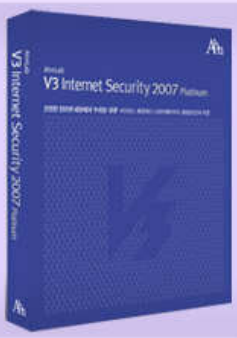
SECURITY LEADER AHNLAB
보/안/리/더/안/랩

- 테마기획 I
- 테마기획 II
- 네티즌 리뷰 1
- 네티즌 리뷰 2
- 네티즌 리뷰 3
- 네티즌 리뷰 4

네티즌 리뷰

파워 유저, V3 IS 2007 Platinum의 장단점을 낱낱이 해부하다



8월~9월에 걸쳐 파코즈하드웨어, 케이벤치, 베타뉴스, 매니안닷컴 등의 인터넷 커뮤니티 사이트에서 V3 IS 2007 Platinum의 대규모 리뷰 이벤트를 진행했다. 각종 소프트웨어, 하드웨어를 꼼꼼하게 사용해보고 상세한 평가를 내리는 '파워 유저'들이 낱낱이 해부한 V3 IS 2007 Platinum의 장단점을 알아보자. 〈편집실〉

매니안닷컴-조성태 | 베타뉴스-허승욱 | 케이벤치-고혜은 | 파코즈-박혜림

1. 컴퓨터 사양

CPU : AMD 2500 바톤

RAM : 512MB

OS : Windows Xp sp2

이정도는 이제 보편적인 컴퓨터 사양이라고 생각된다.

2. V3 Internet Security 2007 Platinum 메인 화면

위와 같이 기본적인 보안 상태를 보여주는 메뉴가 나오는데 현재 컴퓨터의 보안 상태를 3단계로 나누어서 신호등 모양으로 보여준다. 시스템 보안 설정 상태와 개인 보안 설정 상태를 체크할 수 있도록 사용 링크를 누르면 아래와 같은 다이얼로그 창이 뜨면서 옵션 설정을 누구나 손쉽게 변경할 수 있는 인터페이스를 제공한다.

3. 다양한 기능의 V3로 변신

기존의 V3에서는 바이러스 검사와 실시간 감시 방화벽 정도의 기능을 했었지만, V3 IS 2007에서는 기능면과 성능면에서 확 달라진 모습을 보이고 있다.

V3는 바이러스 전문 치료, 스파이제로는 스파이웨어 전문 치료 기능을 각각 제공했던것에 비해서 이제 V3 프로그램에서 통합적으로 2가지 기능을 사용할 수 있게 되었다는 점이 사용자의 입장에선 가장 편리해진 기능이다.

게다가 윈도우 기본 방화벽을 사용하면서 왠지 모를 불안감 혹은 기본 방화벽을 뚫고 들어오는 수많은 웜 바이러스 때문에 다른 방화벽을 따로 설치하여 사용해야했던 수고스러움을 한번에 해결할 수 있게 되었다.

4. 각각의 달라진 점에 대해서 살펴 보기

V3를 써왔던 분들이라면 검사 항목과 실시간 감시 부분에 대해서는 모두 알고 계시리라고 생각되기 때문에 또 지루하게 같은 부분에 대해서 설명을 생략하도록 하겠다.

매크로 바이러스 차단 정책 - 매크로 바이러스란 마이크로소프트 오피스 제품군에서 비주얼 베이직으로 매크로를 작성하여 보다 쉽게 문서 작성을 할 수 있도록 하는 기능인데, 오피스 제품군의 결함이나 오버 버퍼 플로우 등을 활용하여 매크로를 작성했을 경우 특수한 기능을 실행할 수 있는데, 이러한 매크로들을 미리 V3가 읽어들여서 악성 패턴이 발견되면 오피스에서 실행할 수 없도록 미리 차단하는 기능이다. 모두 차단으로 설정하면 모든 매크로를 사용할 수 없으므로 매크로를 사용하지 않는다면 모든 매크로 차단 옵션도 쓸만하다.

바이러스 검사 고급 설정 -

1. 공유폴더 해제하고 검사 기능 - 본인의 컴퓨터에 공유된 폴더를 검사하고 싶지 않을때 체크하면 된다. 하지만 네트워크 공유된 폴더를 경유해서 바이러스가 이동하는 경우가 많으므로 대부분 체크하지 않고 사용한다.

2. 쉘 프로세스를 멈추고 검사 - 예전에 만들어지는 대부분의 바이러스는 독립적인 실행파일에 기생해서 실행되는데 비해서 요즘의 바이러스는 대부분 인터넷 익스플로어에 OCX(액티브엑스)나 DLL 파일로 익스플로어가 로딩될때 Attach되어 실행된다. 따라서 바이러스를 치료하기 위해선 익스플로어의 작동을 중단하고 치료해야하는데 익스플로어가 운영체제의 쉘이기 때문에 바이러스 치료하기 위해서 윈도우 재부팅을 하는 경우가 있었다. 하지만 몇몇 파일삭제 프로그램중에 UnLock과 같은 방식으로 바이러스가 익스플로어에 Attach되어 있을 경우 Detach해서 익스플로어에서 떼어낸 후 파일을 삭제하는 것과 같이 V3에서도 이러한 기능을 사용할 수 있게 되었다. 따라서 바이러스 치료를 위해서 재부팅 하는 경우가 획기적으로 줄어들게 되었다.

3. 분산 검사 - 바이러스를 검사하는 방식은 여러가지가 있을 수 있는데, CPU가 2개 이상이 될 경우에는 멀티스레드로 검사하는 것이 더 효율적이다. 윈도우는 기본적으로 비동기 IO를 지원하므로 입출력 대기 시간이 있을 경우 다른 스레드가 CPU를 활용하는 편이 더 빠르다. 윈도우 소켓 프로그래밍에서는 이러한 방식을 IOCP(입출력 완료포트)라 하는데 V3에서도 멀티 CPU일 경우에는 이러한 기능을 사용하는 것으로 보인다. 따라서 CPU가 듀얼 코어 이상인 분들을 이 옵션을 체크하면 보다 빠른 검사가 가능하다.

4. 설정된 속도로 바이러스 검사 - 이 부분은 윈도우 작업 관리자에서 프로세스에서 오른쪽 마우스 버튼을 누를 경우 우선 순위 설정 메뉴가 나오는 것을 볼 수 있는데 높음으로 해주면 윈도우에서 해당 프로그램의 우선 순위를 올려줌으로써 좀더 많은 CPU 시간을 할당 해주는 원리이다. 따라서 이 옵션을 켜두면 CPU 점유율이 더 올라가는 것을 볼 수 있다.

기타 고급기능 설정

1. 공유 폴더에 접근하여 바이러스를 감염시키는 컴퓨터 추적 - 웜 바이러스의 경우에 139포트(윈도우 netbeui 프로토콜이 사용하는 포트)로 공유 폴더가 열려 있는지 검사해서 공유폴더에 계속적으로 접근 시도하여 비밀번호를 풀고 들어오려는 시도를 하는 경우도 있다. 따라서 특정 시간 동안 몇회 이상(예: 10초 동안 1000번)의 시도를 할 경우엔 바이러스로 간주하여 해당 IP주소를 차단함으로써 계속적인 웜바이러스의 침투 시도를 사전에 막을수 있는 기능이다.

2. V3 Internet Security 프로그램 자체 보호 - V3를 공격하는 바이러스가 있다는 사실을 모르는 분들이 의외로 많다. 심지어 예전의 V3는 자신이 바이러스에 걸렸는데도 불구하고 바이러스 검사를 해서 다른 파일들에게 계속 감염시키는 경우도 발생하였다. 그러나 몇년전의 안철수 연구소의 기술력과 지금의 기술력은 많은 차이를 보여주고 있다. 요즘의 바이러스들은 DLL 인젝션이나 Attach 기능은 기본적으로 갖추고 있고, 심지어 자기 암호화 방식까지 갖춘 차세대 바이러스까지 등장했다. 이에 안철수 연구소에서도 핵쉴드 등을 개발하면서 프로그램 방어 시스템에 대한 많은 발전이 있었다. 이 기술을 이번 V3 IS 2007에 적용한 것으로 보인다.

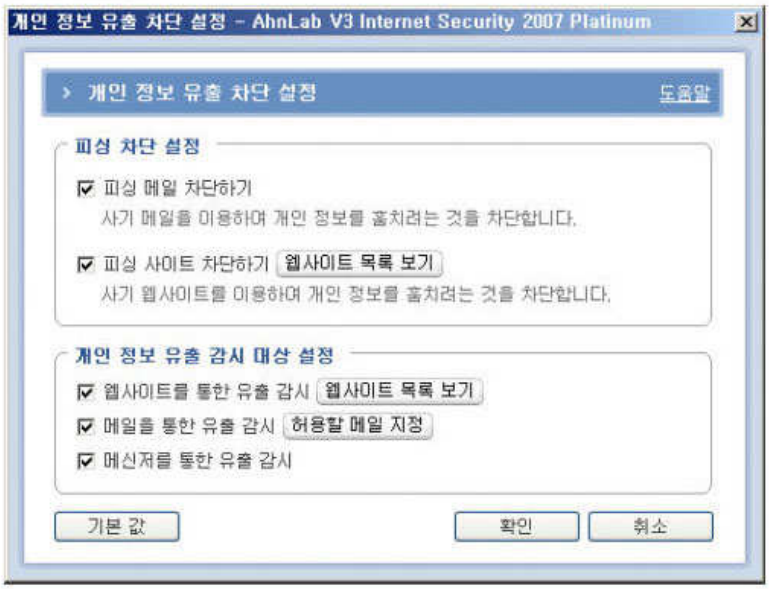
3. Microsoft Office 프로그램이 여는 파일을 자동으로 검사 - 오피스 제품군을 사용하면서 불편한 점이 매크로 바이러스나 원하지 않는 작동을 하는것에 대해서 MS에서 패치를 제공하기 전까진 막을 수 없다는 점이었다. 그러나 V3에서 이러한 작동을 하는 바이러스를 발견하면 바로 v3엔진에 업데이트 해서 오피스 제품군의 작동하기 전에 차단해 주기 때문에 Office를 쓰면서 불안한 점을 어느정도 예방할 수 있다. 그러나 오피스 제품군의 속도 저하가 느껴진다면 이 옵션 선택에 대해서 고려해보고 사용하길 권장한다.

스파이웨어 실시간 검사 - ActiveX로 설치되는 스파이웨어가 나날이 발전하고 있다. 자신도 모르는 사이에 JaveScript와 여러가지 회피 기법을 이용해서 인터넷의 곳곳에 숨어 있기 때문에 스파이웨어가 1개도 없는 컴퓨터를 보기 드물 정도다. 하지만 1-2년 전부터 안철수 연구소에서 스파이제로 서비스를 제공하면서 많은 검증을 받았고 신뢰도도 높아졌다. 필자도 예전의 V3보다는 스파이제로가 더 믿음직하다는 느낌을 받았었다. V3 IS 2007에서는 기존의 스파이제로 기능을 고스란히 물려받아서 스파이제로에 대한 걱정을 말끔히 씻을 수 있게 되었다.

해킹 차단(방화벽 기능) - 기존의 윈도우 방화벽으로 불안했었다면 V3 개인 방화벽 사용을 강력히 권장한다. 기존의 방화벽 시스템은 프로그램이 실행될때 차단할지 실행할지 선택하거나 원하는 포트 번호를 막는 수준이었다면, V3의 새로운 방화벽 시스템은 네트워크 침입 차단에 서버급 보안 시스템에서나 볼수 있는 네트워크 패킷 패턴 분석에 의한 침투 방지 기능을 포함하고 있다.
예를 들어 A 웜 바이러스가 포트 스캔을 2번 한 후에 어떤 패킷을 보내고 2초 후에 다시 포트 스캔 후 어떤 패킷을 보낼 경우에 이러한 패턴이 발견되면 해당 IP를 막는 기능이라고 보면 되겠다. 이러한 기능이 중요한 이유는 예전에 블래스트웜 대란과 같이 특정패킷의 UDP 패킷 공격과 같은 웜 바이러스가 컴퓨터에 침투하기 전에 그러한 패킷 패턴을 분석하여 미리 막음으로써 바이러스가 걸리고 난 후에 치료하는 것이 아니라 그러한 웜 바이러스의 침투 자체를 미연에 방지하는 시스템이라고 보면 된다.

개인 정보 보호 - 개인 정보 보안 상태에 4가지 기능이 담겨져 있다.

1. 개인 정보 유출 차단



인터넷 피싱 차단 : 피싱이란 낚시다. 예를들어 인터넷 뱅킹을 이용하고 있는데 kbxxx.com으로 직접 주소를 입력하지 않고 국xxx 바로가기 링크를 눌러서 이동했을 경우에 aaa.com과 같은 kbxxx.com의 모양을 그대로 본따서 만든 사이트로 이동하게 되었다고 가정하자, 인터넷 이용자는 아무 생각 없이 aaa.com이 kbxxx.com인줄 알고 로그인 아이디 비밀번호를 입력하는 순간 바로 aaa.com DB에 입력안 ID와 패스워드가 입력된다. 이것이 바로 피싱인데, 쏙 ID, 패스워드 뿐만이 아니라 익스플로어에 남아 있는 쿠키 정보를 훔쳐와도 세션정보를 가지고 로그인 할 수 있는 것이 사용자의 부주의에 의한 아주 심각한 크래킹 기법이 된다는 것이다. V3에는 이러한 피싱을 방지하는 기능이 추가된 것이다.

게다가 메일이나 메신저를 이용한 피싱도 막아주는 기능을 추가하여 인터넷을 사용하는데 좀더 안심하고 편하게 이용할 수 있다.

2. 웹사이트 필터링 - 간혹 인터넷을 돌아다니다 보면 새로운창이 계속 뜨면서 익스플로어가 꺼지지 않는 사이트가 있다. 이러한 사이트의 주소를 웹사이트 필터링에 넣어두면 해당 주소가 입력된 사이트는 접근하지 않으므로 이러한 불편한 점을 미리 방지할 수 있다.

3. 파일 암호화 - 인터넷으로 파일을 전송할 경우에 중간에 패킷 스니핑으로 데이터를 빼내갈 우려가 있거나 내 컴퓨터에서 다른 사람이 접근하지 못하게 데이터를 암호화 하고 싶은 경우에 특별한 프로그램을 설치해서 사용했어야 했다. 그러나 V3에는 파일 암호화 기능을 추가하여 파일에 패스워드를 걸어서 암호화하여 패스워드를 알지 못할 경우에는 풀 수 없도록 하는 기능을 추가하였다. 암호입력 3회 실패시 다시 클릭해서 풀도록 프로그램을 종료하는 기능을 가지고 있다.

ASPack 변형으로 압축(Packing)한 후 약청스 내부 Encryptor 알고리즘을 사용해을 것으로 보인

다. 이 외의 특별한점을 발견할 수 없으므로 기업용이 아닌 개인용으로 사용하길 추천한다.

4. 파일 완전 삭제 - 윈도우에서 파일을 삭제하면 FAT(File Allocation Table)나 NTFS 파일 시스템중에서 파일의 시작 1글자를 지운다. 따라서 파일 복구 프로그램등을 이용해서 파일의 첫번째 글자를 넣어주고 파일이 위치한 부분의 섹터를 다 찾아주면 파일 복구가 가능하다. 이러한 복구가 불가능하게 하기 위해선 파일이 위치한 곳 위에 데이터를 덮어쓰는 방법으로 지워야 하는데, 다른 프로그램을 설치하지 않아도 V3에서 이러한 기능을 제공한다.

기본값으로 US DOD 알고리즘으로 지우지만 일반 사용자라면 저 방법이 속도가 느리게 되므로 낮음이나 아주 낮음을 사용하는 것이 속도면에서 도움이 될 것이다.

메일 보안 - 아웃룩 익스프레스로 메일을 보는 사람들에게 매우 필요한 기능이다. 특히 웹메일이 아닌 아웃룩으로 메일을 관리하는 사람들에게는 메일에 첨부된 바이러스와 스팸메일 차단이 잘 안되는 점 또한 메일 차단 옵션 설정등이 불편하여 아웃룩 자체가 스팸메일과 바이러스의 온상이 되는 경우가 허다하다 V3는 바로 이러한 위험이나 불편한 점에서 벗어나서 보다 괘적한 환경으로 만들어준다.

마지막으로 로그보기 기능이 있다. V3에서 일어난 모든 일들에 대한 로그가 남기 때문에 로그만 분석해 보더라도 언제 내 컴퓨터가 어떤 상황에 처해 있었는지를 판단해서 보안 설정을 더 강화할 것인가 아니면 지금보다 보안 설정을 낮출 것인가를 판단할 수 있게 된다.

V3 IS 2007은 이전의 V3와는 달리 통합 윈도우 보안 시스템으로 새롭게 태어났다. 초창기부터 V3를 사용했다가 V3를 믿지 못해서 봉인했던 유저들은 다시 한번 V3 IS 2007을 사용해보길 추천한다. 그만큼 획기적이고 다양한 기능을 가진 통합 관리 시스템으로 바뀐 V3 !!!
이제는 컴퓨터에 V3하나면 모든게 해결되지 않을까?

마치면서.. 이번 필드테스트를 할 수 있게 기회를 준 베타뉴스 관계자 분들에게 감사하고, 지금까지 외면 당했던 V3를 다시 새로운 모습으로 만들어준 안철수연구소 개발자분들에게도 깊은 감사의 말씀을 전합니다.

나도 한마디!

페이지조회수: 769

작성자 비밀번호

내 용 글올리기

작성자 김린경 [삭제]

내 용 리뷰 깔끔하고 내용도 좋네요 ^^; 잘 보았습니다.

작성자 김현수 [삭제]

내 용 마치 제품의 설명서를 읽는 듯한 느낌이네요... 아주 자세하게... 이야... 막, 사용하고싶어집니다^^

작성자 V3 사용자 [삭제]

내 용 좋은 리뷰였습니다.역시 v3~!@

2006년 11.12월호

[11,12월호] 2006년 11월 6일
월요일 발행 (제 29호)