



피해갈 수 없는 탐지력

# 알약

월간 보안동향 보고서

## 목차

### Part I. 3 월의 악성코드 통계

1. 악성코드 통계.....	2
(1) 감염 악성코드 Top 15.....	2
(2) 카테고리별 악성코드 유형.....	3
(3) 카테고리별 악성코드 비율 전월 비교.....	3
(4) 월별 피해 신고 추이.....	4
(5) 월별 악성코드 DB 등록 추이.....	4
2. 악성코드 이슈 분석 - “보호받는 시스템 DLL 파일을 감염시키는 악성코드” .....	5
3. 허니팟/트래픽 분석.....	7
(1) 상위 Top 10 포트.....	7
(2) 상위 Top 5 포트 월별 추이.....	7
(3) 악성 트래픽 유입 추이.....	8
4. 스팸메일 분석.....	9
(1) 일별 스팸 및 바이러스 통계 현황.....	9
(2) 월별 통계 현황.....	9
(3) 스팸 메일 내의 악성코드 현황.....	10

### Part II. 3 월의 보안 이슈 돋보기

1. 3 월의 보안 이슈.....	11
2. 3 월의 취약점 이슈.....	14



Part I 3월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2010년 3월 1일 ~ 2010년 3월 31일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	-	A.ADV.Admoke	Adware	61,708
2	↑1	S.SPY.Lineag-GLG	Spyware	54,384
3	↓1	V.DWN.el.39xxxx	Trojan	37,684
4	New	V.DWN.SystemAny	Trojan	33,862
5	New	Trojan.Generic.3268128	Trojan	27,094
6	↑1	V.WOM.Conficker	Worm	23,719
7	↑3	S.SPY.OnlineGames-H	Spyware	23,523
8	↑1	H.HJK.SearchPack	Hijacker	20,711
9	New	S.SPY,WoWar	Spyware	19,805
10	New	Exploit.Cosmu.A	Exploit	15,067
11	New	Trojan.AutorunINF.Gen	Trojan	13,352
12	↓7	V.DWN.VB.paran	Trojan	13,245
13	New	Trojan.Generic.3265382	Trojan	12,164
14	-	Win32.Virtob.6.Gen	Virus	11,657
15	New	Trojan.Generic.3316858	Trojan	11,574

※ 자체수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다.

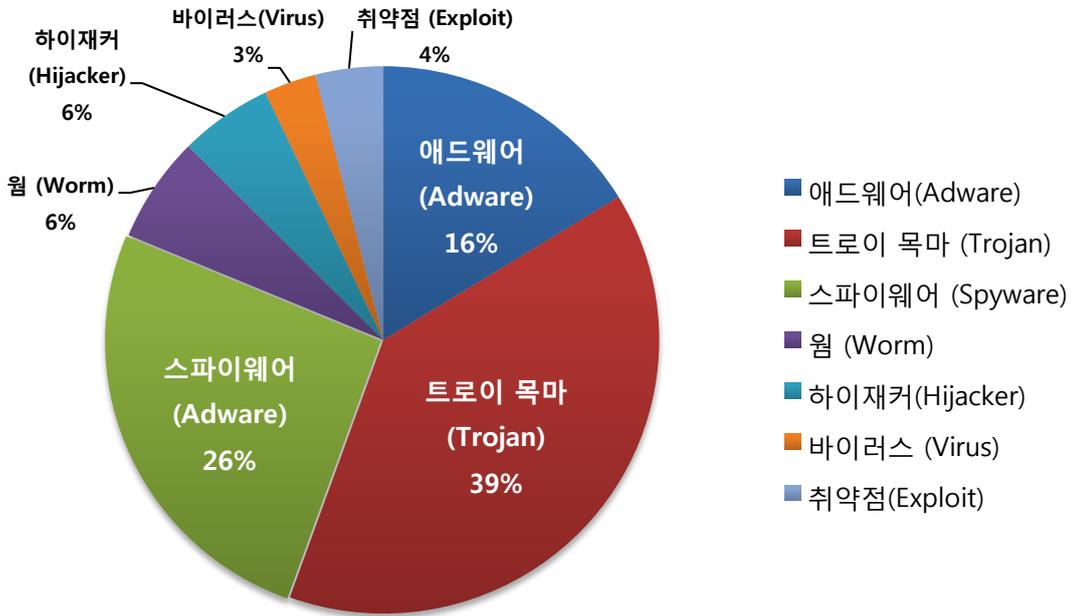
3월의 감염 악성코드 TOP 15는 A.ADV.Admoke이 64,295건으로 TOP 15 중 1위를 차지하였으며, S.SPY.Lineag-GLG이 54,384건으로 2위, V.DWN.el.39xxx이 37,684건으로 3위를 차지하였다.

이외에도 3월에 새로 Top 15에 진입한 악성코드는 7종이다.

이번 달의 특이사항은 3월 10일에 공개된 CVE-2010-0806 관련 취약점을 이용한 국내·외 인터넷 사이트의 변조가 많았으며, 그로 인해 변조 스크립트를 탐지하는 Exploit.Cosmu.A이 새로 순위 건에 진입하였고, 변조된 스크립트에서 다운로드 되는 S.SPY.OnlineGames-H, S.SPY.Lineag-GLG, S.SPY.WoWar 등이 높은 감염 비율을 나타내고 있다.

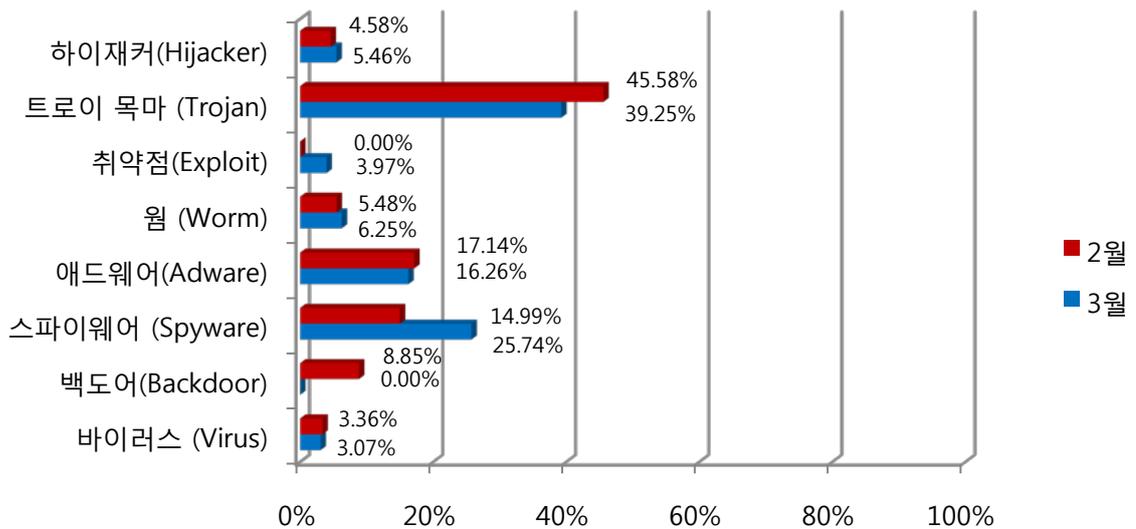


## (2) 카테고리별 악성코드 유형



악성코드 유형별 비율은 트로이 목마(Trojan)가 39%로 가장 많은 비율을 차지하고, 애드웨어(Adware)가 16%, 스파이웨어(Spyware)가 26%의 비율을 각각 차지하고 있다. 이번에 39%의 가장 높은 비율을 차지한 트로이목마(Trojan)는 보안이 취약한 웹 사이트에서 유포된 경우가 많이 발견되었다.

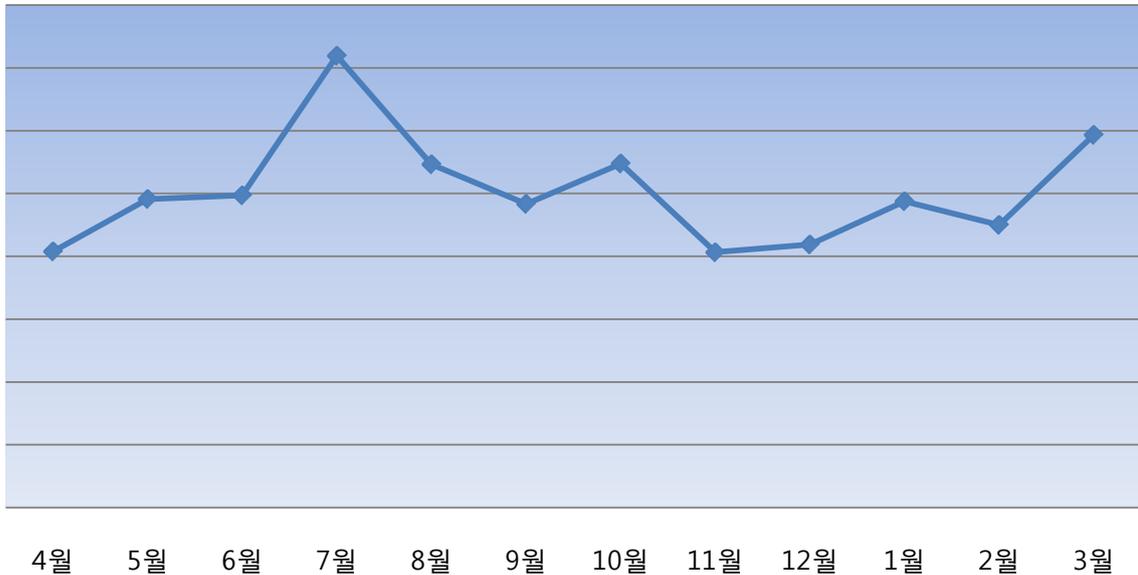
## (3) 카테고리별 악성코드 비율 전월 비교



카테고리별 악성코드 비율을 전월과 비교하면, Exploit.Cosmu.A의 감염 증가로 인해 취약점(Exploit)이 비율이 약 4%정도 증가하였고, 변조된 웹사이트에서 다운로드 되는 악성파일로 인해 스파이웨어(Spyware) 또한 약 10% 이상 증가하였다.

#### (4) 월별 피해 신고 추이

[2009년 4월 ~ 2010년 3월]

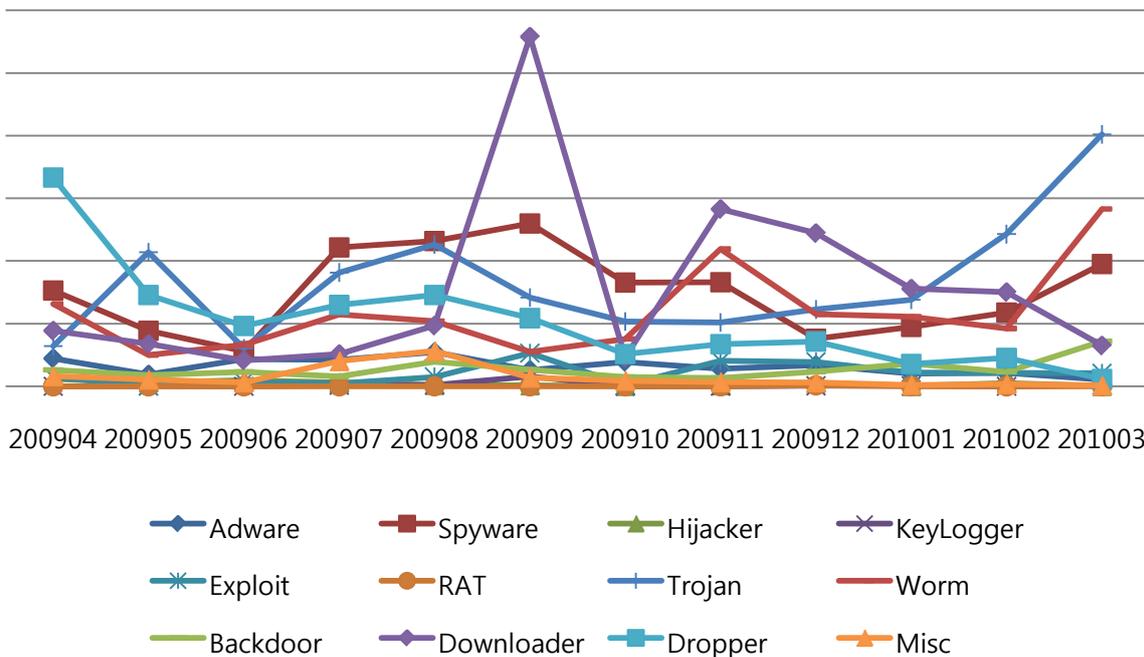


※ 알약 사용자의 신고를 합산해서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프이다. 3월의 경우 전달보다 신고 건수가 증가했으며 새로운 취약점을 통한 공격 및 악성코드 증가로 인한 요인으로 판단된다.

#### (5) 월별 악성코드 DB 등록 추이

[2009년 04월 ~ 2010년 3월]



Part I 3월의 악성코드 통계

2. 악성코드 이슈 분석 - “보호받는 시스템 DLL 파일을 감염시키는 악성코드”

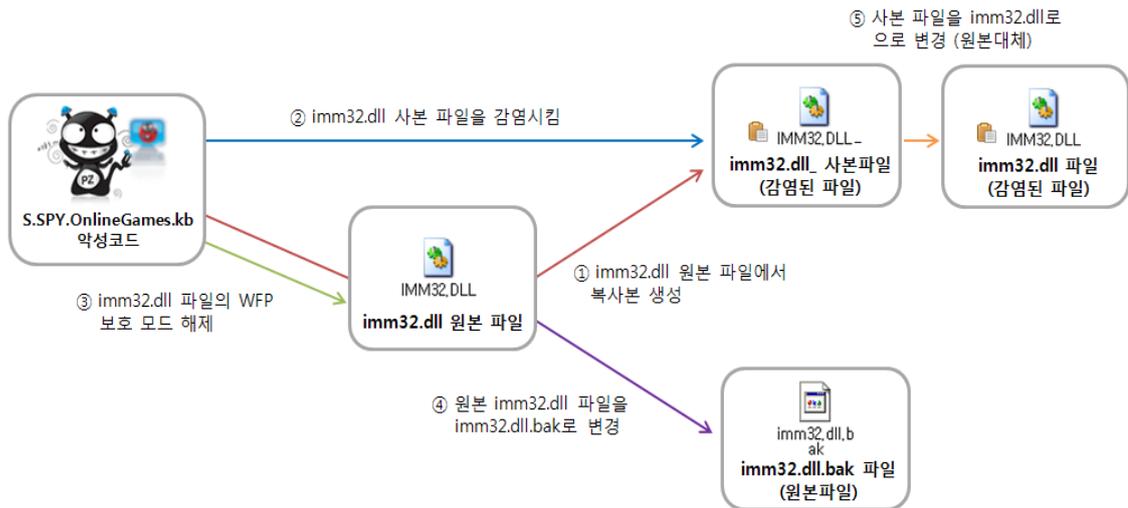
최근의 악성코드는 시스템 DLL 파일을 주목하기 시작했다.

시스템 DLL 을 감염시키면 프로세스가 생성되었을 때마다 해당 DLL 이 로드(Load)되 결국에는 악성코드가 실행될 수 있기 때문이다.

이렇게 좋은 타겟(Target)이 또 어디 있겠는가!

하지만, 윈도우 운영체제는 WFP(Windows File Protection)라는 기술을 사용해 시스템 파일을 보호하므로 악성코드가 시스템 파일을 감염시키기 위해서는 약간의 트릭이 필요하다. S.SPY.OnlineGames.kb 악성코드의 경우 Undocumented API 를 사용하여 WFP 를 우회하며 아래의 과정을 통해 감염시킨다.

- S.SPY.OnlineGames.kb WFP 우회 및 감염 과정 -



- ① Imm32.dll 원본 파일에서 복사본 생성(imm32.dll\_)
- ② Imm32.dll 사본 파일(imm32.dll\_)을 감염시킴
- ③ Imm32.dll 파일의 WFP 보호모드 해제
- ④ 원본 imm32.dll 파일을 imm32.dll.bak로 변경
- ⑤ 사본 파일(imm32.dll\_)을 imm32dll으로 변경(원본대체)

간단히 정리하자면 원본을 직접 변경하거나 삭제 후 다시 생성하는 것이 아닌, 사본을 만든 후 감염된 사본 파일을 원본과 대체하는 방식이다.

영화를 보면 스파이가 건물에 들어갈 때 security system을 bypass하기 위해 전력을 끊는 장면이 나온다. 일단 스파이는 건물 안으로 들어가는 것이 가장 중요하기 때문이다.

위의 방법도 이와 비슷한 방법이라고 볼 수 있다.

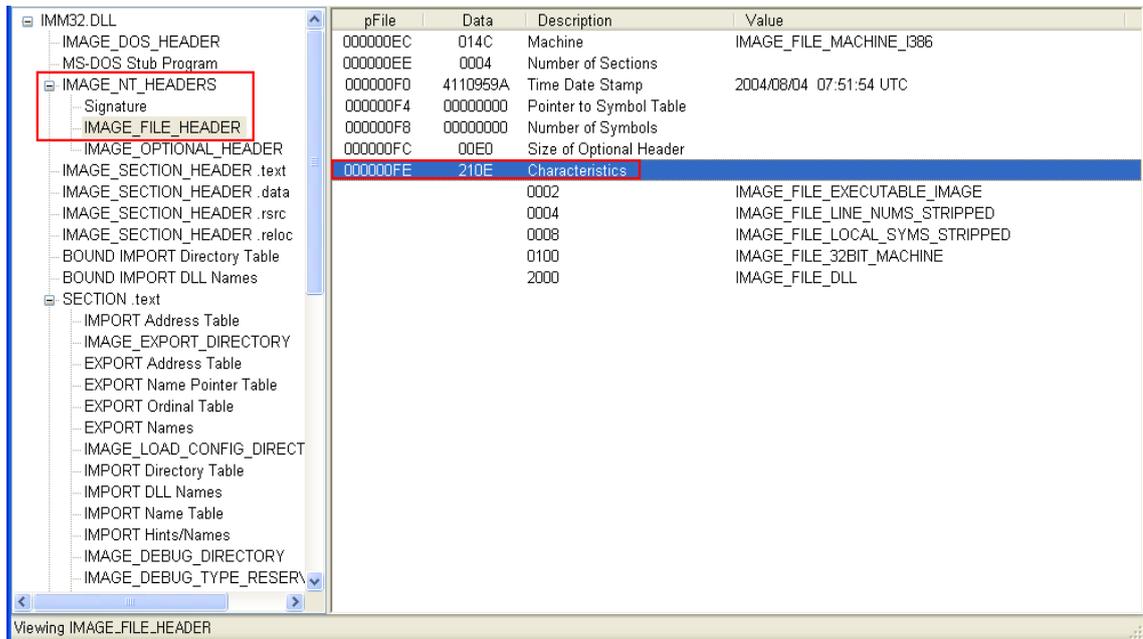
WPF는 기본적으로 이벤트를 감시한다. 이벤트를 잠시 동안 무력화 시키고 그 사이에 파일을 변경시킨다. 그 뒤 security system이 다시 동작하더라도 이미 스파이는 건물로 진입한 후이다. 만약 dllcache에 있는 파일과 시스템 DLL의 무결성을 주기적으로 체크하는 방식이라면 바로 탐지가 가능하다.

또 다른 재미있는 특징은 하나의 파일을 DLL과 EXE로 다룬다는 것이다. 파일 헤더의 IMAGE\_FILE\_HEADER.Characteristics를 0x210e로 바꾼다. 0x210e는 실행 가능한 DLL 파일이라는 뜻이고, 이는 EXE 파일을 DLL로 바꾸는 기능을 한다. 윈도우 PE 로더는 해당 파일이 EXE인지 DLL인지를 파일 헤더의 IMAGE\_FILE\_HEADER.Characteristics로 판단한다.

그러므로 이 값만 바꿔주면 EXE ⇔ DLL로의 변환이 자유롭다.

마치 암수가 한 몸에 존재하는 자웅동체처럼 하나의 파일에 EXE와 DLL가 함께 존재한다. 그래서 하나의 파일을 EXE로 사용할 수도 있고 DLL로 사용할 수도 있다.

단지 2 바이트만 바꾸었을 뿐인데 EXE가 DLL이 되었다. 이것이 자웅동체의 비밀이다.



<그림 : imm32.dll의 IMAGE\_FILE\_HEADER.Characteristics 정보>

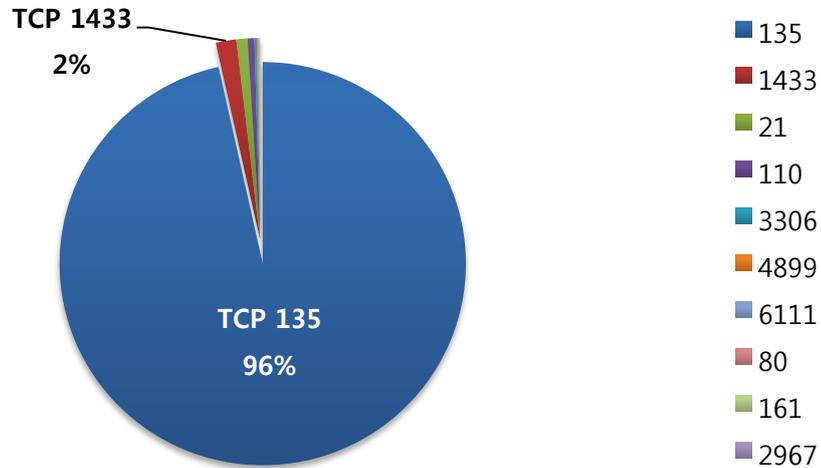
S.SPY.OnlineGames.kb는 (주)네오플에서 제작한 던전애파이터의 계정 정보(ID/패스워드)를 훔치는 스파이웨어(Spyware)로써, 시스템 DLL이 악성코드의 타겟(Target)이 되고 있으며, 감염시키는 imm32.dll은 악성 DLL 파일을 로드 하는 역할만 하기 때문에 해당 DLL 파일만 삭제하면 되지만, 더욱 정교해지고 많은 기능을 사용하는 악성코드가 나온다면 시스템에 큰 피해를 입힐 수 있을 것이다.

마지막으로 일반 PC 사용자는 S.SPY.OnlineGames.kb를 직접 치료를 하는 것이 매우 어려운 관계로 알약 같은 최신의 백신을 사용해 치료하는 것을 권장한다.

Part I 3월의 악성코드 통계

3. 허니팟/트래픽 분석

(1) 상위 Top 10 포트

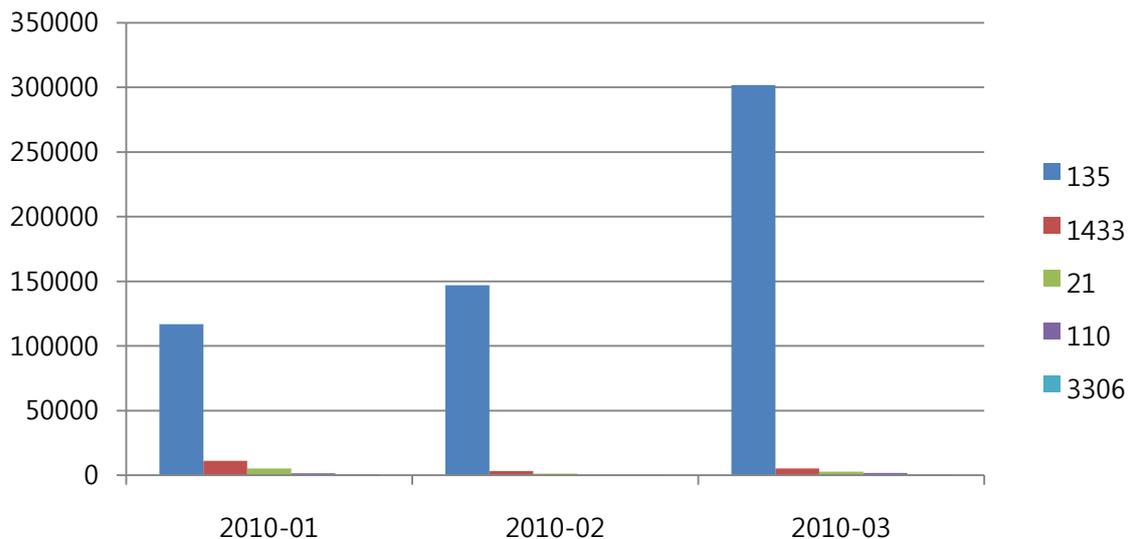


3월에는 여전히 TCP 135번 트래픽이 대부분을 차지하고 있으며, TCP 1433(SQL) 관련 포트 트래픽은 2%, 나머지 포트를 통한 트래픽이 소량 수집되었다.

주로 TCP 135번의 트래픽은 악성 봇넷(Botnet)에 참여하는 좀비 PC에서 추가 감염 PC를 확보하기 위한 목적이며, 윈도우의 최신 보안 패치 설치, 특수문자와 영문자, 숫자들을 조합한 정교한 비밀번호와 방화벽 사용으로 악성 트래픽으로부터 PC를 안전하게 보호할 수 있다.

(2) 상위 Top 5 포트 월별 추이

[2010년 1월 ~ 2010년 3월]

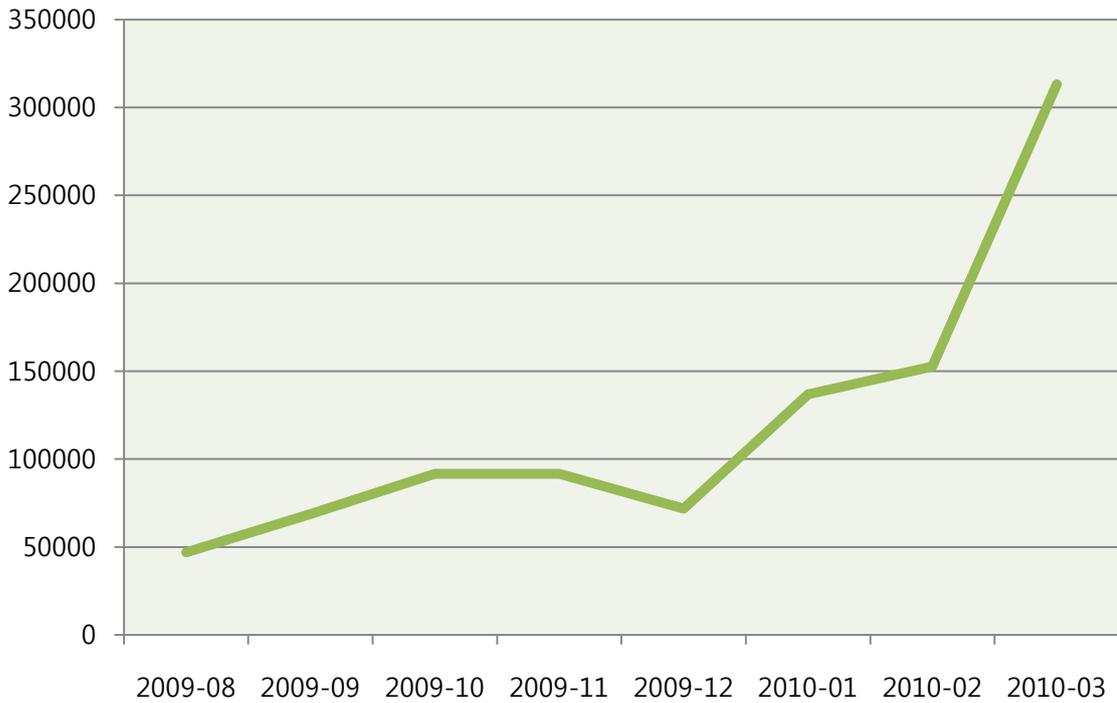


135 번 포트를 통한 트래픽이 1월부터 3월까지 급증세를 보이고 있으며, 1433 포트의 경우 감소 추세를 보이고 있다.

기존에 설치된 악성코드가 자동화된 공격을 시도하거나 봇넷(Botnet)에 의한 공격 트래픽과 FTP 나 POP 서버 등 계정이 필요한 포트에 사전 대입방식으로 계정 탈취를 노리는 트래픽이 주를 이루어 지난달과 차이는 거의 없으나 트래픽의 빈도가 2 배 이상 증가 했다.

### (3) 악성 트래픽 유입 추이

[2009년 8월 ~ 2010년 03월]



악성 트래픽이 지속적으로 증가하는 추이를 보이고 있으며, 마이크로소프트의 보안 패치뿐만 아니라 Acrobat Reader(PDF), Flash (SWF) 등 많이 사용되고 있는 소프트웨어의 보안업데이트도 신경 써야 한다.

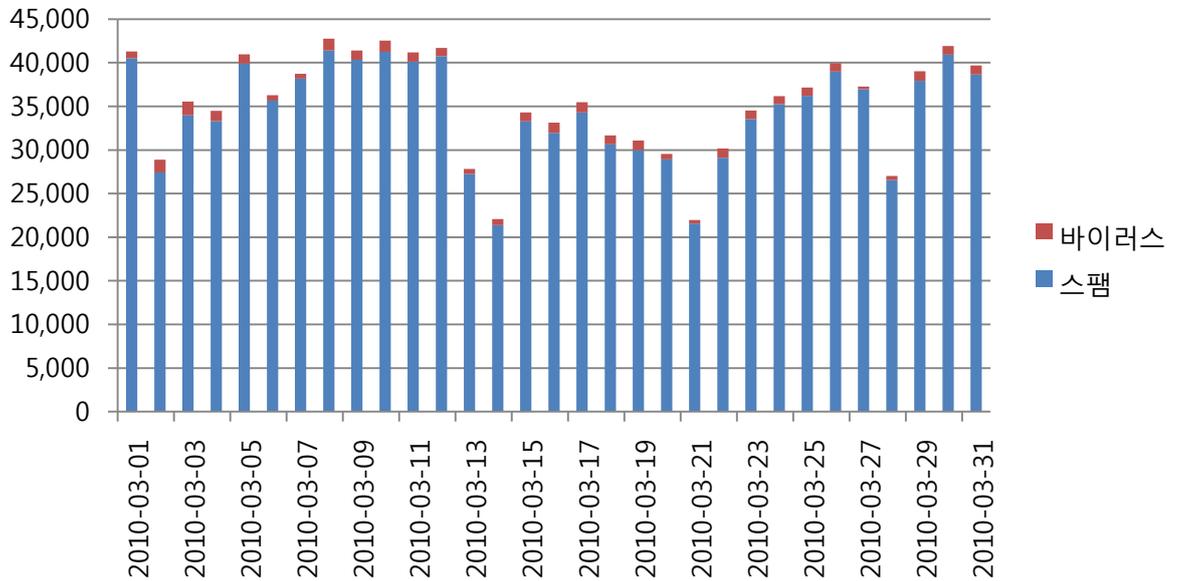
일반 PC 사용자 입장에서 매번 스스로 찾아서 업데이트 하는 것이 어렵다면 해당 프로그램의 자동 업데이트 기능이나 팝업 알림을 사용해 업데이트하는 것을 권장한다.



Part I 3월의 악성코드 통계

3. 스팸 메일 분석

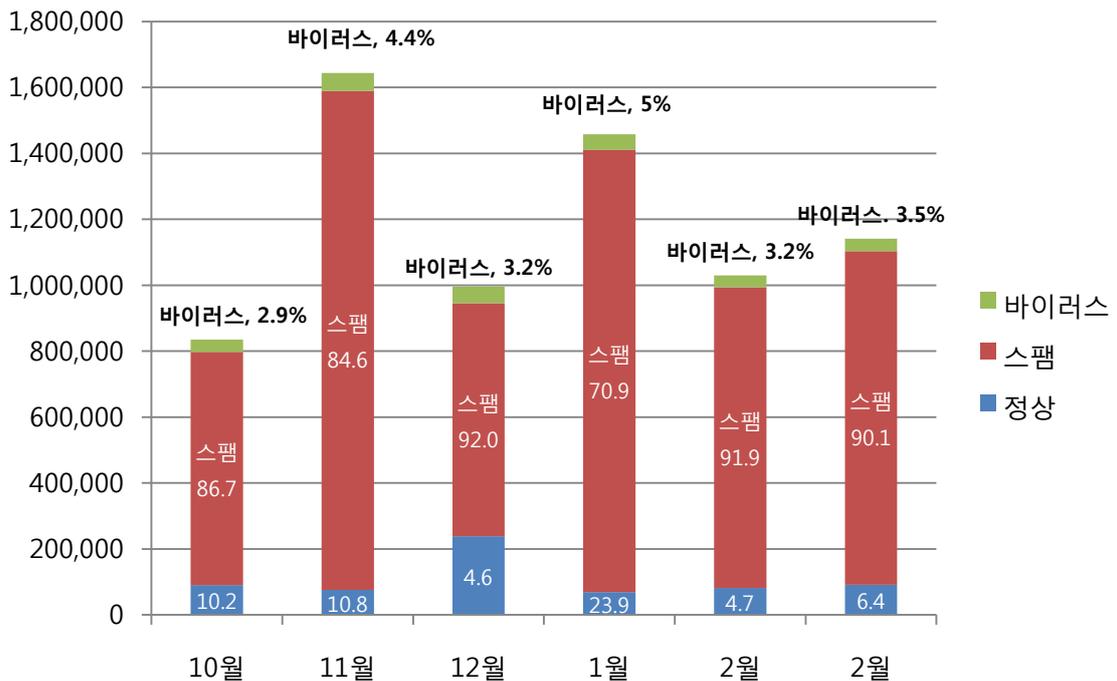
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 수신된 악성코드 첨부, 스팸메일의 개수를 나타낸 그래프이다. 3월의 경우 스팸메일과 악성코드가 첨부된 메일 발송이 전달에 비해 소폭 증가하였다.

(2) 월별 통계 현황

[2009년 10월 ~ 2010년 3월]



월별 통계 현황은 악성코드 첨부 및 스팸메일이 전체메일에서 차지하는 비율을 나타내는 그래프이다.

전체 메일 중 정상 메일이 6.4%를 차지하며, 스팸 메일은 가장 많은 90.1%, 바이러스 메일은 3.5%를 차지하였다. 2월에 비해 스팸메일이 약 1.8% 증가하였으며, 바이러스 메일 또한 약 0.3% 증가하였다.

### (3) 스팸 메일 내의 악성코드 현황

[2010년 3월 1일 ~ 2010년 3월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Virut-T	12,920	43.82%
2	W32/MyDoom-H	4,359	14.79%
3	Mal/ZipMal-B	3,951	13.40%
4	W32/Mytob-C	2,300	7.80%
5	VPS-090709-DDoS-2	2,152	7.30%
6	Troj/CryptBx-ZP	752	2.55%
7	W32/Sality-I	486	1.65%
8	W32/Vetor-A	320	1.09%
9	W32/MyDoom-Gen	308	1.04%
10	Troj/BredoZp-S	211	0.72%

스팸 메일 내의 악성코드 현황은 3월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프이다. 현재 W32/Virut-T이 43.82%로 계속 1위를 차지하고 있다.

2위는 14.79%를 차지한 W32/MyDoom-H, 3위는 13.40%를 차지한 Mal/ZipMal-B이다.

특히, 3월달에는 브레도랩 웜(Bredolab Worm)에서 발생된 스팸 메일들이 지속적으로 나타나 전파를 위한 메일 발송이 현재도 매우 활발함을 알 수 있다.



Part II 3월의 이슈 돋보기

1. 3월의 보안 이슈

2월에는 대한민국 SW 기업 경쟁력 대상에서 보호/보안 SW 부문 최우수상 수상, 이스트소프트 미주 법인 설립, 설 명절을 앞두고 브레도랩 악성코드 확산, 밴쿠버 올림픽과 김연아의 인기를 틈탄 가짜 백신 유포 기승, SNS 서비스를 통한 기업 해킹 전년 대비 70% 이상 증가 소식 등 다양한 보안 이슈들이 많았습니다.

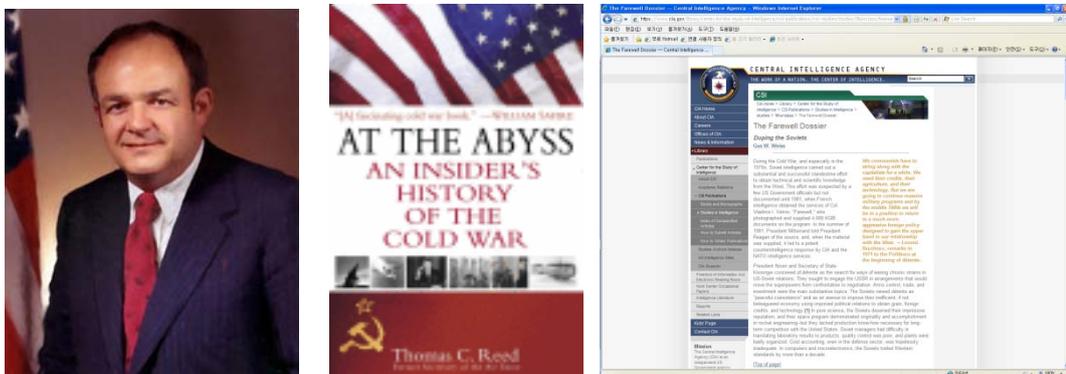
• 소련의 붕괴? 미국의 트로이목마 악성코드 때문?

소련과 미국과의 냉전이 한창이었던 시절 전세계의 40%를 차지할 만큼 엄청난 천연가스매장량을 자랑하는 소련이 천연가스를 수출, 이용하기 위해 시베리아 횡단 파이프 수송관건설 계획을 세웠습니다.

하지만, 파이프 수송관도 원활한 천연가스 공급을 위해서는 반드시 소프트웨어를 통해 자동 제어를 해야 되나 소련은 이러한 소프트웨어 개발 기술을 가지고 있지 못했습니다. 이에 소련은 KGB 요원들을 캐나다에 위치한 미국의 소프트웨어 개발 회사에 위장 취업해 자동 제어 관련 소프트웨어를 입수하여 노력하였고 미국은 1982년 1월 3일에 트로이목마가 탑재된 자동 제어 소프트웨어를 의도적으로 소련에 유출시켰습니다.

그 후 소련은 유출한 소프트웨어를 활용해 천연가스 파이프 수송관을 건설, 운영해왔지만 1982년 6월 30일 미국의 트로이목마 악성코드에 의해 수송관이 폭발하게 되었고, 수출 중단으로 인한 엄청난 경제적 손실로 1986년에 개방과 개혁 노선으로 체제 변경, 1991년 12월 25일에는 결국 소련이 붕괴하게 됩니다.

그 당시 미국의 레이건 대통령의 주재로 열린 긴급회의에서 와이즈 박사가 파이프 수송관 소프트웨어를 의도적으로 유출하는 대신 그 소프트웨어 안에 트로이목마를 심어놓자고 제안하였고 대통령이 이를 받아들여 소련이 소프트웨어를 빼내도록 유도했습니다. 트로이목마는 파이프 펌프의 속도와 밸브가 치명적으로 오작동하도록 설계되었으며 20년이 지난 CIA의 문서와 미국의 前 국방장관 토마스 리드(Thomas C. Reed)의 "At The Abyss" 책이 출간되면서 사건의 진실이 자세하게 밝혀지게 되었습니다.



<미국 前국방 장관 토마스 리드(Thomas C. Reed) 사진 및 저서, 美 CIA 공개 문서>

### • 스타크래프트2 해킹 버전 악성코드가 드글드글~

1990년 말 국내에 인터넷 돌풍과 PC방의 급격한 성장을 일으킨 블리자드(Blizzard)의 스타크래프트가 새로운 베타 버전을 출시하며 비공개 테스트에 돌입했습니다.

국내의 게이머들의 뜨거운 관심 속에 벌써부터 스타크래프트2 베타 해킹 버전이 P2P와 웹하드를 통해 공유되고 있는 실정입니다.

현재 해킹 버전의 경우 스타크래프트2와 전혀 관계 없는 가짜 파일이나 악성코드를 심어놓고 배포하는 사례도 자주 발견되고 있어 사용자들의 각별한 주의가 요구됩니다. 또한, 앞으로 스타크래프트2의 인기에 힘입어 시디키(CD-Key)나 계정 유출에 최적화된 악성코드 또한 발견될 가능성이 매우 높으므로 최신 버전의 알약 백신과 실시간 감시를 사용하는 것이 중요합니다.



### • 2년간 32억원 게임머니 빼돌려 호화생활 즐긴 게임 업체 직원 검거

국내의 한 인터넷 게임업체에서 근무하는 직원이 자신이 관리하는 게임의 캐시를 빼돌려 허위 ID 140개로 분산해 관리하다 최근 경찰에 검거되었습니다.

이번에 검거된 직원은 게임머니 32억원을 아이템 거래 사이트를 통해 현금화했으며 이렇게 얻은 돈으로 수입차 구입, 해외여행 등 호화 생활을 즐겼던 것으로 드러났습니다.

이번 사건 역시 그 동안 계속 제기되었던 기업의 내부자 통제 문제로 볼 수 있으며, 게임 회사 뿐만 아니라 다른 기업에서도 충분히 발생할 수 있는 사안이므로 몇 가지 IT 보안 솔루션 구비와 운영에서 끝나는 것이 아닌 내부 직원의 직무분리 및 순환 같은 인적 통제 정책을 함께 실시해야만 앞으로 이러한 유사 사건이 재발되는 것을 막을 수 있을 것입니다.

### • 사장님들~ 정보보호 투자에도 신경 써주세요~

방송통신위원회와 한국인터넷진흥원에서 발표한 "2009년 정보보호 실태조사"에 의하면 2300개 조사 대상 기업 63.6%의 정보보호 투자가 전혀 없는 것으로 나타났습니다.

최근의 개인정보 유출, DDoS 사건 등 여러 기업과 직접적으로 연관된 보안 이슈가 많았지만 경제 침체로 인해 대다수의 기업 정보보호 투자가 미루어진 것으로 보여집니다. 하지만, 정보보호 투자의 경우 이제는 보험적 성격이 아닌 기업의 존폐 여부까지 고려해야 할 만큼 그 중요도가 점점 높아지고 있으며, 최근 개인정보 관련 사건을 판결한 법원의 입장도 최대한의 기업정보보호 의무를 강조하는 방향으로 변화하는 추세입니다.

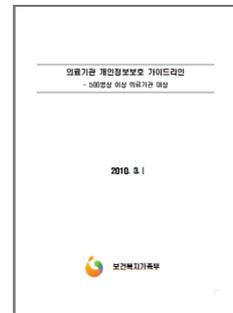
• **대형병원 개인정보보호 가이드라인 배포 시작**

지난 3월 16일 보건복지가족부에서는 500병상 이상의 대형병원을 대상으로 한 개인정보보호 가이드라인을 배포하기 시작했습니다.

이번 가이드라인에서는 500명 이상의 기관은 개인정보보호 실무책임자 또는 보안실무책임자 중 1명을 정규적으로 채용하고, 1000병상 이상의 기관은 개인정보보호 실무책임자와 보안실무책임자 각각 1명을 두되 필요에 따라 1명은 아웃소싱도 가능합니다.

이외에도 환자 진료를 통해 얻은 개인정보가 안전하게 보호될 수 있도록 사용자 인증, 접근권한, 네트워크, 로그 관리, 침해사고 예방 및 대응에 관련된 기술적, 물리적 세부 지침이 담겨져 있습니다.

개인정보보호와 환자 개인의 정보에 대한 중요성이 점점 강화되고 있는 시대적 상황에서 앞으로 500병상의 대형병원 뿐만 아니라 중형, 소형 병원 순으로 세부적인 가이드라인 또한 제정될 것으로 보여집니다.



• **빵빵 터지는 기업의 개인정보 유출 사건, 당당히(?) 세계 10위권 안에 진입!**

2008년에는 유명 인터넷 A쇼핑 사이트와 정유업체에서 대량의 개인정보 유출을 넘어 올해 3월 국내 최대 규모의 2,000만 개인정보 유출 사건이 연이어 발생했습니다.

전국민의 반에 달하는 개인정보가 해커에게 유출되었을 것으로 알려진 이번 사건이 전 세계 개인정보 유출 사고 순위 10위안에 당당히 진입할 수 있을 것 같습니다.

2008년 대규모 개인정보 유출 사고 이후에 바로 여러 기업들이 과감한 정보보호 투자와 관심을 나타냈다면 올해의 대형 개인정보 유출 사고 또한 충분히 예방 가능했기 때문에 더욱 많은 아쉬움이 남습니다.

**Largest Incidents**

RECORDS	DATE	ORGANIZATIONS
130,000,000	2009-01-20	Heartland Payment Systems
94,000,000	2007-01-17	TJX Companies Inc.
90,000,000	1984-06-01	TRW, Sears Roebuck
76,000,000	2009-10-05	National Archives and Records Administration
40,000,000	2005-06-19	CardSystems, Visa, MasterCard, American Express
30,000,000	2004-06-24	America Online
26,500,000	2006-05-22	U.S. Department of Veterans Affairs
25,000,000	2007-11-20	HM Revenue and Customs, TNT
17,000,000	2008-10-06	T-Mobile, Deutsche Telekom
16,000,000	1986-11-01	Canada Revenue Agency

OSF 화면 캡처.

Part II 3월의 이슈 돋보기

2. 3월의 취약점 이슈

• **Microsoft 3월 정기 보안 업데이트**

Internet Explorer 누적 보안 업데이트와, Windows Movie Maker의 취약점으로 인한 원격 코드 실행 문제점, Microsoft Excel의 취약점으로 인한 원격코드 실행 문제 해결 등을 포함한 3월 정기 보안 업데이트를 발표하였습니다.

<해당 제품>

Microsoft Windows XP, Windows Vista, Windows 7 (MS10-016)

Windows Movie Maker 2.1, 2.6, 6.0

Microsoft Office XP, 2003, Excel Viewer SP1~SP2

Microsoft SharePoint Server 2007 SP1~SP2

<취약점 목록>

MS10-016(980182) : Internet Explorer 누적 보안 업데이트

MS10-016(975561) : Windows Movie Maker의 취약점으로 인한 원격코드 실행 문제점

MS10-017(980150) : Microsoft Excel의 취약점으로 인한 원격코드 실행 문제점

<해결책>

Windows Update를 수행하거나 Microsoft 보안 공지 요약 사이트에서 해당 취약점들의 개별적인 패치 파일을 다운로드 받을 수 있습니다.

한글 : <http://www.microsoft.com/korea/technet/security/Bulletin/ms10-mar.msp>

영문 : <http://www.microsoft.com/technet/security/Bulletin/ms10-mar.msp>

• **VBScript를 이용한 원격코드 실행 취약점(CVE-2010-0483)**

윈도우 2000과 XP, 2003에서 Internet Explorer을 사용하는 도중 F1(도움말)키를 누르도록 유도하는 메시지가 나왔을 때 PC 사용자가 F1 키를 누르면 미리 공격자가 지정한 도움말 파일을 로드해 악성코드를 실행할 수 있는 취약점입니다.

현재 이 취약점은 Microsoft의 공식 패치가 발표되지 않은 제로데이(Zeroday) 상태이며, 본 취약점을 악용한 악성코드 유포가능성이 높으므로 PC 사용자들의 주의가 필요합니다.

<해당 제품>

Windows 2000 Service Pack 4

Windows XP Service Pack 2~3 (64bit CPU 환경 포함)

Windows Server 2003 Service Pack 2 (Itanium, 64bit CPU 환경 포함)

※ Windows Vista/7/2008 시스템은 이번 취약점에 해당되지 않습니다.

<임시 해결책>

- 1) 현재까지 Microsoft의 공식적인 패치가 발표되지 않은 상황이므로 보안이 취약한 웹사이트에는 가급적 방문하지 않습니다.
- 2) Internet Explorer를 사용하는 도중에 F1 키를 누르도록 권유하는 메시지를 보더라도 절대 F1 키를 누르지 않습니다. (중요!)

(예시 메시지 형식)

※ 메시지의 상세 내용은 달라질 수 있으나 아래의 비슷한 형식에 F1를 누르라는 내용이 들어있다면 이번 취약점을 이용한 VBScript로 볼 수 있습니다.



- 3) ACL(Access Control List)에서 winhlp32 (Windows Help System)을 제한 설정합니다.  
명령 프롬프트(cmd)에서 아래의 명령어를 입력합니다.  
echo Y | cacls "%windir%\winhlp32.exe" /E /P everyone:N

※ ACL 설정 후에는 Windows Help System과 도움말 기능이 정상 작동하지 않을 수 있습니다. 복구를 원하는 경우 명령 프롬프트에서 아래의 명령어를 입력합니다.  
echo Y | cacls "%windir%\winhlp32.exe" /E /R everyone

<관련 홈페이지>

<http://www.microsoft.com/technet/security/advisory/981169.msp>

## • Internet Explorer 신규 취약점을 통한 정보유출 취약점

Internet Explorer 6~7 버전의 iepeers.dll 모듈에서 유효하지 않은 포인터 참조로 인해 원격코드가 실행 가능한 취약점이 발견되었습니다.

공격자는 악성 사이트 링크를 통해 공격 사이트에 접속하도록 유도 한 후 악성코드를 실행시킬 수 있습니다.

### <해당 제품>

Microsoft Internet Explorer 6 Service Pack 1 (Win2000, XP, 2003 Server)

Microsoft Internet Explorer 7 (XP, 2003 Server, Vista, 2008 Server)

### <해결책>

Windows Update를 수행하거나 Microsoft 보안 공지 요약 사이트에서 해당 취약점들의 개별적인 패치 파일을 다운로드 받을 수 있습니다.

한글 : <http://www.microsoft.com/korea/technet/security/Bulletin/ms10-018.msp>

영문 : <http://www.microsoft.com/technet/security/Bulletin/ms10-018.msp>

## • 공개 웹게시판 제로보드 XE의 XSS 취약점

국내 PHP 기반의 공개 웹게시판인 제로보드 XE에서 XSS 취약점이 발견되 이를 통한 홈페이지 변조 및 원격실행이 가능하고, 추가적으로 관리자 권한을 획득할 수도 있는 취약점이 발견되었습니다.

### <해당 제품>

제로보드 XE 1.4.0.9 이하 버전

※ 제로보드 XE 1.4.0.10 이상 버전은 해당 취약점으로부터 안전합니다.

### <해결책>

이미 취약한 버전의 제로보드 XE를 운영하고 있는 경우 config.ini.php 파일과 func.inc.php 파일을 운영중인 게시판 config 디렉토리에 설치합니다.

또는, config 폴더의 func.ini.php 파일을 아래와 같이 수정해도 됩니다.

./config/func.inc.php

```
654. $attrs = preg_replace('/(\r|\n| )+on
    (click|dblclick|mousedown|mouseup|mouseover|mouseout|mousemove|keydown|keyup|keypress|load|unload|a
    +([= ]+)/is', ' _on$2=', $attrs);
```

새로 구축하는 홈페이지에서 제로보드를 사용할 경우 제로보드 XE 1.4.0.10 버전을 내려 받아 설치해야 합니다.

### <관련 홈페이지>

<http://www.xpressengine.com/18776625>

Contact us...

**(주)이스트소프트 알약긴급대응팀**

Tel : 02-881-2364

E-mail : [help@alyac.co.kr](mailto:help@alyac.co.kr)

알약사이트 : [www.alyac.co.kr](http://www.alyac.co.kr)

알툴즈 8.0 행정업무용 S/W 선정 기념 이벤트

알툴즈의 새 버전인 알툴즈 8.0이 2010년 상반기 행정업무용 소프트웨어에 선정되었습니다. 이제 공공기관에서도 더욱 업그레이드 된 알툴즈 8.0을 만나보실 수 있습니다. 여러분의 보다 편리한 업무환경을 위해 계속 진화하는 알툴즈가 되겠습니다.

기간: 3월 8일 ~ 5월 14일    대상고객: 100 user 이상 구매하시는 모든 기관

대상제품: 공공기관용 알툴즈통합팩 7.0    내용: 구매 수량 별 경품 및 알툴즈 8.0 라이선스 제공

공공기관용 알툴즈 구매하기 >

2010년 하반기에 알툴즈 통합팩 8.0이 조달등록 되면서 가격이 인상될 예정이오니 이번 이벤트 기간 중에 알툴즈도 저렴하게 구매하시고 경품의 혜택도 놓치지 마세요~

혜택 1. 알툴즈 7.0을 구매 하시면 알툴즈 8.0 라이선스를 드립니다.

혜택 2. 구매수량에 따라 푸짐한 경품을 드립니다.

구매 수량	경 품
1,000 user 이상	울트라씬 노트북
500~ 999 user	27" LCD 모니터
300~ 499 user	E-Book 뷰어
100~ 299 user	외장하드 500GB

상기 경품은 영구사용권 구매 기준입니다. (연간사용권 구매 시 별도 협의)

\* 상품이미지는 실제와 다를 수 있으며 사진공지 없이 변경 될 수 있습니다.