13. 안전한 사이버 환경 구축-II

안동대학교 컴퓨터공학과
차세대 네트워크 연구실

안동대학교
ANDONG NATIONAL UNIVERSITY

목차

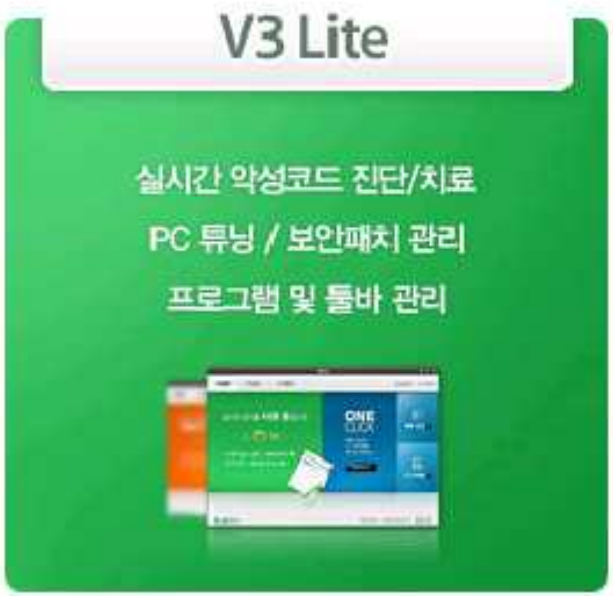
- 백신 프로그램
- 스마트폰의 보안
- 방화벽
- 보안관련 사이트

백신 프로그램

- 악성 소프트웨어를 찾아서 제거하는 기능을 갖춘 컴퓨터 프로그램으로 앤티바이러스 소프트웨어라고도 한다.
- 원래 목적은 바이러스를 제거하는 것이었으나 현재는 피싱 공격, 트로이 목마, 웜 등의 다양한 악성코드를 처리한다.
- 백신 프로그램의 종류
  - 개인 사용자는 무료, 기업이나 공공기관 및 PC방은 유료인 프로그램
    - 안철수 연구소의 V3 Lite(http://www.ahnlab.com)
    - 이스트소프트(ESTsoft)의 알약(http://alyac.altools.co.kr/)
    - 네이버백신(http://security.naver.com)
  - 유료 프로그램
    - Avast 안티바이러스(http://www.avast.co.kr/)
    - 시만텍의 노튼 안티바이러스(http://kr.norton.com)

안철수 연구소의 V3(Vaccine 3)

- V3 Lite(무료), V3 365 클리닉(유료)
  - 바이러스, 트로이목마, 스파이웨어, 피싱 등 다양한 보안 위협에 효과적으로 대응하는 국산 TS(Total Security) 통합 엔진 장착
  - 가볍고 용량이 적음
  - 2011년 8월의 'VB100' 바이러스 백신 프로그램 성능평가: 중상위권 유지
  - 지원사양: Win 2000/XP/VISTA/7, …



V3 설치

- V3 Lite - 안철수연구소(http://www.ahnlab.com)

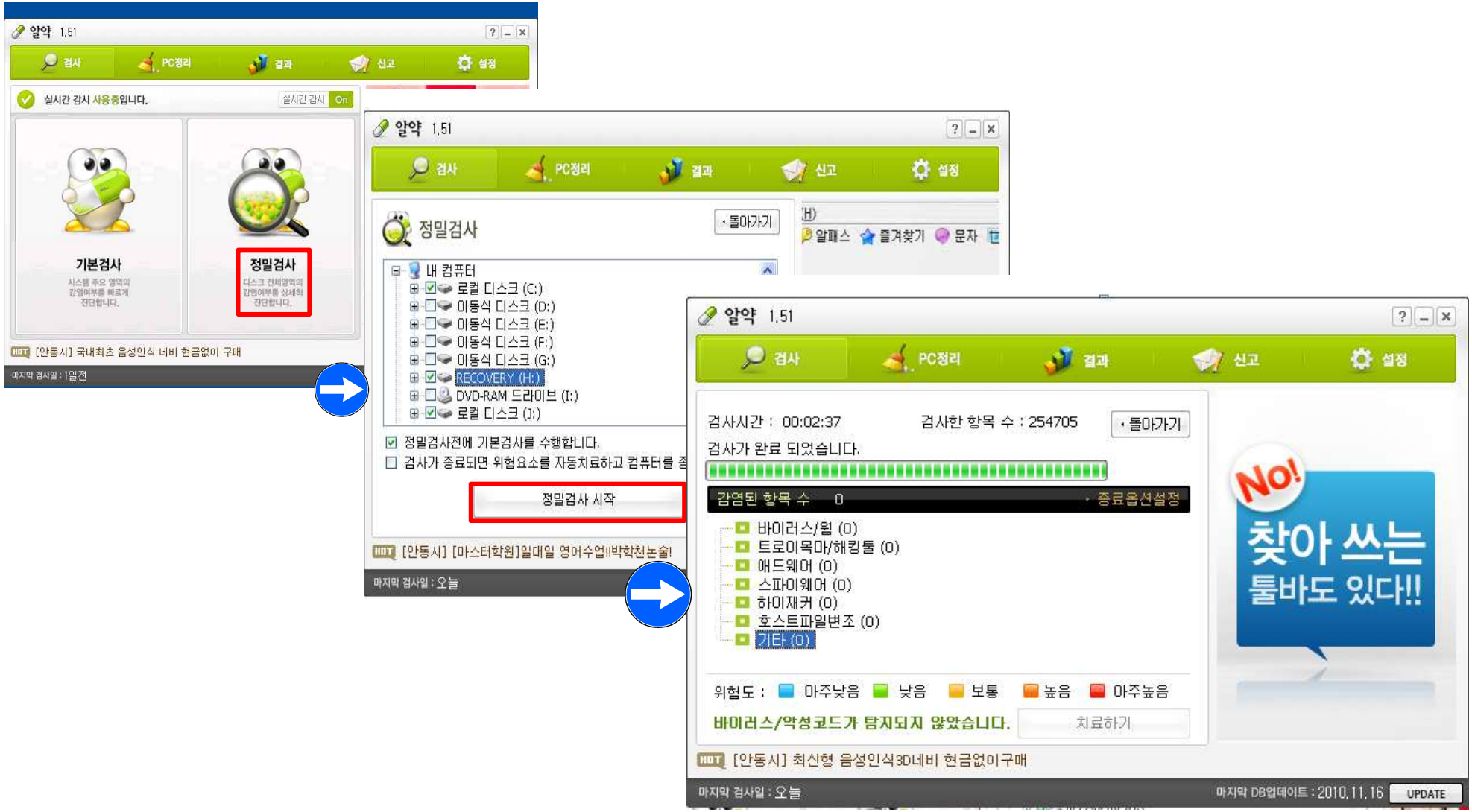
V3 실행


V3 Lite
HOME
PC검사
PC튜닝
환경 설정 | 고객센터
PC검사
검역소
로그보기
· 실시간 검사 : 사용 중
· 마지막 검사 날짜 : 2010-11-13 (오늘)
빠른 검사는 감염되기 쉬운 영역만을 프로그램 자체 설정에 따라 검사하고 치료합
정밀 검사는 사용자가 원하는 옵션을 선택하여 검사할 수 있습니다.
빠른 검사
정밀 검사
안철수연구소 인터넷 관련 상담은 한국인터넷진흥원 e클린센터 ☎118
엔진 버전 : 2010,
V3 Lite
HOME
PC검사
PC튜닝
환경 설정 | 고객센터
내 컴퓨터
로컬 디스크 (C:)
로컬 디스크 (D:)
My Disc (E:)
DVD 드라이브 (H:)
사전 검사 영역 선택
메모리
프로세스
시작 프로그램
부트 영역
스파이웨어 감염 위험이 높은 영역
유해 가능 프로그램
검사 파일 형식 선택
모든 파일
감염되기 쉬운 파일
실행 파일
매크로 파일
스크립트 파일
사용자 지정 확장자 파일
압축 파일
고급 설정
기본 값
검사 시작
취소
안철수연구소 인터넷 관련 상담은 한국인터넷진흥원 e클린센터 ☎118
엔진 버전 : 2010,11,14,00
업데이트

알약

- 이스트소프트(ESTsoft)가 개발한 바이러스 검사 소프트웨어
- 루마니아에서 개발된 비트디펜더(BitDefender)와 영국의 소포스 엔진 사용
  - 2011년 8월의 'AV Comparatives' 바이러스 백신 프로그램 성능평가: 최우수 제품으로 선정(5위)
- 지원사양: Windows 2000/XP/Vista/7, …

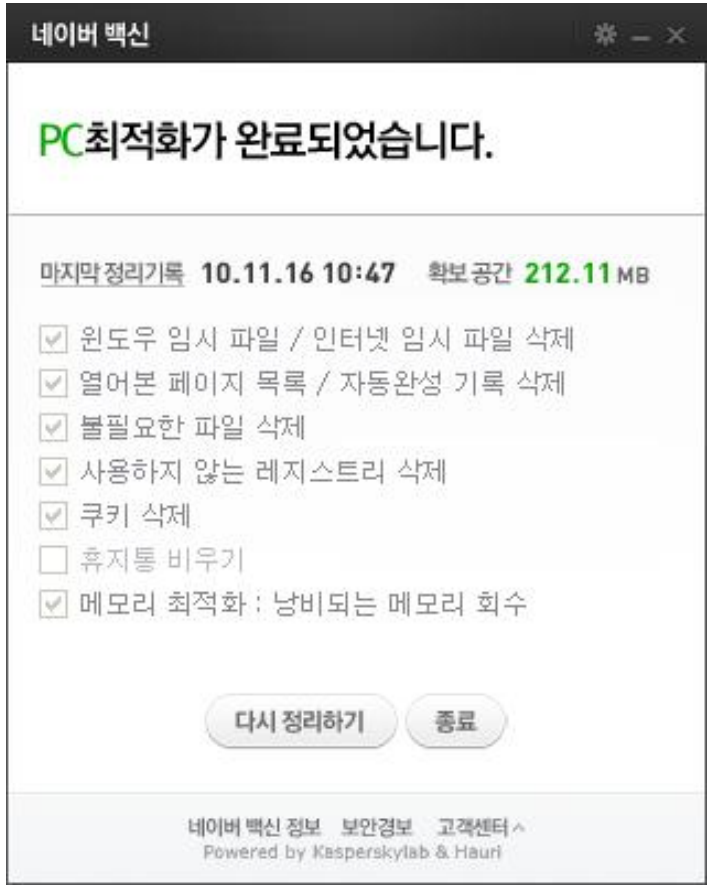
알약 실행


알약 1.51
검사
PC정리
결과
신고
설정
실시간 감시 사용중입니다.
실시간 감시 On
기본검사
시스템 주요 영역의 감염여부를 빠르게 진단합니다.
정밀검사
디스크 전체영역의 감염여부를 상세히 진단합니다.
[안동시] 국내최초 음성인식 네비 현금없이 구매
마지막 검사일 : 1일전
정밀검사
돌아가기
내 컴퓨터
로컬 디스크 (C:)
이동식 디스크 (D:)
이동식 디스크 (E:)
이동식 디스크 (F:)
이동식 디스크 (G:)
RECOVERY (H:)
DVD-RAM 드라이브 (I:)
로컬 디스크 (J:)
정밀검사전에 기본검사를 수행합니다.
검사가 종료되면 위험요소를 자동치료하고 컴퓨터를 종
정밀검사 시작
[안동시] [마스터학원]일대일 영어수업!!박학천논술!
마지막 검사일 : 오늘
검사시간 : 00:02:37
검사한 항목 수 : 254705
검사가 완료 되었습니다.
감염된 항목 수 0
종료옵션설정
바이러스/웜 (0)
트로이목마/해킹툴 (0)
애드웨어 (0)
스파이웨어 (0)
하이재커 (0)
호스트파일변조 (0)
기타 (0)
위험도 : 아주낮음 낮음 보통 높음 아주높음
바이러스/악성코드가 탐지되지 않았습니다.
치료하기
No!
찾아 쓰는
툴바도 있다!!
[안동시] 최신형 음성인식3D네비 현금없이구매
마지막 검사일 : 오늘
마지막 DB업데이트 : 2010.11.16
UPDATE

네이버 백신

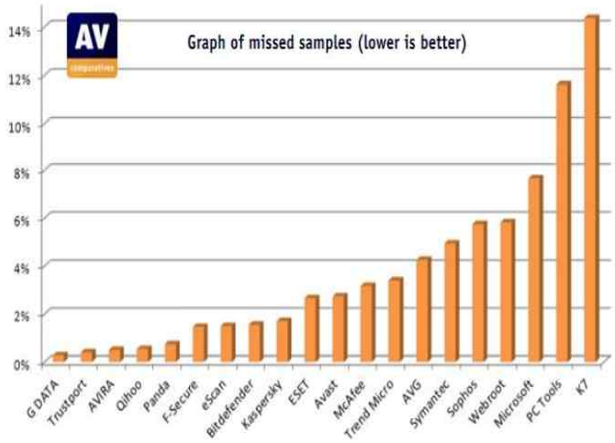
- 포털사이트 네이버에서 무료로 제공하는 백신 소프트웨어
- 러시아의 카스퍼스키 엔진과 한국의 하우리 엔진 사용
  - 2011년 8월의 'AV Comparatives' 바이러스 백신 프로그램 성능평가: 최우수 제품으로 선정(6위)
- 지원 사양: Win 2000/ XP/VISTA/7,…

네이버 백신의 PC 최적화



AV Comparatives 성능평가(2011.8)

❑ 탐지 누락율



❑ 종합평가

AWARDS (based on detection rates and false alarms)	PRODUCTS
최우수 제품 AV ADVANCED+ ★★★ ON DEMAND DETECTION TEST comparatives AUG 2011	✓ G DATA ✓ AVIRA ✓ Panda ✓ F-Secure ✓ Bitdefender ✓ Kaspersky ✓ ESET ✓ Avast ✓ McAfee ✓ Trend Micro
우수제품 AV ADVANCED ★★ ON DEMAND DETECTION TEST comparatives AUG 2011	✓ Trustport* ✓ Qihoo* ✓ eScan* ✓ AVG* ✓ Symantec* ✓ Microsoft

❑ 탐지율(높을수록 좋음)

1.	G DATA	99.7%
2.	Trustport	99.6%
3.	AVIRA, Qihoo	99.5%
4.	Panda	99.3%
5.	F-Secure, eScan	98.5%
6.	Bitdefender	98.4%
7.	Kaspersky	98.3%
8.	ESET, Avast	97.3%
9.	McAfee	96.8%
10.	Trend Micro	96.6%
11.	AVG	95.7%
12.	Symantec	95.1%
13.	Microsoft	92.3%
14.	PC Tools	88.4%
15.	K7	85.6%

❑ 오진율(적을수록 좋음)

1.	McAfee	0
2.	Kaspersky, Microsoft, Panda	1
3.	ESET	3
4.	F-Secure, Trend Micro	6
5.	Bitdefender	8
6.	Avast	10
7.	AVIRA	11
8.	G DATA	14
9.	Sophos, Webroot	16
10.	K7	23
11.	Qihoo	25
12.	eScan	29
13.	PC Tools	45
14.	AVG	51
15.	Symantec	57
16.	TrustPort	59

* 오진율이 높은 프로그램: 정상적인 프로그램을 악성코드로 진단하여 치료 또는 삭제를 권유함

테스트에 투입된 Worms(웜바이러스) 9,707개, Backdoores/Bots(백도어/봇) 20,502개, Trojans(트로이목마) 170,352, other malware/viruses(기타 악성코드/바이러스) 5,482개

AV Comparatives 성능평가(2010.2)

- Av-Comparative(2010년 2월)의 국외 20개 프로그램 평가

1. G DATA AntiVirus 2010 99.6%
2. AVIRA AntiVir Premium 9 99.3%
3. Panda Antivirus Pro 2010 99.2%
4. TrustPort Antivirus 2010 99.1%
5. McAfee AntiVirus Plus 2010 98.9%
6. PC Tools Spyware Doctor with AV 7.0 98.7%
7. Symantec Norton Anti-Virus 2010 98.6%
8. F-Secure Anti-Virus 2010 97.8%
9. ESET NOD32 Anti-Virus 4.0 97.7%
10. BitDefender Antivirus 2010 97.5%
11. eScan Anti-Virus 10 97.5%
12. avast! Free Antivirus 5.0 97.3%
13. Kaspersky Anti-Virus 2010 97.1%
14. K7 TotalSecurity 10.0 96.4%
15. Microsoft Security Essentials 1.0 96.3%
16. AVG Anti-Virus 9.0 94.2%
17. Sophos Anti-Virus 9.0 93.7%
18. Norman Antivirus & Anti-Spyware 7.30 92.7%
19. Trend Micro AntiVirus plus AntiSpyware 2010 90.7%
20. Kingsoft Antivirus 2010 81.8%

스마트폰의 보안

- 손안의 PC로 불리는 스마트폰은 PC가 안고 있는 보안 위험을 그대로 안고 있다.
- 아이폰과 안드로이드 운영체제가 폭발적인 성장세를 보이면서 악성코드도 덩달아 급증세를 나타내고 있으며, 금전적인 이득을 노리는 악성코드가 대부분을 차지한다.
- 2010년 국가정보보호백서에 따르면 2009년 상반기에 발견된 전 세계 스마트폰 악성코드는 520여종에 이른다.

스마트폰의 보안 피해사례

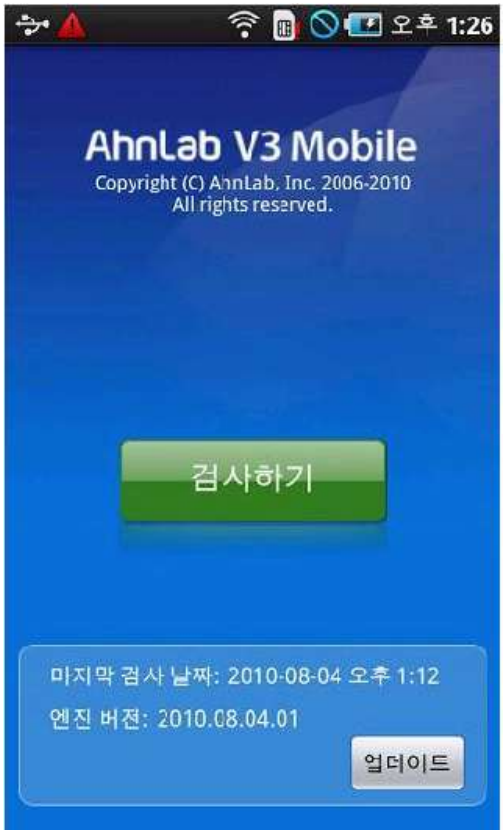
- 카스퍼스키랩은 스마트폰 최초의 트로이목마 악성코드가 2010년 8월 러시아에서 발견됐다고 밝혔다.
  - 겉으로는 정상적인 동영상 재생 프로그램으로 보이지만 안드로이드 운영체제 기반의 스마트폰에 설치하면 사용자 몰래 값비싼 유료 서비스 번호로 문자메시지를 보내 통신요금을 과다하게 청구하는 프로그램이다.

- 국내에서는 2010년 4월엔 사용자 몰래 50초 간격으로 국제전화를 걸도록 하는 악성코드인 트레드다이얼이 등장해 155건의 감염 사례가 발생한 바 있다.

- 2010년 미국에선 휴대폰 배경화면을 마음대로 바꿀 수 있게 해주는 프로그램을 내려받은 수백만 명이 텍스트 문자와 사이트 방문기록을 자신도 모르는 사이에 해커에게 전송당함.

스마트폰의 보안 프로그램

- 안철수 연구소의 V3 Mobile
- 스마트폰지킴이: 스마트폰 내의 유해 어플들에 대한 검사 및 차단
- 맥어피(McAfee): 각종 바이러스와 스파이웨어 진단 및 치료



스마트폰 지킴이의 실행

❑ 스마트폰의 유해 어플 분류

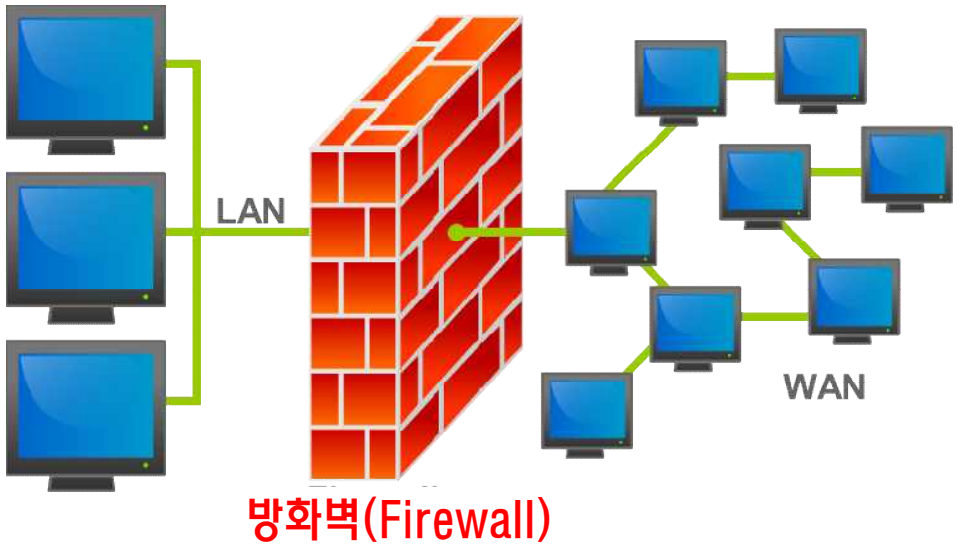
- 바이러스, 악성코드, 음란성컨텐츠, 스팸광고성 App,이상 동작 등

맥어피(McAfee)의 실행

- 알려진 모바일 악성코드에 대한 치료/삭제
- 모바일 악성코드 실시간 감시: 스마트폰으로 파일의 다운로드 또는 복사 및 프로그램이 실행될 때, 모바일 악성코드 감지 및 치료/삭제

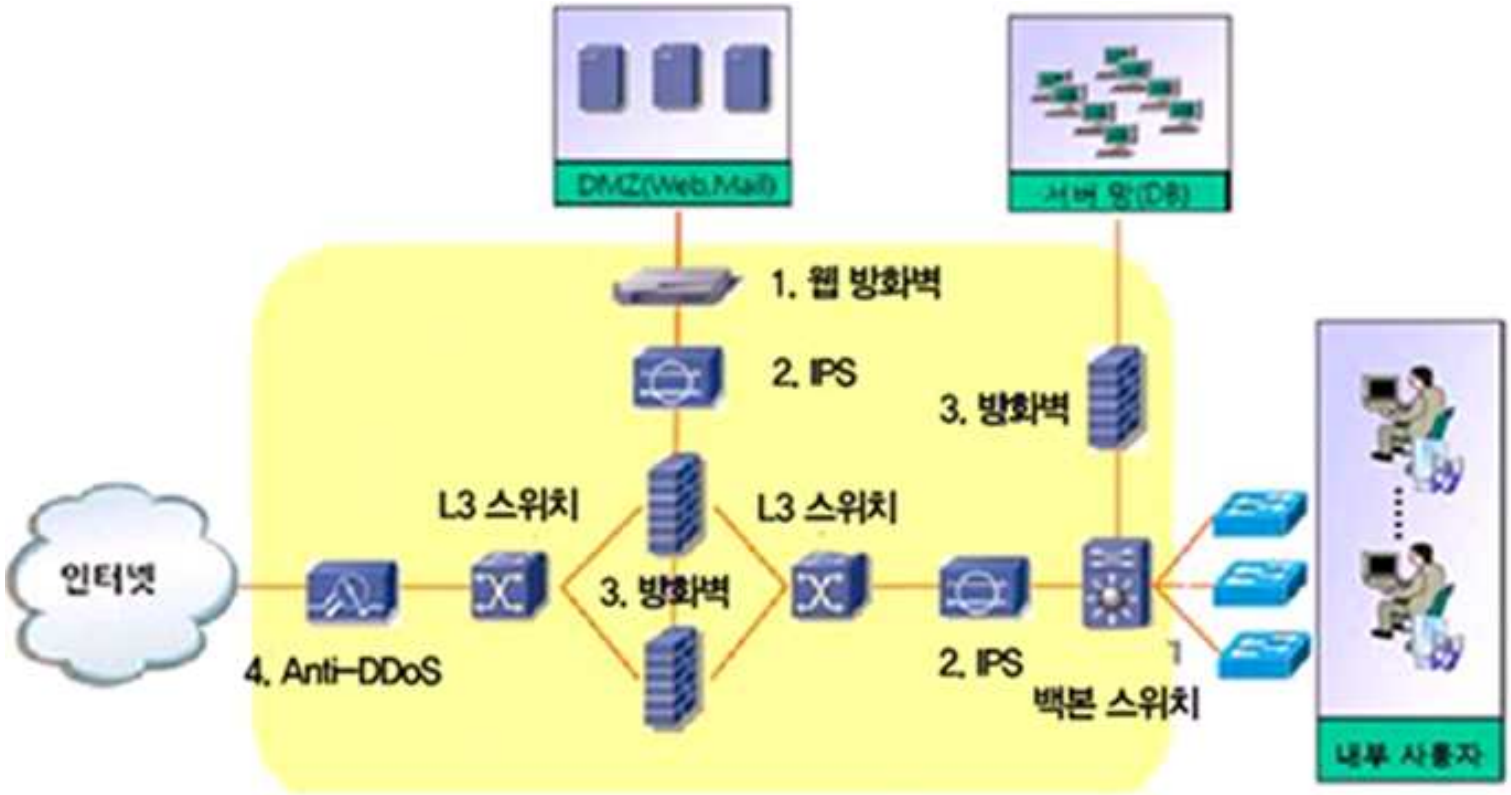
방화벽

- 네트워크를 지나는 메시지의 정보를 확인 후 정책에 따라 목적지 컴퓨터로 해당 정보의 전달 여부를 결정하는 하드웨어나 소프트웨어 장치
- 네트워크를 통해 해커 또는 악성 소프트웨어의 침투를 차단



네트워크의 보안 구성 [1/2]

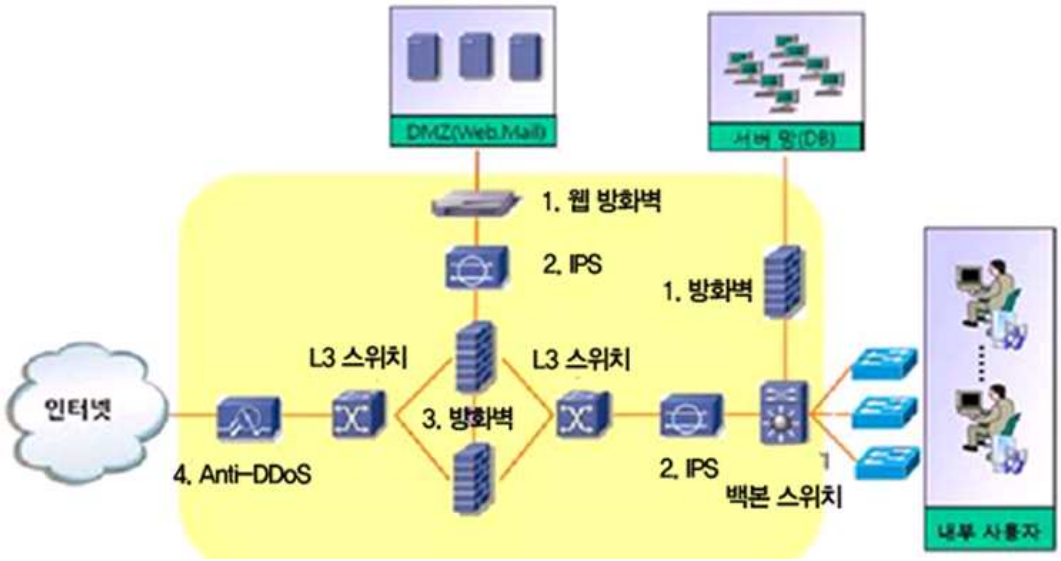
- 내부사용자, DMZ 그리고 서버 망을 같이 보유하고 있는 대다수 사이트의 네트워크 보안 구성(참고: 안철수연구소의 네트워크 보안 Good case Study)
  - ① 웹 방화벽(Web Application Firewall)
  - ② IPS(침입방지시스템)
  - ③ 인터넷 및 서버 망의 방화벽
  - ④ Anti-DDoS(DDoS 대응장비)



네트워크의 보안 구성 [2/2]

❑ 인터넷 및 서버 망의 방화벽

- 인터넷에 대한 방화벽을 구축하여 외부/DMZ/내부 망의 보안 도메인으로 분리 및 접근제어
- 중요한 정보를 보유하고 있는 서버 망에 별도의 방화벽을 구축하여 외부는 물론 내부 사용자로부터의 불법적 접근 차단

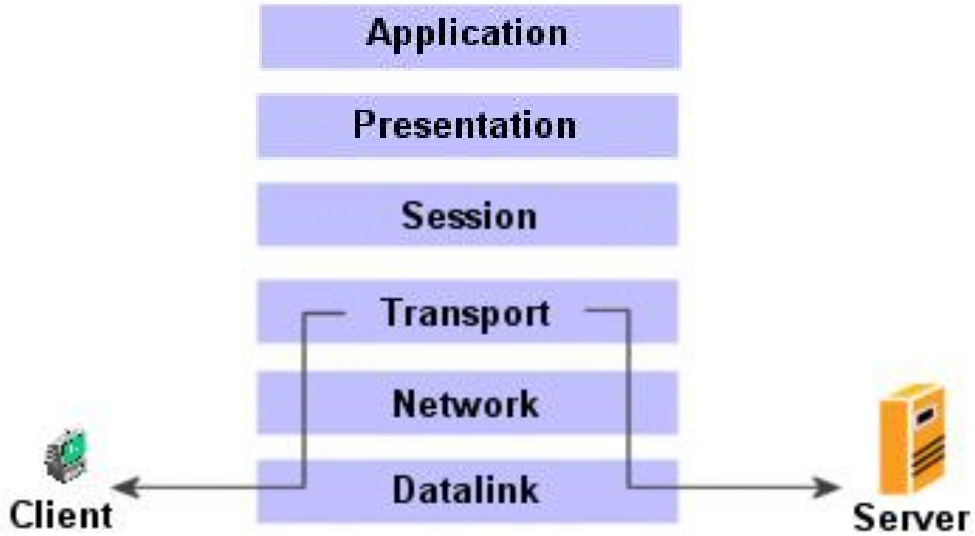


❑ 웹 방화벽

- 근래에 웹 서비스 공격이 많이 발생하므로 웹 서비스가 중요한 사이트의 경우 웹 서비스에 특화된 웹 방화벽 구축
- 웹 서버의 주요 정보에 대한 무결성을 검증하므로 공격에 의한 내부 정보의 변조를 방어

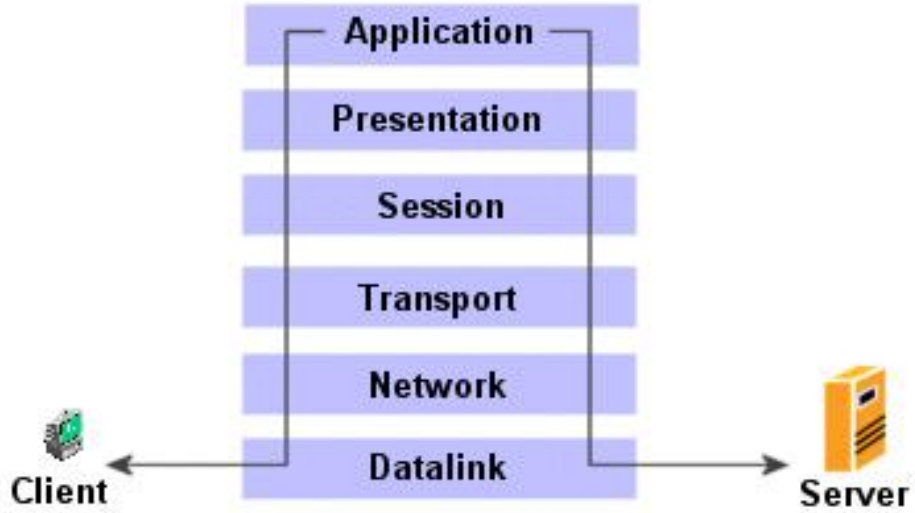
방화벽의 유형(1/3)

- 패킷 필터링 방화벽(Packet Filtering Firewall)
  - 네트워크 계층과 트랜스포트 계층에서 동작하며, 패킷의 주소와 포트 번호 등이 적용되는 보안 규칙에 따라 통과 여부를 결정
  - 3 및 4 계층에서 동작하므로 다양한 응용 서비스의 수용이 가능
  - 세션에 대한 정보를 추적하지 못하며 메시지의 내용에 대한 제어가 불가능
    - 메일 바이러스 같은 경우 패킷 헤더만의 정보를 기준으로 통과 여부를 결정 → 내부 데이터의 분석이 불가능하므로 바이러스의 위험에 노출됨



방화벽의 유형(2/3)

- 응용 게이트웨이 방화벽(Application Gateway Firewall)
  - OSI 7계층 및 응용 서비스에서 동작하며 세션에 대한 정보를 추적할 수 있음
  - 수락할 수 있는 요청 메시지가 도착하면 방화벽이 이를 목적지 서버에 전송하고, 서버로부터 응답을 받아 이를 다시 해당 클라이언트에게 전달하는 프락시 서버로 동작할 수 있음
  - 단점
    - 미리 정의된 응용만 수용이 가능
    - 다양하게 발전하는 새로운 응용을 위하여 새로운 방화벽의 게이트웨이 프로그램 요구

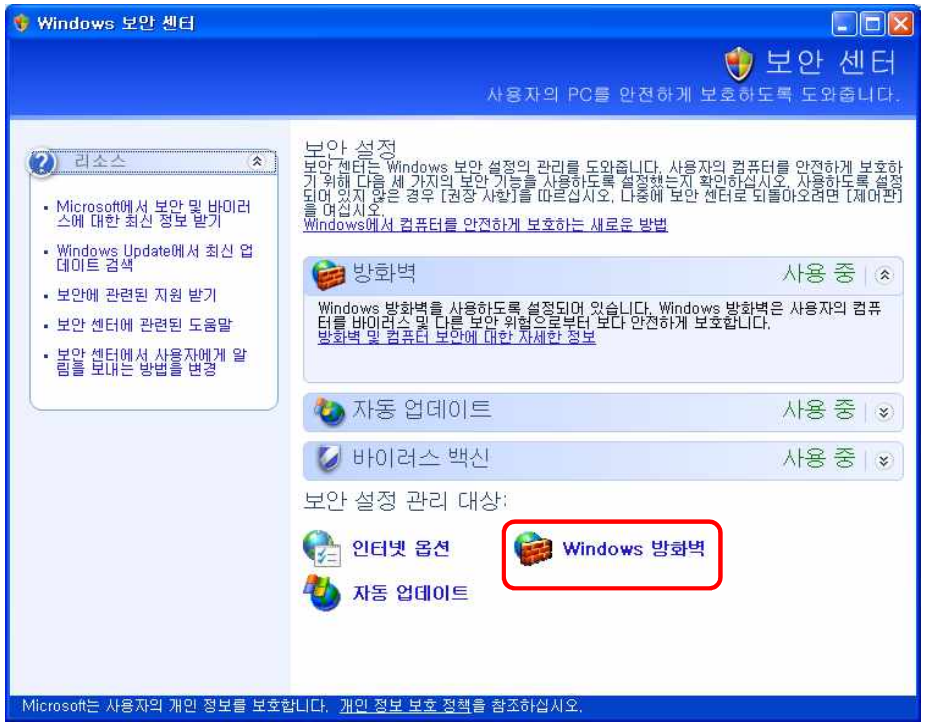


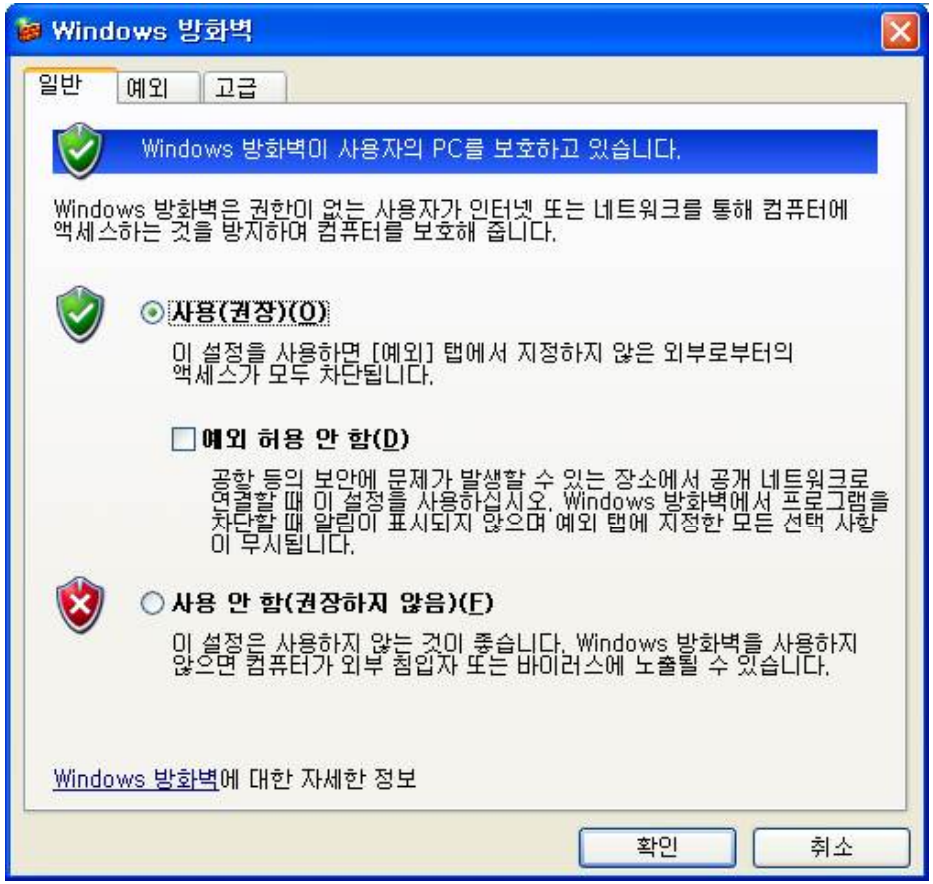
방화벽의 유형(3/3)

- 하이브리드 게이트웨이 방화벽(Hybrid Gateway Firewall)
  - 패킷 필터링과 응용 게이트웨이 방식의 장점을 취하여 결합한 방식
    - 패킷 레벨의 접근 제어뿐만 아니라 응용 프로그램의 제어를 가짐
    - 응용 게이트웨이 방식의 최대 단점인 다양한 응용 서비스의 수용에 대한 제약은 패킷 필터링 방식으로 제공
  - 최근의 제품들은 대부분 하이브리드 게이트웨이 방화벽으로 개발되고 있음

윈도우 방화벽(1/3)

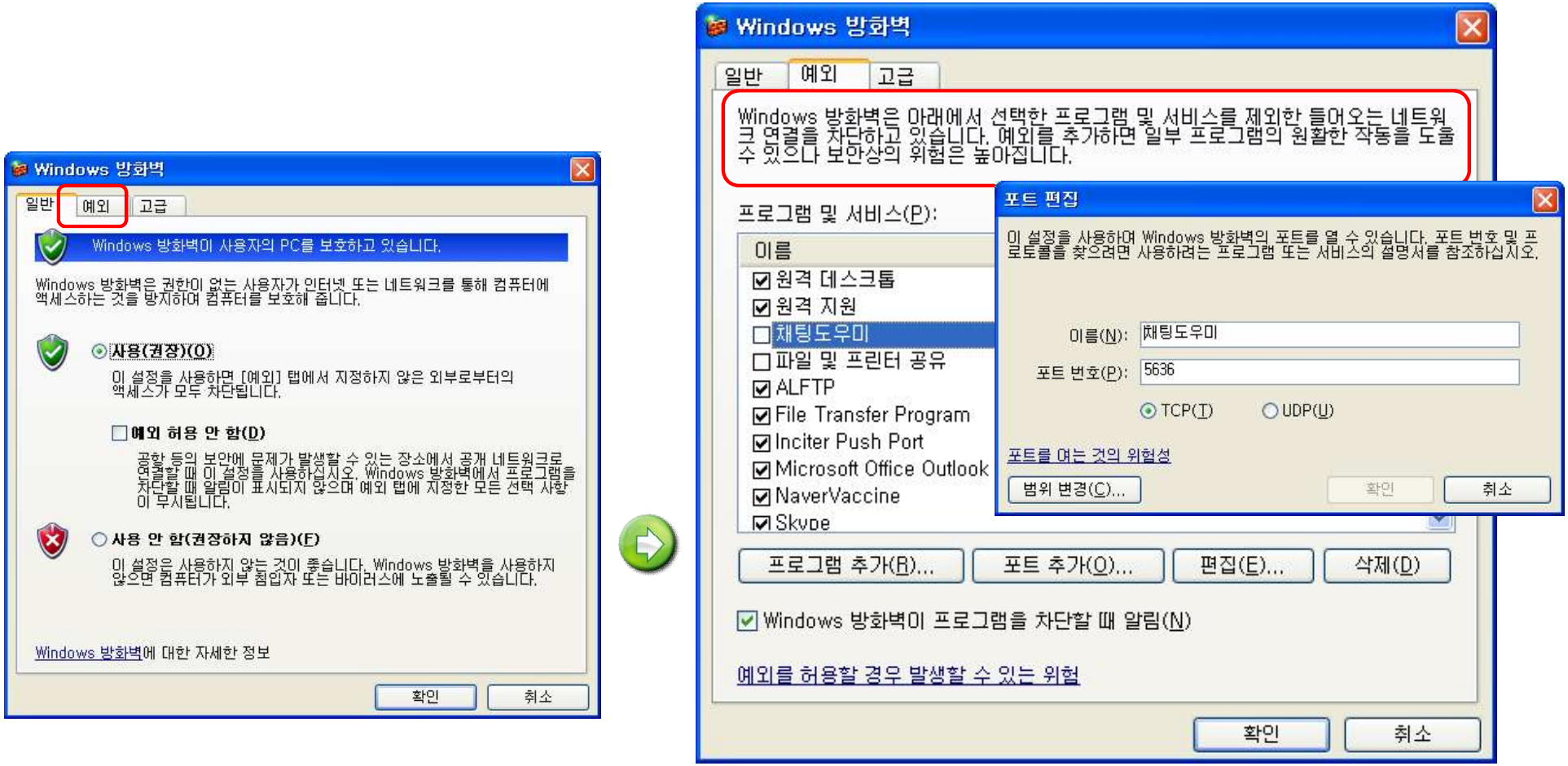
- 권한이 없는 사용자가 인터넷 또는 네트워크를 통해 컴퓨터에 액세스하는 것을 방지하여 컴퓨터를 보호
- 제어판 → 보안센터 → Windows 방화벽





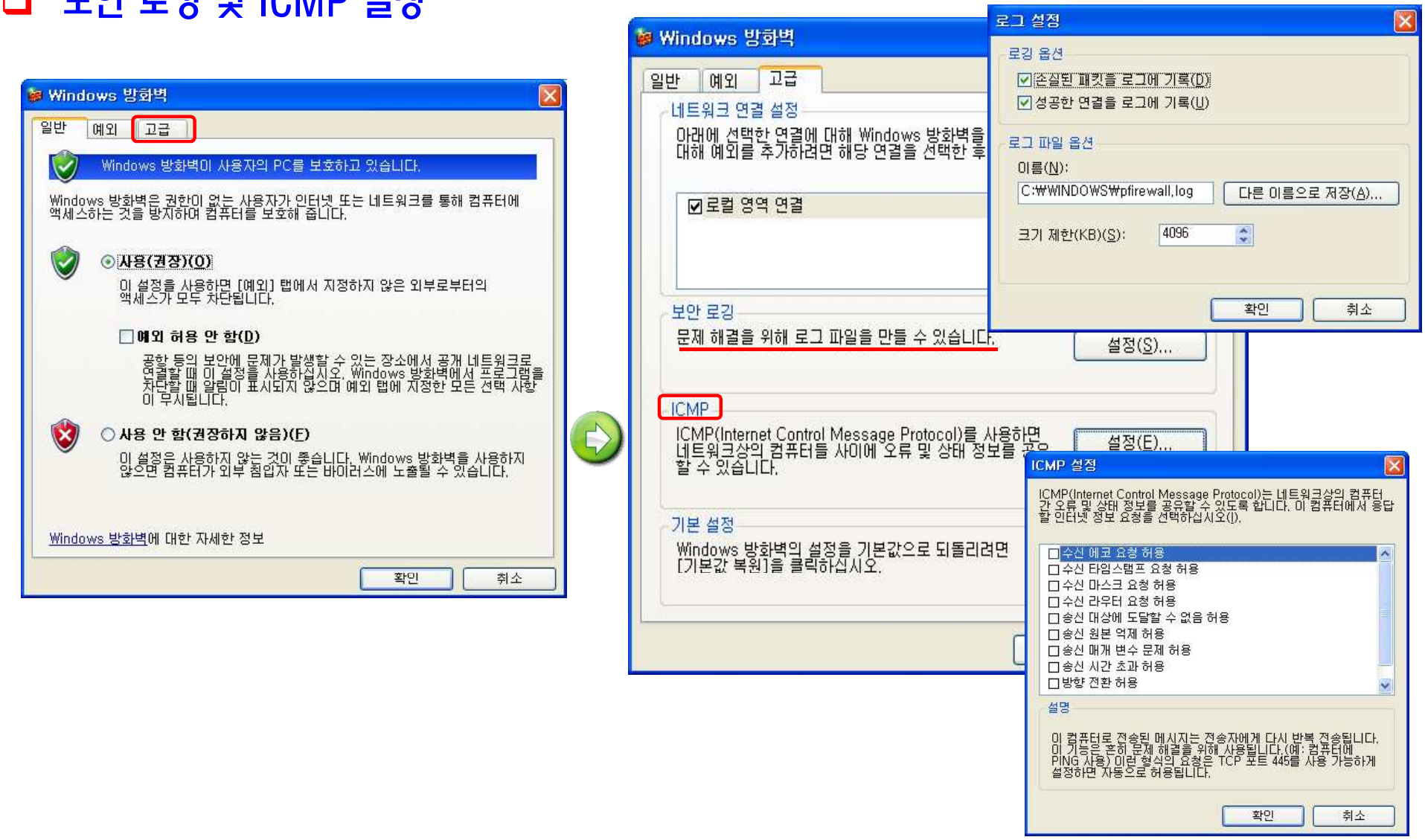
윈도우 방화벽(2/3)

❑ 액세스할 수 있는 프로그램 및 서비스 선택



윈도우 방화벽(3/3)

❑ 보안 로깅 및 ICMP 설정



인터넷 침해 대응 센터(1/4)

❑ KISA의 인터넷 침해 대응 센터(http://www.krcert.or.kr/)

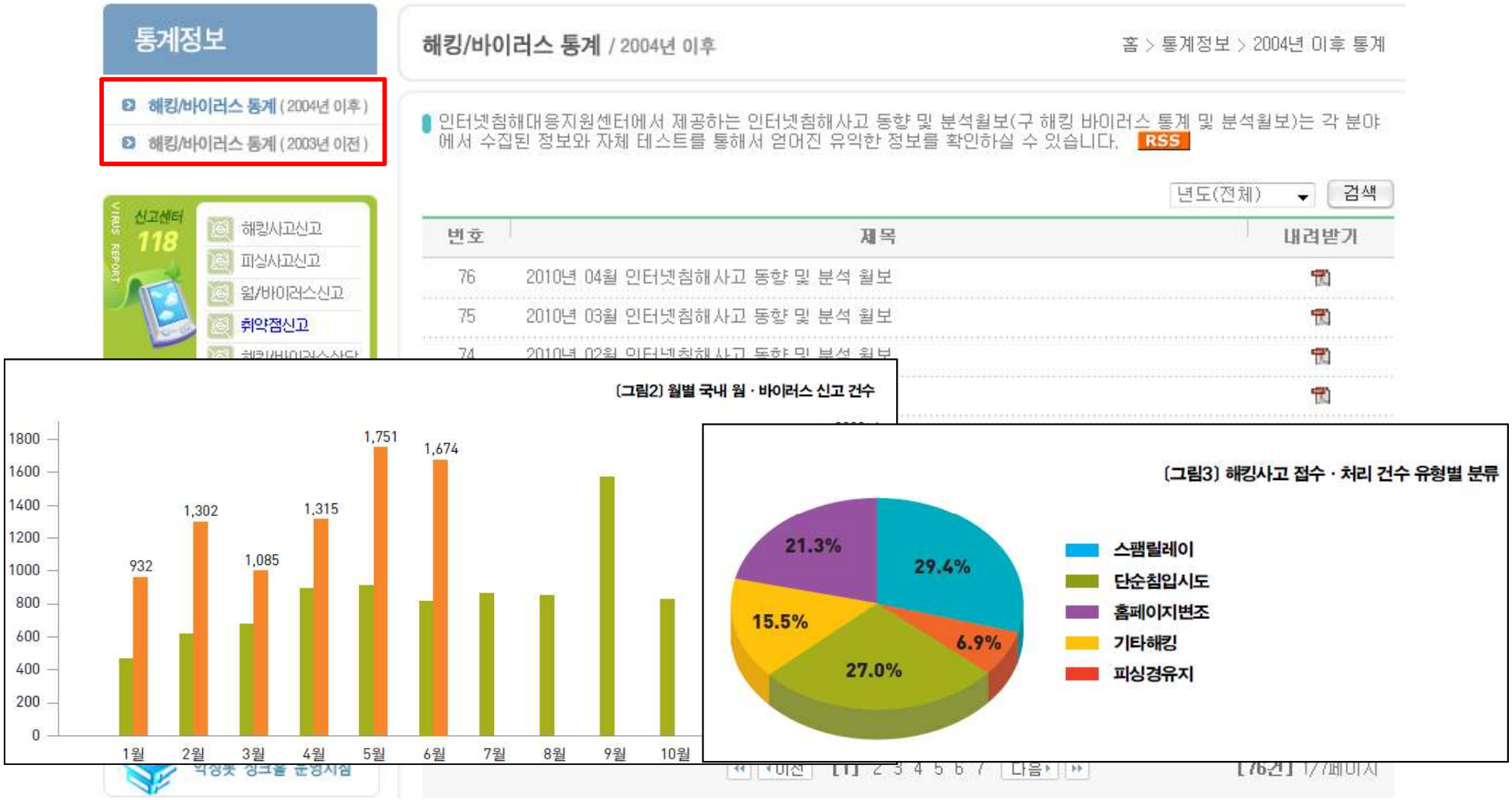
- ❖ 인터넷침해대응센터 운영
  - 365일 네트워크 모니터링
  - 해킹 및 바이러스 경보 발령
- ❖ 침해사고 분석 및 기술 지원
  - 해킹 및 바이러스 기법과 대처방안 연구
  - 비상상황 발생시 긴급대응 지원
  - 바이러스 샘플 채취 및 관련 기술 개발
  - 침해사고 상담 접수 및 처리
- ❖ 침해사고 대응 협력체계 구축

인터넷 침해 대응 센터(2/4)

❑ 보안 정보 : 악성프로그램으로 인한 피해를 예방하기 위한 경보 발령 정보

인터넷 침해 대응 센터(3/4)

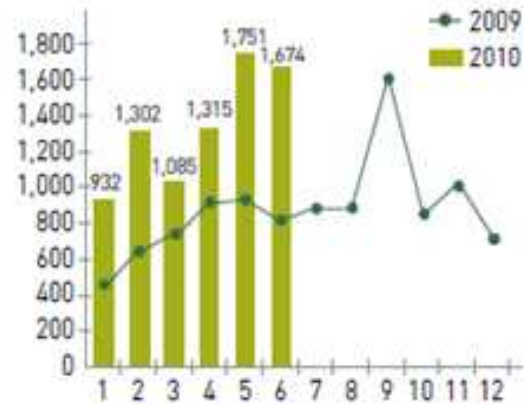
❑ 통계정보 : 통계정보를 통해 사고 동향 및 분석



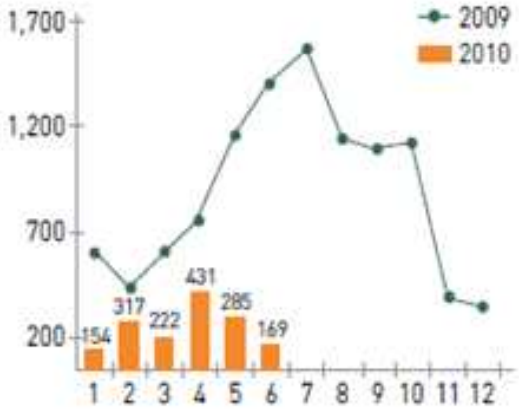
인터넷 침해 대응 센터(4/4)

❑ 월별 침해사고 통계

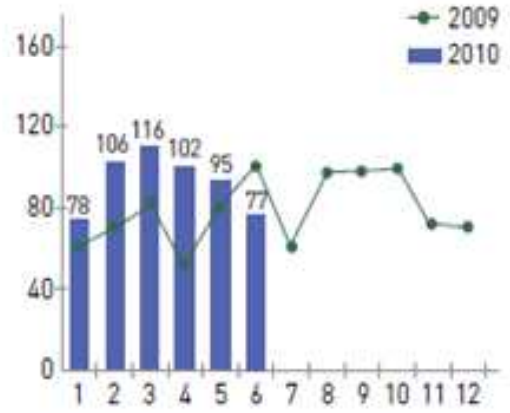
웜 · 바이러스 신고 접수건수



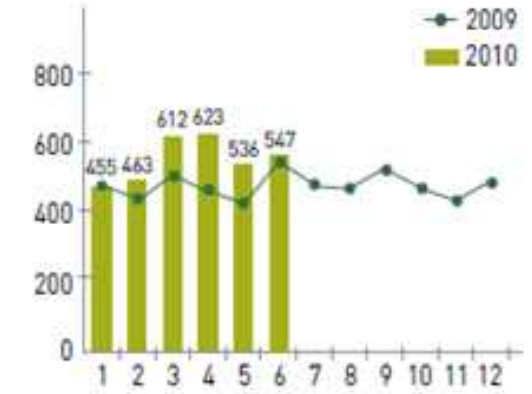
스팸릴레이 신고 처리건수



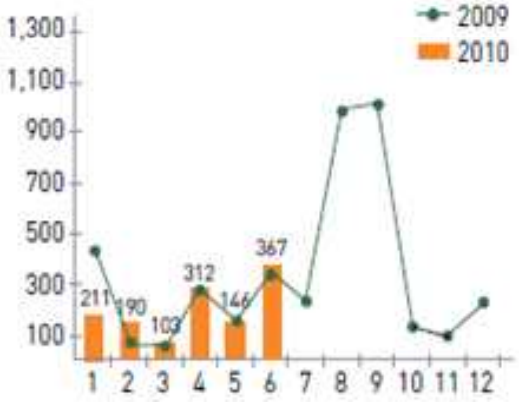
피싱 경유지 신고 처리건수



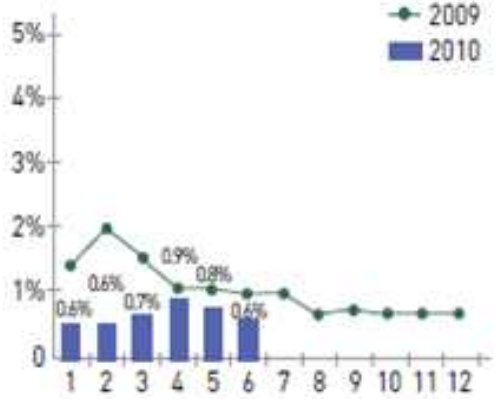
단순침입시도+기타해킹신고 처리



홈페이지 변조사고 처리건수



악성 Bot 감염비율



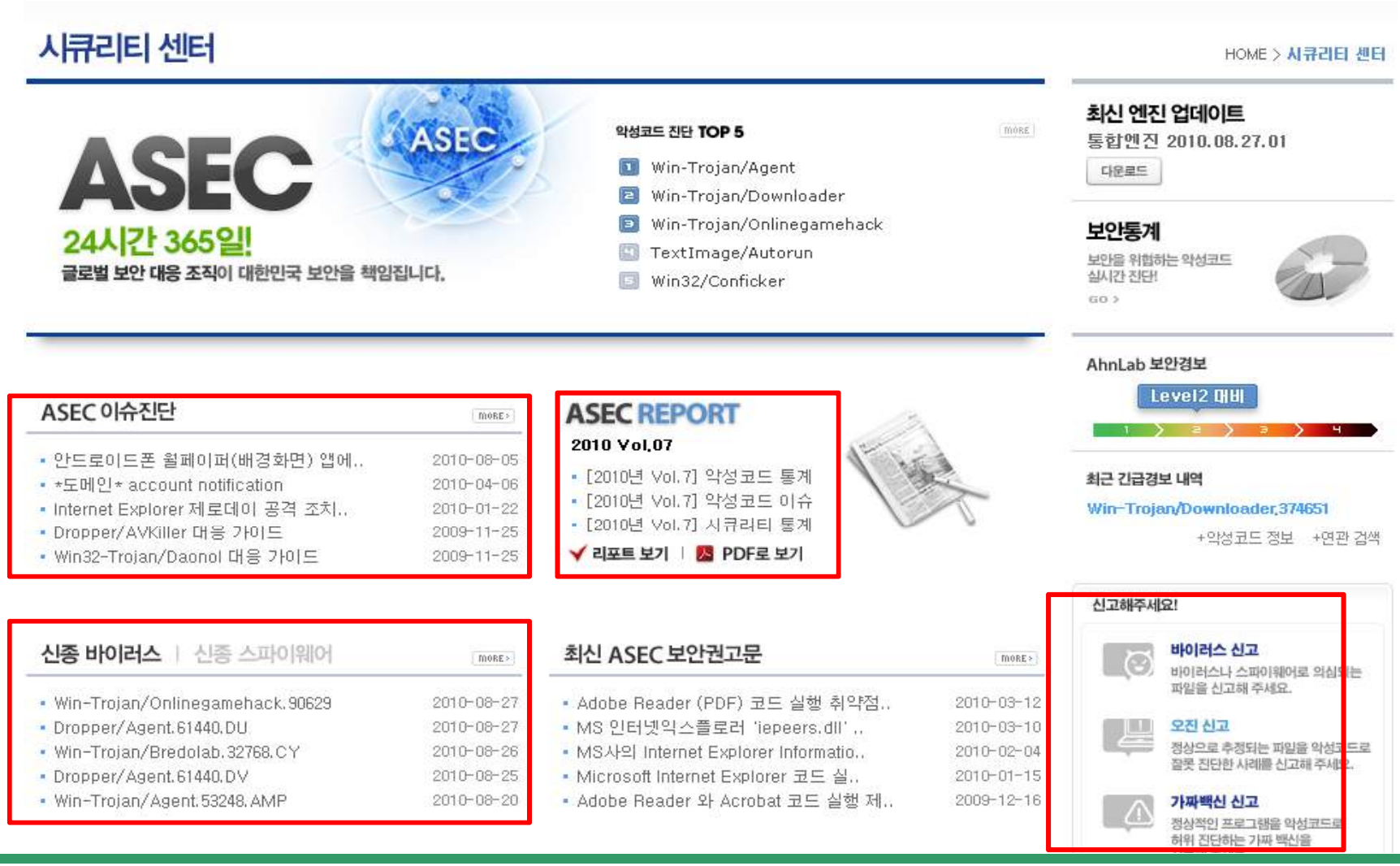
안철수 연구소(1/5)

❑ 안철수 연구소(http://www.ahnlab.com/)

- ❖ 시큐리티 센터
  - 전문가 진단
  - 보안 통계
  - 바이러스 신고 센터
- ❖ 보안정보
  - 보안 뉴스, 전문가 칼럼
  - 보안 용어 사전, 보안 지식 광장
  - 보안 기초정보, PC활용 정보 등
- ❖ 다운로드
  - 제품 관련 파일 다운로드

안철수 연구소(2/5)

- 시큐리티 센터: 전문가 진단, 보안 통계, 바이러스 신고 센터
- ASEC: AhnLab Security Emergency response Center



안철수 연구소(3/5)

❑ 시큐리티 센터의 악성코드 통계

[2010년 Vol.7] 악성코드 통계

출처 : 안철수연구소 조회수 : 1035 | 2010-08-12

2010년 7월 악성코드 통계현황은 다음과 같다.

순 위	등 락	악성코드명	건 수	비 율
1	0	TextImage/Autorun	361089	15.6%
2	0	Win32/Induc	244086	10.5%
3	7	JS/Exploit	239345	10.3%
4	0	JS/Redir	166639	7.2%
5	1	Win32/Olala.worm.57344	115682	5%
6	-1	Win32/Parite	110738	4.8%
7	5	Win-Trojan/Inject.1588224	99516	4.3%
8	-1	Win32/Virut.B	90494	3.9%
9	NEW	Win-Trojan/Agent.110592.PP	89049	3.8%
10	-1	Win32/Conficker.worm.Gen	88490	3.8%
11	NEW	HTML/IFRAME	88079	3.8%
12	NEW	Win-Trojan/Downloader.24576.AGK	81181	3.5%
13	NEW	JS/Agent	79750	3.4%
14	NEW	Win-Trojan/OnlinegameHack6.Gen	75520	3.3%
15	0	Win32/Virut	73128	3.2%
16	NEW	JS/Iframe	72170	3.1%
17	-3	TextImage/Sasan	67906	2.9%
18	-1	TextImage/Viking	61884	2.7%
19	NEW	Win-Trojan/Securisk	55333	2.4%
20	-7	Als/Bursted	54548	2.4%
			2314627	100%

[표 1-1] 악성코드 감염보고 Top 20

보안 통계

VIRUS Win-Trojan/Onlinegamehack.90629

최초 입력시간 : 2010-08-27 14:53 (GMT+9) 최종 수정시간 : 2010-08-27 14:53 (GMT+9)

기본정보 | 상세정보 | 해결 및 예방 | 기타정보

다른 이름	Trojan.Gen, TSPY_LEGMIR.SMXD, Trojan-GameThief.Win32.WOW.abjh, Trojan.Generic.4564428, TR/Hijacker.Gen, Win32:Lmir-KB			
위험도	시스템 위험도	네트워크 위험도	확산 위험도	현재 확산도 그래프 / 위험등급
	높음	낮음	매우낮음	낮음
생성 파일명				
대표적 증상	사용자 정보 유출			
활동 플랫폼	윈도우		감염/설치 경로	파일실행, 다른 악성코드
종류	트로이목마(정보유출)		형태	실행파일
제작국	불분명		최초 발견일	2010-08-19 (현지시각 기준)

▪ 증상 및 요약

Win-Trojan/Onlinegamehack.90629 는 특정 온라인 게임의 사용자 계정을 훔쳐서 특정 메일주소로 전송하는 트로이목마이다.

신종 악성코드

안철수 연구소(4/5)

- 보안정보: 보안뉴스, 용어사전, 지식광장, 보안과 PC상식

안철수 연구소(5/5)

❑ 제품 관련 파일 다운로드

보안뉴스(1/2)

❑ 보안뉴스(http://www.boannews.com/)

- ❖ 보안 기사 제공
- ❖ 보안 실무자들의 정보 공유
- ❖ 보안 클리닉 무료통합 보안서비스 제공

보안뉴스(2/2)

- 보안 실무자들의 정보 공유 및 보안 프리웨어 자료 제공

기타 보안관련 사이트

- 청소년 정보 이용 안전망(http://www.greeninet.or.kr)
- 한국인터넷진흥원의 인터넷침해대응 (http://www.kisa.or.kr/business/violation/main.jsp)
- 한국인터넷진흥원의 보호나라(http://www.boho.or.kr/index.jsp)
- 정보보호기술 온라인 학습장(http://www.sis.or.kr)

요점정리(1/2)

- 백신 프로그램: 악성 소프트웨어를 찾아서 제거하는 기능을 갖춘 컴퓨터 프로그램
  - 안철수 연구소의 V3 Lite(http://www.ahnlab.com)
  - 이스트소프트(ESTsoft)의 알약(http://alyac.altools.co.kr/)
  - 네이버백신(http://security.naver.com)
  - Avast 안티바이러스(http://www.avast.co.kr/)
- 스마트폰의 보안: 손안의 PC로 불리는 스마트폰은 PC가 안고 있는 보안 위험을 그대로 안고 있다.
  - 2009년 상반기에 발견된 전 세계 스마트폰 악성코드는 520여종(2010년 국가정보보호백서)
- 방화벽
  - 네트워크를 지나는 메시지의 정보를 확인 후 정책에 따라 목적지 컴퓨터로 해당 정보의 전달 여부를 결정하는 하드웨어나 소프트웨어 장치
  - 네트워크를 통해 해커 또는 악성 소프트웨어의 침투를 차단

요점정리(2/2)

- 방화벽의 유형
  - 패킷 필터링 방화벽: 네트워크 계층과 트랜스포트 계층에서 동작하며, 패킷의 주소와 포트 번호 등이 적용되는 보안 규칙에 따라 통과 여부를 결정
  - 응용 게이트웨이 방화벽: OSI 7계층 및 응용 서비스에서 동작하며 세션에 대한 정보를 추적할 수 있음
  - 하이브리드 게이트웨이: 패킷 레벨의 접근 제어뿐만 아니라 응용 프로그램의 제어를 가짐
- 인터넷 보안 관련 사이트