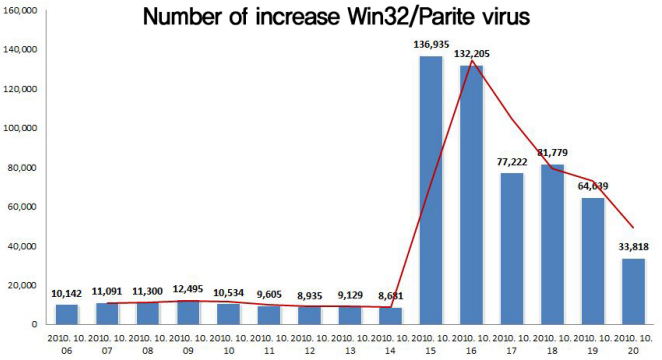


[그림1-7] 허위 USPS 운송메일로 위장한 악성코드의 JPEG 형태 본문

메시지 본문을 JPEG 로 처리 하는 것은 일반적으로 안티 스팸 솔루션을 회피하는 목적으로 종종 사용된다. 첨부된 파일은 Dropper/Malware.178176.AB 로 진단된다. 실행이 된 경우 루마니아를 거쳐 독일에 위치한 특정 시스템으로부터 가짜 백신을 다운로드 하여 설치 하게 된다. 일반적으로 국내에서는 영어로 된 제목과 본문을 갖는 메일은 거부감을 갖게 되는 게 일반적이다. 따라서 이러한 메일을 받았을 때 첨부파일을 실행해보는 사람은 많지 않을 것이라고 추정 할 수 있다. 하지만 가짜 백신을 설치하여 금적적인 이익을 노리는 악성코드 제작자들은 이미 가짜 백신이라는 검은 시장이 그들간의 경쟁심화와 함께 포화 상태에 이르고 있다라는 것을 느끼고 있을지도 모른다. 이들이 스스로 자멸을 할지 아니면 온라인 게임의 사용자 계정을 탈취하는 트로이목마처럼 특정 유형의 형태만 계속 살아 남을지 아직은 미지수 이다. 그러나 그들의 치열한 경쟁구도 속에 이미 어설프지만 한글로 번역된 가짜 백신도 나온 만큼 더욱 더 정교한 형태의 한글화된 허위 메일과 가짜 백신이 우리에게 피해를 입힐지도 모르는 만큼 출처가 불분명한 메일에는 보다 더 주의를 기울일 필요가 있다.

국내에 감염 보고가 많았던 패리티(Parite)와 팔레보(Palevo)

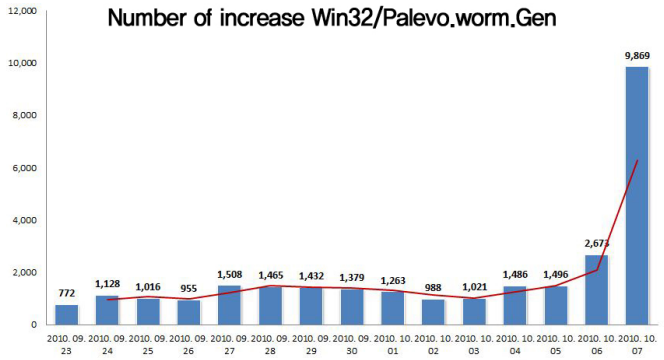
이번 달 10월초와 중순 Win32/Parite 와 Win32/Palevo.worm.Gen 바이러스의 감염 보고 건 수가 일시적으로 급격히 증가 하였다. 특히 Parite 바이러스는 이미 발견 보고가 있은 지 8년도 넘은 오래된 (파일 감염형 악성코드)바이러스 이다. 수집된 감염된 파일을 확인해 보니 이 바이러스에 감염된 파일을 국산 애드웨어에 많이 감염이 되어 있었다. 감염추이는 다음과 같다.



[그림1-8] Win32/Parite 바이러스 증가건수

2010년 10월15일에 고점을 기록하고 하락추세에 있다. Parite 바이러스는 이전에도 다른 악성코드가 감염되어 발견 되거나 이와 비슷하게 애드웨어 등에 감염되어 배포가 된 사례가 있었다. 이번 경우에도 애드웨어에 감염되어 일시적으로 배포가 된 사례로 파악 되었다. 고의성이 없다면 애드웨어 업체는 프로그램 배포 전 감염사실을 몰랐거나 백신으로 검사를 해보지 않은 것으로 추정 해볼 수 있다. 글을 작성하는 현재 감염건수는 월초와 크게 다르지 않는 것으로 파악 되었다.

두 번째는 Palevo 웜의 급격한 증가였다. 10월7일에는 평소와 다르게 급격히 증가한 모습을 그래프를 통해서 알 수가 있다.

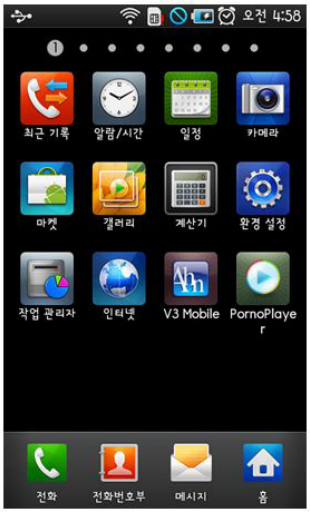


[그림1-9] Win32/Palevo.worm.Gen 증가건수

급격히 증가한 원인에 대하여 명확하지는 않지만 Palevo 웜은 USB 형태의 이동식 디스크를 통해서도 전파가 된다. 또한 로컬 드라이브에 존재하는 파일을 삭제 하여도 Explorer.exe 에 삽입된 악의적인 스레드를 제거하지 않는다면 지속적으로 외부와 통신하며 USB 삽입 시 복사본을 감염시키고 자신의 다른 변형을 다운로드 하여 실행한다. 따라서 추정해보면 봇마스터가 봇넷 운영력을 극대화 하려고 감염된 기존 시스템을 통하여 변형을 유포하여 일시적으로 감염, 보고 건수가 증가 한 것으로 추정된다.

안드로이드폰의 성인 동영상 플레이어로 위장한 악성코드

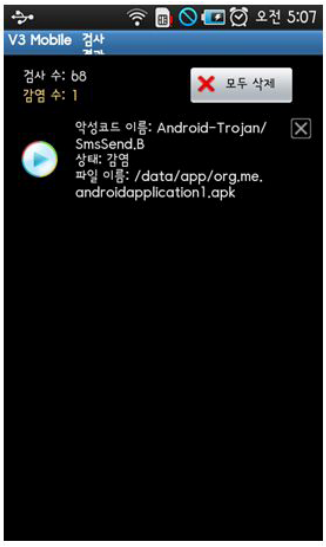
안드로이드OS로 구동되는 스마트폰에서, 어플리케이션 설치 시 사용자에게 SMS 요금을 과금시키는 PornoPlayer라는 이름의 악성코드가 확인되었다. 해당 어플리케이션은 최신 엔진으로 업데이트된 V3 Mobile 제품에서 Android-Trojan/SmsSend.B 로 진단/치료 가능하다. 아래 그림 1-10은 해당 악성코드가 설치된 화면이며, 설치된 악성코드는 성인 동영상 플레이어 관련 이름으로 WMP(Windows Media Player) 아이콘 모양을 띄고 있다.



[그림 1-10] WMP로 위장한 PornoPlayer

위와 같이 성인 동영상 플레이어로 위장하여 설치되는 악성코드는, 특정 번호로 SMS 메시지를 보내 사용자에게 요금을 과금시키는 기능을 수행하게 된다.

아래의 그림은 V3 Mobile 제품에서 Android-Trojan/SmsSend.B 진단명으로 진단된 화면이다.



[그림 1-11] PornoPlayer가 진단된 화면

관련 악성 어플리케이션은 2010년 8월 10일(Android-Trojan/Sms-Send)에 최초 확인된 이후로 9월 9일(Android-Trojan/SmsSend)과 10월 14일(Android-Trojan/SmsSend.B)에 추가로 변종이 발견되었다.

스마트폰 사용자의 사생활을 침해하는 스파이웨어

스마트폰을 대상으로 통화 내역, 문자 송수신 내역, 위치 정보, 이메일 내용 등등 민감한 개인 정보를 외부로 유출하는 스파이웨어(Spyware)가 해외에서 개발되고 판매되고 있다. 이들 스파이웨어는 심비안(Symbian/Symbian9), 윈도우모바일(Windows Mobile), 블랙베리(BlackBerry), 아이폰(iPhone), 안드로이드(Android)등 현재 존재하는 대부분의 스마트폰에서 사용할 수 있도록 다양한 플랫폼용 버전을 각각 제작해서 서비스하고 있다. 이들 스파이웨어가 설치되면 해당 스마트폰의 사용자의 개인 정보 및 사생활이 모두 스파이웨어 제작 업체로 전송되고, 해당 스파이웨어 프로그램을 구입한 사용자는 웹사이트에서 접속해서 관련 내역을 확인할 수 있다. 해외에선 주로 바람을 피는 남편과 아내를 감시하거나 직원 감시, 자녀보호, 스마트폰 데이터 자동 백업등의 목적으로 서비스하고 있다. 문제는 해당 스파이웨어가 자신의 스마트폰에 설치된 사실을 모르고 스마트폰을 사용하는 경우이다. 실제 사용자가 설치에 동의하지 않았음에도 불구하고 스파이웨어가 설치되어 동작하며 개인의 중요한 정보는 물론 개인 사생활 내역을 외부로 유출시키는 행위이므로 이는 불법적인 행위에 해당한다. 얼마 전 국내에서 안드로이드폰용 스파이웨어인 Android-Spyware/Mobilefonex가 발견 되었다. 이런 스파이웨어가 스마트폰에 설치되면 악성코드 검사를 통하지 않고서는 사용자가 직접 확인하기 어려워 감염 사실을 모른 채 개인 정보가 지속적으로 유출될 수 있다. 또한 국내에서도 동일한 목적으로 해당 스파이웨어를 유포할 수 있으므로 얼마든지 피해자는 발생할 수 있다. 따라서 스마트폰 전용 백신을 사용하여 주기적으로 악성코드 감염 여부를 검사해 보는 것이 좋다. 또

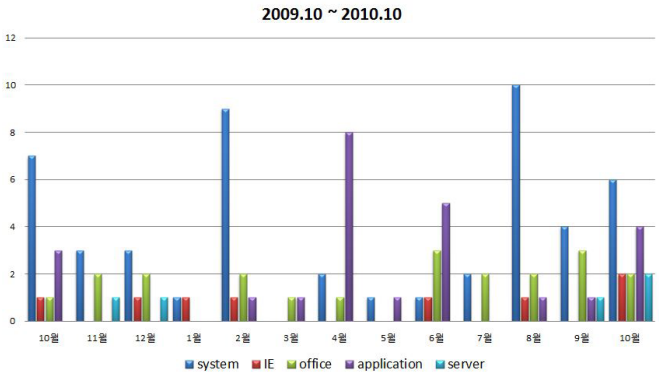
한, 탈옥(JailBreaking), 루팅(Rooting)과 같이 단말기 운영체제 소프트웨어를 변조하는 행위는 하지 않는 것이 바람직하다.

2. 시큐리티 동향

시큐리티 통계

10월 마이크로소프트 보안 업데이트 현황

마이크로소프트사로부터 발표된 이번 달 보안 업데이트는 총 16건이다.



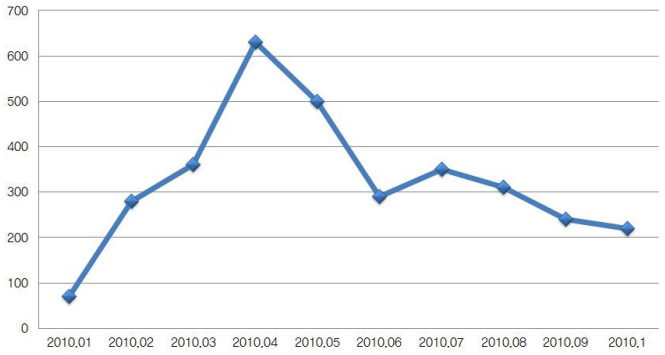
[그림 2-1] 공격 대상 기준 별 MS 보안 업데이트

위험도	취약점	POC
긴급	MS10-071 Cumulative Security Update for Internet Explorer	무
중요	MS10-072 Vulnerabilities in SafeHTML Could Allow Information Disclosure	무
중요	MS10-073 Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege	무
보통	MS10-074 Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution	무
긴급	MS10-075 Vulnerability in Media Player Network Sharing Service Could Allow Remote Code Execution	무
긴급	MS10-076 Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution	무
긴급	MS10-077 Vulnerability in .NET Framework Could Allow Remote Code Execution	무
중요	MS10-078 Vulnerabilities in the OpenType Font (OTF) Format Driver Could Allow Elevation of Privilege	무
중요	MS10-079 Vulnerabilities in Microsoft Word Could Allow Remote Code Execution	무
중요	MS10-080 Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution	무
중요	MS10-081 Vulnerability in Windows Common Control Library Could Allow Remote Code Execution	무
중요	MS10-082 Vulnerability in Windows Media Player Could Allow Remote Code Execution	무
중요	MS10-083 Vulnerability in COM Validation in Windows Shell and WordPad Could Allow Remote Code Execution	무
중요	MS10-084 Vulnerability in Windows Local Procedure Call Could Cause Elevation of Privilege	무
중요	MS10-085 Vulnerability in SChannel Could Allow Denial of Service	무
보통	MS10-086 Vulnerability in Windows Shared Cluster Disks Could Allow Tampering	무

[표 2-1] 2010년 8월 주요 MS 보안 업데이트

이번 달은 다수의 원격 취약점에 대한 업데이트를 포함하여, 시스템 6건, IE 2건, 오피스 2건, 어플리케이션 4건, 서버 2건에 대한 업데이트가 진행되었다.

악성코드 침해 웹사이트 현황



[그림 2-2] 월별 침해 사이트 통계

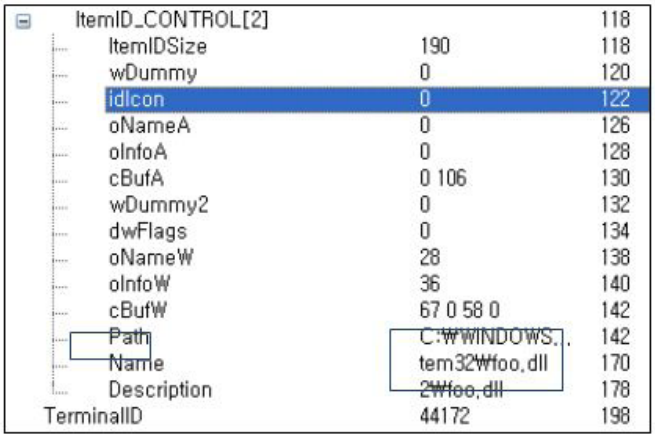
[그림 2-2]는 월별 악성코드 침해 사이트 현황을 나타낸 그래프로, 전월에 비해 침해 사이트가 다소 감소하였다. 이번달에도 주로 ARP Spoofing과 결합된 게임핵, 윈도우 정상 파일을 패치하는 게임핵 등이 침해 사이트를 통해서 유포되었고 해당 악성코드 유포를 위해 MS10-018취약점을 가장 많이 사용하였다.

"보안 업데이트가 뭐죠?" 라고 물어보는 무관심에서 벗어나 이제 PC를 좀더 안전하고 편리하게 사용하기 위해서는 기본적으로 보안 업데이트를 정기적으로 실시하고, 백신도 최신 엔진으로 업데이트와 함께 주기적인 시스템 검사가 필요하다.

시큐리티 이슈

LNK 취약점(CVE-2010-2568)

이 번달 초 스턱스넷 악성코드가 국내외에서 큰 이슈가 되었다. 스턱스넷 악성코드가 사용한 여러 취약점 중 LNK(CVE-2010-2568) 취약점에 대한 내용을 보고자 한다. LNK(CVE-2010-2568) 취약점을 이용하여 윈도우 탐색기로 LNK Shortcut File(바로가기 파일)이 위치한 디렉터리를 열기만 하면 바로가기 파일이 자동으로 실행이 된다.



[그림 2-3] 악성 Shortcut 파일의 구조

LNK 취약점은 바로가기 파일의 idlcon의 값이 0으로 셋팅되어지면 바로가기 파일의 Path에 나와있는 DLL파일을 Load하여 실행된다.

```
0:005> ub SHELL32!_LoadCPLModule+0x113 L1
SHELL32!_LoadCPLModule+0x10e:
77424fd3 15001a3877      adc     eax,offset SHELL32!_imp__LoadLibraryW (77381a00)
0:012> g
Breakpoint 0 hit
eax=00000001 ebx=00f2ee7c ecx=00007c0f edx=00120003 esi=00000001 edi=7c80a634
eip=7c80acd3 esp=00f2e9c0 ebp=00f2ec18 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
kernel32!LoadLibraryW:
7c80acd3 8bff            mov     edi,edi
0:005> dd esp
00f2e9c0  77424fd8 00f2ee7c 000fe39c 00f2ee78
00f2e9d0  00000000 00000020 00000008 00f2ee7c
0:005> db 00f2ee7c
00f2ee7c  43 00 3a 00 5c 00 57 00-49 00 4e 00 44 00 4f 00  C.:.\.W.I.N.D.O.
00f2ee8c  57 00 53 00 5c 00 73 00-79 00 73 00 74 00 65 00  W.S.\.s.y.s.t.e.
00f2ee9c  6d 00 33 00 32 00 5c 00-66 00 6f 00 6f 00 2e 00  m.3.2.\.f.o.o...
00f2eeac  64 00 6c 00 6c 00 00 00-2c aa 13 00 b0 a9 13 00  d.l.l...,.......
```

[그림 2-4] 악성 Shortcut 파일의 실행 모습

SHELL32!_imp_LoadLibraryW 함수를 시작으로 바로가기 파일의 Path에 DLL 파일을 Load 하여 실행하게 된다.

[그림 2-5] USB 매체를 이용한 악성 Shortcut 파일의 Path

일반적으로 USB 매체를 이용하는 바이러스는 autorun.inf를 이용하였는데, 이번에는 LNK 취약점을 이용한 바로가기 파일과 악성코드를 USB 루트(Root) 디렉터리에 넣고 사용자가 윈도우 탐색기로 USB 루트 디렉터리를 열면 자동실행이 되도록 하여 USB 매체를 통해 전파하도록 하였다.

9월 0-Day로 발표된 LNK Shortcur File 취약점은 여러 악성코드로 배포되고 있으며, 현재는 Microsoft에서 패치가 이루어진 상태다.

Firefox 0-Day 취약점(CVE-2010-3765)

노벨 평화상 웹 사이트에서 Firefox에 존재하는 알려지지 않은 0-Day 취약점을 악용하여 악성코드를 유포한 사고가 발생하였다.

```
04AA0000   90              NOP
04AA0001   90              NOP
04AA0002   EB 0F          JMP SHORT 04AA0013
04AA0004   58              POP EAX
04AA0005   5B              POP EBX
04AA0006   8918            MOV DWORD PTR DS:[EAX],EBX
04AA0008   83FB FF         CMP EBX,-1
04AA000B   74 0B           JE SHORT 04AA0018
04AA000D   83C0 04         ADD EAX,4
04AA0010   EB F3           JMP SHORT 04AA0005
04AA0012   90              NOP
04AA0013   E8 ECFFFFFF     CALL 04AA0004
```

[그림 2-6] Firefox 0-Day 취약점을 이용한 쉘코드 부분

```
WinExec(cmd.exe /c FOR /R "%USERPROFILE%₩Local Settings₩Application
Data₩Mozilla₩Firefox₩Profiles₩" %i IN (*) DO if %~zi equ 48640 cmd.exe
/c copy "%i" "%temp%₩scvhost.exe" /y & "%temp%₩scvhost.exe")
```

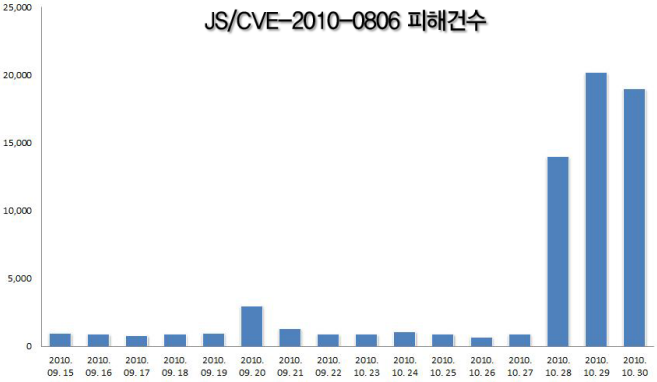
[그림 2-7] 쉘코드(Shellcode)를 이용한 실행 명령

이번 취약점은 Heap Spray 버퍼오버플로우의 이용으로 쉘코드를 실행시켜 악의적인 행동을 하게한다. 현재는 패치가 이루어져 Firefox 3.6.12 또는 Firefox 3.5.15 버전으로 업데이트하면 예방이 가능하다.

MS10-018 취약점 공격 악성코드 증가

2010년 3월 9일 타켓 공격(Targeted Attack) 형태로 악용되어 제로 데이(Zero-Day, 0-Day) 취약점이었던 마이크로소프트(Microsoft)의 MS10-018 인터넷 익스플로러(Internet Explorer) 누적 보안 업데이트(980182)를 악용한 악성코드가 10월 1일을 기준으로 한국에서 다시 증가하고 있는 것으로 ASEC에서 파악하였다.

해당 MS10-018 취약점을 제거 할 수 있는 보안 패치는 3월 31일 마이크로소프트에 의해 제공되고 있으며 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 악용되고 있는 것으로 볼 수 있다. V3에서는 MS10-018 취약점을 악용하는 자바 스크립트(Java Script) 형태의 악성코드를 JS/CVE-2010-0806으로 진단하며 AMP(AhnLab Malicious code Processing system)을 통해 집계된 피해 건수는 아래 그래프와 동일하다.



[그림 2-8] JS/CVE-2010-0806 10월 1일 기준 피해 건수

해당 피해 건수 그래프를 살펴보면 9월 28일 약 14,000건으로 급증하기 시작하여 9월 29일과 9월 30일에는 각각 약 20,200건 그리고 약 19,000건으로 지속되고 있다. 해외 보안 업체의 동향들을 살펴보아도 6월과 7월부터 해당 MS10-018 취약점을 악용하는 스크립트 형태의 악성코드가 증가하고 있음을 알 수 있다. 웹 브라우저의 취약점을 악용하는 JS/CVE-2010-0806와 같은 악성코드는 대부분이 개인 정보 유출 또는 원격제어 기능을 포함하고 있는 다른 악성코드들의 다운로드에 악용되는 것이 일반적인 형태임으로 해당 스크립트 악성코드에 감염될 경우에 제2, 3의 악성코드들의 감염 피해가 우려된다고 할 수 있다.

3. 웹 보안 동향

웹 보안 통계

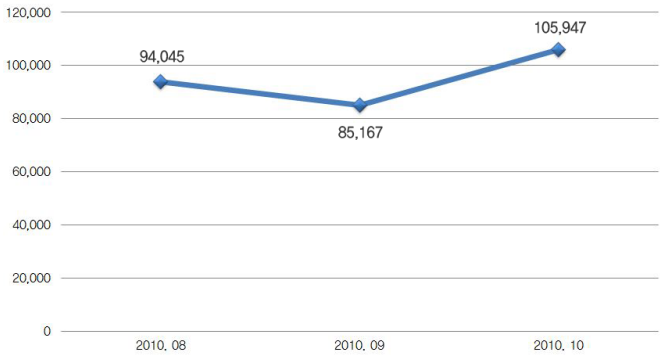
월별 악성코드 보안 요약

구분	건수
악성코드 발견 건수	105,947
악성코드 유형	920
악성코드가 발견된 도메인	794
악성코드 발견된 URL	3,404

[표3-1] 웹 사이트 보안 요약

악성코드 발견 건수는 105,947건이고, 악성코드 유형은 920건이며, 악성코드가 발견된 도메인은 794건이며, 악성코드 발견된 URL은 3,404 건이다. 2010년 10월은 2010년 9월보다 악성코드 발견 건수, 유형 등 모든 수치가 증가하였다.

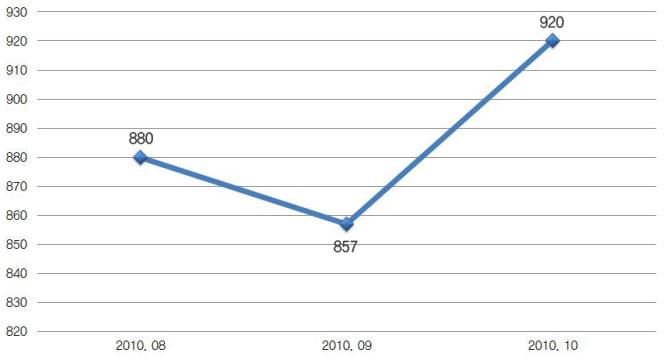
월별 악성코드 발견 건수



[그림 3-1] 월별 악성코드 발견 건수

2010년 10월 악성코드 발견 건수는 전달의 85,167건에 비해 124% 수준인 105,947건이다.

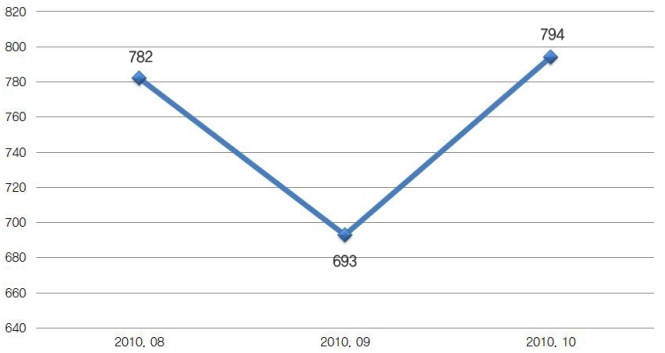
월별 악성코드 유형



[그림 3-2] 월별 악성코드 유형

2010년 10월 악성코드 유형은 전달의 857건에 비해 107% 수준인 920건이다.

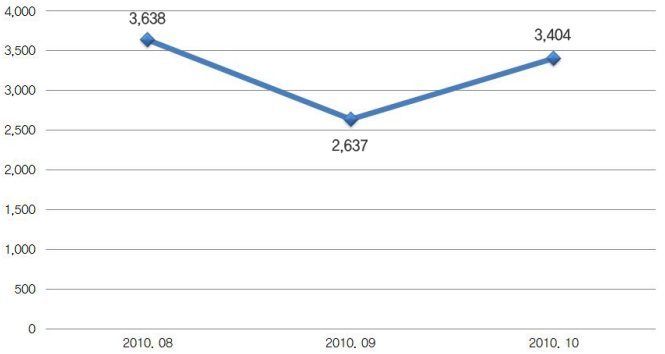
월별 악성코드가 발견된 도메인



[그림 3-3] 월별 악성코드가 발견된 도메인

2010년 10월 악성코드가 발견된 도메인은 전달의 693건에 비해 115% 수준인 794건이다.

월별 악성코드가 발견된 URL



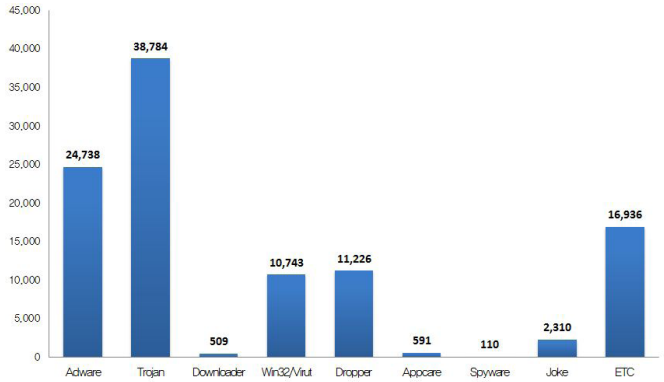
[그림 3-4] 월별 악성코드가 발견된 URL

2010년 10월 악성코드가 발견된 URL은 전달의 2,637건에 비해 129% 수준인 3,404건이다.

악성코드 유형별 배포 수

유형	건수	비율
TROJAN	38,784	36.6 %
ADWARE	24,738	23.3 %
DROPPER	11,226	10.6 %
Win32/VIRUT	10,743	10.1 %
JOKE	2,310	2.2 %
APPCARE	591	0.6 %
DOWNLOADER	509	0.5 %
SPYWARE	110	0.1 %
ETC	16,936	16 %
	105,947	100 %

[표 3-2] 악성코드 유형별 배포 수



[그림 3-5] 악성코드 유형별 배포 수

악성코드 유형별 배포 수에서 트로잔(TROJAN)류가 38,784건 전체의 36.6%로 1위를 차지하였으며, 애드웨어(ADWARE)류가 24,738건으로 전체의 23.3%로 2위를 차지하였다.

악성코드 배포 Top 10

순위	등락	악성코드명	건수	비율
1	↑ 1	Win-Adware/Shortcut.InlivePlayerActiveX.234	15,396	21.1 %
2	New	Win-Trojan/Npkon.53248	12,387	17 %
3	New	Win-Trojan/Sasfis.303616.D	12,296	16.9 %
4	↓ 1	Win32/Induc	7,386	10.1 %
5	New	Win32/Parite	6,196	8.5 %
6	New	Dropper/Onlinegamehack.38400	4,706	6.5 %
7	New	Win-Trojan/Patcher.35840	3,987	5.5 %
8	↓ 2	Win32/Virut.F	3,943	5.4 %
9	-	Win32/Virut.B	3,407	4.7 %
10	↓ 9	Win32/Virut	3,234	4.4 %
			72,938	100 %

[표 3-3] 악성코드 배포 Top 10

악성코드 배포 Top10에서 Win-Adware/Shortcut.InlivePlayerActiveX.234이 15,396건으로 1위를 차지하였으며, Top10에 Win-Trojan/Npkon.53248등 5건이 새로 등장하였다.

웹 보안 이슈

OWASP 2010 TOP 3

지난 Vol.06부터 OWASP 2010 Top10을 하나씩 자세히 살펴보고 있다. 그 세 번째 시간으로 OWASP 2010 Top 3 취약한 인증과 세션 관리[1] 공격에 대해 알아보자.

먼저 취약한 인증과 세션 관리 공격의 주요 사항은 다음의 그림을 통해 알 수 있다.

[그림 3-6] 취약한 인증과 세션 개괄

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

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) : 공격자는 사용자를 위장하기 위해 인증이나 세션 관리의 노출 또는 결함(노출된 계정, 패스워드 혹은 세션 ID)를 이용한다.
- Security Weakness(보안 취약점) : 개발자들은 습관적으로 인증 및 세션 관리 체계를 자주 구축하지만 올바르게 구축하기는 어려운 것이 현실이다. 그 결과 로그아웃, 패스워드 관리, 타임아웃, 사용자 정보 기억, 비밀번호 찾기 질문, 계정 업데이트 등 이러한 습관적인 체계 구축은 종종 결함을 갖고 있다. 또 각기 다르게 구현되기 때문에 결함을 찾기란 쉽지 않다.
- Technical Impacts(기술적 영향) : 이 결함은 일부 혹은 모든 계정에 대한 공격을 허용한다. 성공하는 즉시, 해당 계정이 할 수 있는 모든 것을 할 수 있기 때문에 특별한 권한이 부여된 계정은 자주 공격 대상이 된다.
- Business Impacts(비즈니스 영향) : 영향을 받는 데이터나 어플리케이션 기능의 비즈니스적 가치를 고려한다. 또한 취약점의 공개적 노출에 대한 비즈니스 영향을 고려해야 한다.

2) 공격 시나리오 예

URL Rewriting을 지원하고 URL 상에 세션 ID가 포함된 항공 예약 어플리케이션이 있다고 할 때, 인증된 사용자가 친구에게 항공권 예약 내용을 알려주고자 아래 URL 링크를 E-mail을 통해 보낸다면, 어떤 일이 발생할까?

http://example.com/sale/saleitems;jsessionid=2P0OC2JDPXM0OQSNDLPSKHCJUN2JV?dest=Hawaii

URL의 전송한 사용자는 그의 세션 ID가 노출 되게 되며, 수신 받은 친구는 이 URL 링크를 이용해 메일을 발송한 사용자의 세션과 신용카드 넘버까지 확인하여 추가적인 행위를 할 수 있다.

3) 대응책

취약한 인증과 세션 관리에 대한 대응책으로는 개발자들이 다음과 같은 사항을 준수하여야 한다.

- 강력한 인증 및 세션 관리 통제의 단일 체계를 구축해야 한다.
- OWASP의 어플리케이션 보안 검증 표준(ASVS) 항목의 V2(인증)와 V3(세션 관리)에 정의되어 있는 인증 및 세션 관리 요구사항을 모두 충족시켜야 한다.

- 개발자를 위한 간단한 인터페이스를 갖추어야 한다. 특히, ESAPI 인증자와 사용자 API를 좋은 예를 삼아 구축 시 참고하여야 한다.
- 세션 ID를 도용하는데 사용될 수 있는 XSS 취약점을 막기 위해 노력해야 한다.

[Reference]

OWASP

◆OWASP 인증 Cheat Sheet

◆ESAPI 인증자 API

◆ESAPI 사용자 API

◆OWASP 개발 가이드 : 인증 챕터

◆OWASP 테스트 가이드 : 인증 챕터

External

◆CWE 287 항목 : 부적절한 인증

발행월 : 2010년 10월

ASEC REPORT 집필진

편 집 장 선임 연구원 허 종 오

집 필 진 선임 연구원 정 진 성
선임 연구원 장 영 준
선임 연구원 이 재 호
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